КИБЕРДЗЮЦУ

кибербезопасность для современных ниндзя

Бен Маккарти

no starch press

CYBERJUTSU

Cybersecurity for the Modern Ninja

by Ben McCarty

no starch
press

San Francisco

КИБЕРДЗЮЦУ

кибербезопасность
для современных ниндзя

Бен Маккарти

ПИТЕР®

Санкт-Петербург • Москва • Минск

2022

ББК 32.973.23-018-07
УДК 004.56.53
М15

Маккарти Бен

М15 Кибердзюцу: кибербезопасность для современных ниндзя. — СПб.: Питер, 2022. — 224 с.: ил. — (Серия «Библиотека программиста»).

ISBN 978-5-4461-2958-4

Кибердзюцу — это практическое руководство по кибербезопасности, в основу которого легли техники, тактики и приемы древних ниндзя. Специалист по кибервойне Бен Маккарти проанализировал рассекреченные японские трактаты и рассказывает, как методики ниндзя можно применить к сегодняшним проблемам безопасности, например для ведения информационной войны, проникновений, шпионажа и использования уязвимостей нулевого дня.

16+ (В соответствии с Федеральным законом от 29 декабря 2010 г. № 436-ФЗ.)

ББК 32.973.23-018-07
УДК 004.56.53

ISBN 978-1718500549 англ.

ISBN 978-5-4461-2958-4

Краткое содержание

Оглавление

Посвящается моей прекрасной Саре
и тем беспомощным компаниям, которые боятся
новых идей и в упор не видят своих слабых
сторон, — именно они побудили меня
написать эту книгу

Об авторе

Бен Маккарти — бывший разработчик из АНБ. Один из самых квалифицированных специалистов по кибервойне, служивших на сетевом фронте. Бен успел поработать хакером, специалистом по отработке инцидентов, охотником за угрозами, аналитиком вредоносных программ, инженером по сетевой безопасности, аудитором соответствия, специалистом по анализу угроз и специалистом по развитию. Ему принадлежат несколько патентов и сертификатов в сфере безопасности. В настоящее время занимается исследованием квантовой безопасности в Вашингтоне.

О научном редакторе

Ари Шлосс начал свою карьеру в Министерстве национальной безопасности США. Имеет степень магистра в области ИБ и MBA. В настоящее время работает инженером по безопасности на оборонную компанию в Мэриленде.

Предисловие

Кибербезопасность никогда прежде не была столь важна для экономического процветания и социального спокойствия, как сегодня. Необходимость защиты интеллектуальной собственности бизнеса и персональных данных простых людей имеет первостепенное значение. Киберпреступники становятся быстрее, изобретательнее, организованнее и все лучше обеспечены. Специалисты по кибербезопасности постоянно обнаруживают новые угрозы и отражают новые атаки, несмотря на все принятые меры информационной безопасности (ИБ). Перед нами гонка кибервооружений.

На следующих двухстах страницах Бенджамин Маккарти, блестящий эксперт по анализу киберугроз и исследователь в сфере безопасности, которого я давно знаю, расскажет, как защитить информацию от хакеров.

Когда 15 лет назад я учился в аспирантуре, первым усвоенным мной уроком на занятиях по инженерии безопасности было простое правило: думай как хакер. В сфере кибербезопасности мы активно проповедовали это правило в течение нескольких лет, а то и десятилетий. Но судя по количеству кибератак, которым ежегодно подвергаются разные компании, это сообщение так и не дошло до большого количества ИБ-специалистов. Это происходит по двум причинам. Во-первых, в этом правиле маловато подробностей. Во-вторых, если подробности и есть, их может быть очень трудно понять. Бен решает обе проблемы, изменив формулировку с «думай как хакер» на «думай как ниндзя».

«А это как?» — спросите вы. Ответ кроется в трактатах ниндзя, которые были написаны еще в Средние века, но хранились в строгом секрете до середины XX века. Они только недавно были переведены с японского. В них говорится, как ниндзя думают, разрабатывают стратегии и действуют. Воюя скрытно, они ревностно

хранили в секрете свою стратегию и тактику. Теперь же откровения, ставшие известными благодаря публикации этих трактатов, заслуживают глубокого анализа и могут помочь понять, что на протяжении долгих веков делало ниндзя такими успешными в шпионаже, обмане и внезапных атаках.

Бен проанализировал эти трактаты и извлек из них стратегии, тактики и приемы, которые ниндзя использовали в своих операциях. Он сопоставляет их с современными тактиками, техниками и процедурами (ТТП), применяемыми хакерами для проведения кибератак. Изучение этого руководства и описанных в нем процедур поможет специалистам по безопасности понять образ мышления не только ниндзя, но и киберпреступника. Поняв его, вы сможете научиться мыслить как хакер и усвоить этот принцип безопасности. Это не только поможет вам предсказать следующий потенциальный ход злоумышленника, но и даст время подготовиться к нему и укрепить оборону, помешав нападающему достичь своей цели.

Еще одна причина, по которой Бен использует трактаты ниндзя, — это желание приблизить их ТТП к работе ИБ-специалистов, что тоже разумно, ведь в трактатах ниндзя описаны реальные атаки в физическом мире на физические объекты и в физической среде. Нашему мозгу гораздо легче визуализировать физическую среду, чем виртуальную. Если представить, что тактика и методики хакера применяются в реальном мире, они сразу станут более заметными и понятными. Вы станете понимать, как злоумышленник применяет ту или иную тактику для компрометации некоторого актива или перехода от одного актива к другому. В каждой главе Бен проводит аналогию через теорию за́мка, то есть сначала представляет описываемые события так, как если бы они происходили в средневековом замке, а затем переносит их в киберсреду.

Читателям будет невероятно полезно изучить множество советов и стратегий, описанных Беном. Эти знания сейчас как раз кстати, ведь кибербезопасность становится одной из основных опор нашей экономики. Бен Маккарти с его десятилетним опытом работы в разведке угроз имеет и возможности, и желание научить вас думать как ниндзя и хакер, а также помочь защитить как свою информацию, так и цифровую экономику в целом.

Малек бен Салим,
доктор наук, ведущий исследователь и разработчик
в области безопасности, Accenture

Благодарности

Начну с благодарности моей прекрасной Саре. Она помогала мне с момента чтения черновиков до оформления обложки и дала мне свободу, чтобы я мог написать книгу, большое ей спасибо.

Спасибо Крису Сент-Майерсу за то, что под его руководством я заинтересованно и увлеченно занимался глубоким исследованием вопросов кибершпионажа. Этот опыт важен для понимания того, как мыслят те, кто создает угрозы в данной сфере. Он меня никогда не останавливал, а лишь воодушевлял и многому научил.

Я бесконечно благодарен подразделениям TRADOC и DETMADE Армии США, которые осознали мой потенциал и определили меня в передовое подразделение в сфере кибервойны. Этот уникальный опыт был невероятно важен и помог мне понять, что такое кибербезопасность и каковы методы работы операторов.

Особая благодарность Энтони Каммингсу и его команде за перевод трактатов ниндзя и их публикацию для англоязычного мира. Именно благодаря вашим усилиям и заразительной страсти к ниндзя я нашел вдохновение для написания этой книги.

Спасибо ребятам из издательства No Starch Press, которые помогли улучшить мою работу и превратить ее в книгу, которой я горжусь.

Наконец, спасибо всем, кто был частью моего пути в сфере кибербезопасности. Мне было очень приятно учиться у других профессионалов в этой области и расширять свои знания и понимание сферы компьютерной безопасности. Чтобы написать эту книгу, мне нужно было знать все до последней мелочи.

От издательства

Ваши замечания, предложения, вопросы отправляйте по адресу comp@piter.com (издательство «Питер», компьютерная редакция).

Мы будем рады узнать ваше мнение!

На веб-сайте издательства www.piter.com вы найдете подробную информацию о наших книгах.

Введение

Скажу сразу: я не ниндзя. И даже не историк, изучающий ниндзя, не сенсей и вообще не японец.

Но зато я действительно вел кибервойну, и мои сослуживцы часто называли нас «высокоскоростными ниндзя». Именно тогда я начал замечать, что в кибербезопасности часто звучит слово «ниндзя». И захотел понять, почему вообще употребляется такой термин. Я начал изучать ниндзя в 2012 году, и именно тогда наткнулся на недавние английские переводы японских трактатов, написанных более 400 лет назад (подробнее о них — в разделе «Об этой книге» далее). Эти трактаты были учебными пособиями, которые ниндзя использовали для изучения своего ремесла. То есть это не исторические отчеты, а настоящие учебники. Один из них под названием «Бансэнсюкай» был рассекречен правительством Японии и опубликован (и то не для всех) только после Второй мировой войны, поскольку в течение почти 300 лет эта информация считалась слишком опасной для распространения. В Средние века эти документы не разрешалось видеть никому, кроме ниндзя. На них даже есть предупреждения крупным шрифтом о необходимости защищать информацию ценой своей жизни. Было время, когда лишь обладания таким трактатом было достаточно для того, чтобы тебя казнили. И именно запретный характер материала делал чтение еще более интересным и загадочным. Меня зацепило.

Прочитав более 1000 страниц переведенных материалов, я понял, что инструкции и секретные техники, предназначенные для ниндзя, по сути представляли собой обучение в области обеспечения безопасности информации, проникновения, шпионажа и атак, связанных с тайным доступом в защищенные организации. Многими из этих вещей я ежедневно занимался, работая в сфере кибербезопасности. Учебники 400-летней давности были полны идей о защитной и наступательной безопасности,

которым я не мог найти эквивалентов в современных практиках информационной безопасности. Поэтому учебники, раскрывающие тактику, приемы и процедуры секретной войны, оказались поистине уникальным источником информации. В нашем деле кибершпионы и другие злоумышленники не проводят веб-семинары и не публикуют свои тактики в журналах. Это делает трактаты ниндзя еще более ценными и уникальными.

«Кибердзюцу» превращает тактику, приемы и стратегии древних ниндзя в практическое руководство по кибербезопасности. Кибербезопасность — это относительно молодая и поэтому очень активно развивающаяся сфера. Специалисты в этой отрасли старательно обезвреживают надвигающиеся угрозы или прогнозируют будущие атаки, основываясь на знаниях о том, что уже произошло. Я написал эту книгу, потому что считаю: нам есть чему поучиться у ниндзя, проанализировав представленные в их трактатах сведения о том, как в области информационной безопасности противостоять постоянным серьезным угрозам (Advanced Persistent Threat — APT). Тактики информационной войны, практиковавшиеся еще древними ниндзя, совершенствовались на протяжении сотен лет. Их тактики, техники и процедуры работали в те времена, а сегодня могут стать ключом к тому, чтобы пересмотреть современные модели, передовые практики и концепции кибербезопасности и затем реализовать более зрелые и проверенные временем идеи.

Об этой книге

В каждой главе подробно рассматривается одна тема, связанная с ниндзя, от глубокого изучения истории и философии до анализа и рекомендаций по кибербезопасности. Для удобства чтения все главы организованы следующим образом.

- **Трактаты ниндзя** — краткое введение в инструмент, технику или методологию, используемую ниндзя.
- **Кибербезопасность** — анализ того, как описанная ниндзя концепция может быть применена в сфере кибербезопасности.
- **Что можно сделать** — практические шаги, которые вы можете предпринять, исходя из приведенного ранее анализа, чтобы защитить свою организацию от киберпреступлений.
- **Упражнения по теории за́мка** — упражнения, в котором вас просят избавиться от угрозы, используя вновь изученные понятия из области кибербезопасности.
- **Рекомендуемые меры безопасности и предосторожности** — контрольный список рекомендуемых параметров безопасности и спецификации, основанный на стандарте NIST 800-53 [38], которых вы можете добиться в рамках реализации лучших практик.

Эта книга — не справочник по терминологии ниндзя и не энциклопедия по их философии. Если вам нужно именно это, поищите работы Энтони Камминса и Ёсиэ Минами, которые отредактировали и перевели древние японские трактаты ниндзя для современной аудитории. В этой книге также упоминаются следующие книги Камминса и Минами (подробнее о них в разделе «Учебник ниндзя» далее):

- *The Book of Ninja* (ISBN 9781780284934) — перевод трактата «Бансэнсюкай»;
- *The Secret Traditions of the Shinobi* (ISBN 9781583944356) — перевод трактатов «Синоби хидэн» (или «Нинпидэн»), «Гумпо дзиёсю», а также «Ёсимори хяку-сю»;
- *True Path of the Ninja* (ISBN 9784805314395) — перевод трактата «Сёнинки».

Работы Камминса и Минами очень содержательны, и я настоятельно рекомендую вам прочитать их целиком. Эти книги служат не только источником вдохновения, но и первоисточником для анализа ниндзюцу в этой книге, от военной тактики до образа мышления. Их переводы содержат огромную мудрость и знания, выходящие за рамки того, что я мог бы охватить в этой книге, и приоткрывают завесу исчезнувшего ныне образа жизни. Книга «Кибердзюцу» в большом долгу перед Каммисном и Минами, благодаря огромным усилиям которых современный мир смог познакомиться с этими средневековыми произведениями.

Примечание об упражнениях по теории за́мка

По моему мнению, рассмотрение проблем в индустрии кибербезопасности связано как минимум с тремя сложностями. Во-первых, даже в организациях, занимающихся вопросами безопасности, специалисты без технического образования или другие заинтересованные стороны часто не принимают участия в обсуждении вопросов кибербезопасности, им всё не говорят или вовсе подтрунивают над ними из-за недостатка технических знаний. Во-вторых, виновниками многих проблем с безопасностью на самом деле становятся люди. Мы уже знаем, как защититься от многих угроз с технической стороны, но такие вещи, как некорректные политики, невежество, проблемы с бюджетом или другие ограничения, происходят от людей. И в-третьих, наличие готовых решений проблем с безопасностью и/или легкодоступных в интернете ответов изменило подход людей к их решению.

Чтобы рассмотреть те или иные проблемы, в каждой главе я буду выделять основные вопросы в упражнение по теории за́мка — головоломку (которую, надеюсь, вы не сможете нагуглить), в которой вам будет нужно защитить свой за́мок (сеть) от опасностей, исходящих от вражеских ниндзя (субъектов киберугроз). Аналогия проблем с безопасностью и необходимостью защитить за́мок позволяет вынести за скобки технические аспекты рассуждения и более четко разъяснить суть проблемы усилиями команды. Любому читателю будет понятен сценарий, в котором

ниндзя физически проникает в за́мок, независимо от того, знает ли этот человек что-то о сетях и хакерах. Представив себя хозяином за́мка, вы можете игнорировать любую организационную неразбериху или политические проблемы, которые могли бы возникнуть при реализации предложенных вами решений. Ведь короли и королевы делают то, что хотят.

Для будущего использования

В этой книге вы найдете много идей из области кибербезопасности. Некоторые были позаимствованы из оригинальных трактатов и адаптированы для современных информационных приложений. Другие — это решения, предлагаемые для устранения выявленных мною проблем в коммерческих продуктах или услугах. Некоторые идеи более новы или амбициозны. Я не уверен, как их реализации действительно будут работать, но возможно, кто-то другой, лучше понимающий техническую сторону вопроса, сможет разработать их.

Учебник ниндзя

В этом разделе вы получите полное представление о том, что такое «ниндзя», изучив информацию, отраженную в исторических источниках. Постарайтесь забыть все, что вы узнали о ниндзя из фильмов и художественной литературы. Поначалу вы наверняка испытаете некоторое замешательство, недоверие и когнитивный дискомфорт, так как изложенные в трактатах факты будут противоречить давно устоявшимся стереотипам и убеждениям, и особенно это шокирует тех из вас, кто в детстве мечтал стать ниндзя.

Ниндзя в истории

Ниндзя назывались по-разному. Те ниндзя, которых нам демонстрирует западная культура XXI века, — это тоже *ниндзя*, но их называли также *синоби*, *ятой*, *нинпей*, *суппа*, *кандзи*, *раппа* и *укамибито* [7, 8]. Ниндзя известны нам как неуловимые и загадочные воины, но на самом деле здесь все чуть проще: синоби были элитными шпионами и наемными воинами в древней Японии. Набирали их как из крестьян [40], так и из самураев — в качестве примера можно упомянуть Натори Масатаке [7] и Хаттори Хандзо [6]. Ниндзя, вероятно, в той или иной форме существовали по всей Японии, но редко упоминались в исторических записях вплоть до войны Тайра и Минамото XII века [7]. Несколько веков спустя Япония погрязла в распрях и кровопролитии, и в этот период феодалы [40] нанимали синоби для шпионажа, саботажа, убийств и погромов [29]. Даже основополагающий трактат китайского военного стратега V века до н. э. Сунь Цзы «Искусство войны» подчеркивает необходимость использования ниндзя для достижения победы [7].

Ниндзя были чрезвычайно искусны в информационном шпионаже, проникновении во вражеские лагеря и разрушительных атаках. Синоби были, пожалуй, первой серьезной постоянной угрозой в истории (APT0, если угодно). В условиях постоянных конфликтов они непрерывно оттачивали и совершенствовали свои методы, тактики, инструменты, приемы и процедуры, добавляя к практическим навыкам еще и теорию — *ниндзюцу*. В трактате «Бансэнсюкай» говорится: «Важнейший принцип ниндзюцу — избегать мест, где противник внимателен, и наносить удары там, куда он не смотрит» [5]. Таким образом, действуя как тайные агенты, ниндзя тайно передвигались к цели (например, к замку или деревне), собирали информацию, находили бреши в защите цели, проникали внутрь для совершения шпионажа, саботажа, поджога или убийств [40].

Во время продолжительной эпохи Эдо (XVII век) спрос на ремесло синоби сократился, а ниндзя постепенно канули в Лету [40]. Их мастерство перестало быть востребованным, и они занялись другими делами, но их методы были настолько эффективными, что даже сегодня синоби в произведениях искусства предстают как одни из величайших воинов в истории и специалистов по информационной войне. Иногда им даже приписываются невероятные способности вроде невидимости.

Трактаты ниндзя

Знания синоби, скорее всего, передавались от учителя к ученику, сверстниками друг другу, а также через руководства, написанные практикующими синоби до и в течение XVII века. Это и были трактаты ниндзя. Вполне вероятно, что в семьях, произошедших от синоби, есть и другие, пока неизвестные трактаты, в которых могут храниться и иные секреты, но их содержание либо не было проверено историками, либо не обнародовано. Исторические тексты, которые есть у нас, являются ключом к пониманию синоби, а изучение этих источников для извлечения знаний из фактов помогает отделить реальность от мифов, непроверенного фольклора и стереотипов поп-культуры, которые непременно уведут любой разговор о ниндзя не в ту сторону.

Среди наиболее значимых трактатов ниндзя следующие.

- **«Бансэнсюкай»** — энциклопедический 23-томный сборник сведений о навыках, тактике и философии ниндзя, собранный из опыта множества синоби.

  Этот трактат, составленный Фудзибаяси в 1676 году, являет собой попытку сохранить навыки и знания о ниндзюцу для будущих поколений. Кроме того, этот трактат, по сути, — резюме для приема на работу и экзамен на владение навыками, написанный синоби для сёгунов, которым могут понадобиться их услуги в менее мирном будущем.

- **«Синоби хидэн» (или «Нимпидэн»)** — это коллекция трактатов, которые, как считается, были написаны около 1655 года и затем переданы семье Хаттори

Хандзо на хранение до того дня, когда их можно будет опубликовать. Эти трактаты, возможно, наиболее полезны с практической точки зрения и раскрывают техники и инструменты синоби, используемые в реальной работе, включая схемы оружия и спецификации для его создания.

- **«Гумпо дзиёсю» (или Shiyoshu)** — обширный трактат, в котором описываются вопросы военной стратегии, управления, инструментов, философии и использования синоби в военное время. Считается, что он был создан Огасавара Сакуун Кацудзо в 1612 году. Трактат также содержит «Ёсимори хяку-сю» — сборник из 100 стихотворений о ниндзя, призванных научить синоби навыкам и мудрости, необходимым для успеха в их миссиях.
- **«Сёнинки»** — учебное пособие, разработанное в 1681 году Натори Сандзюро Масатакэ, самураем и новатором в военном деле. Эта книга написана для тех, кто уже достиг совершенства в физической и умственной подготовке, но нуждается в освежении знаний и более глубоком понимании руководящих принципов и техник ниндзюцу.

Философия ниндзя

Важно проникнуться ценностями и мировоззрением ниндзя, не углубляясь при этом в мистицизм или спиритизм. Я считаю, что философия ниндзя граничит с ремеслом хакеров с оттенками инь и ян и синто-буддизма. И хотя знакомство с философией ниндзя не обязательно для понимания их тактик и техник, почерпнуть мудрость из этих работ, определенно, было бы полезно.

Сердце под острием клинка (или «словно острие»)

Японское слово *«синоби»* (忍) состоит из иероглифов, обозначающих лезвие (刃) и сердце (心). Интерпретировать его значение можно по-разному.

Один из них — сердце синоби должно быть словно клинок, то есть стальное и острое. Лезвие меча острое и крепкое, но гибкое — это инструмент, предназначенный для убийства людей, одновременно являющийся продолжением духа и воли его владельца. Это согласуется с японской концепцией *кокоро* — соединения сердца, духа и разума в единое целое. В этом контексте изображение дает представление о сбалансированном мышлении, необходимом для того, кто желает стать ниндзя.

Другое толкование — «сердце под лезвием». В этом прочтении клинок представляет собой экзистенциальную угрозу. Это не только физическая угроза, из-за которой синоби рискует жизнью, но и оружие, которое надежно охраняет бьющееся сердце. В прочтении *оньёми* (китайский) 忍 означает «упорствовать», что подчеркивает внутреннюю силу, необходимую для работы в качестве шпиона

на вражеской территории под постоянной угрозой. Синоби должны были выполнять опасные задания, а это иногда означало необходимость находиться в тылу врага в течение длительного времени в ожидании удачного момента, то есть рисковать жизнью.

Правильный ум

«Бансэнсюкай» гласит, что синоби должен обладать «правильным умом», иначе он обречен на поражение. Достижение этого редкого состояния означает постоянную концентрацию, сосредоточенность и осознание своей цели — это внимательность, которая превращается в щит.

Ожидается, что синоби должен принимать решения, будучи «доброжелательным, праведным, лояльным и верным» [5], даже если его ремесло — это заговоры и обман. Эта философия наделяла синоби сосредоточенностью и спокойствием в моменты сильного напряжения, например в бою или во время тайной операции. «Достигнув внутреннего покоя, — сообщает “Сёнинки”, — вы можете постичь то, чего не осознают другие» [7].

«Правильный ум», как считалось, делает синоби более динамичными стратегами. Когда другие воины безрассудно бросались в бой, острота ума синоби позволяла им сохранять спокойствие и действовать по обстоятельствам. Их учили мыслить нестандартно, все подвергать сомнению. Историк Энтони Камминс сравнивает такое мышление с мышлением современных акул бизнеса. Если их оружие выходило из строя, они использовали слова. Если и речь не давала результата, они переставали мыслить со своей позиции и пытались постичь мысли врага [7]. Правильный ум позволял понять врага и внешние обстоятельства и совершить, казалось бы, невозможное.

В «Сёнинки» об этом говорится кратко: «Нет ничего удивительнее человеческого ума» [7].

Техника ниндзя

Методы проникновения, подробно описанные в трактатах ниндзя, иллюстрируют поразительную эффективность процессов сбора информации, используемых синоби. Они практиковали два основных способа проникновения: *ин-нин* (темное ниндзюцу), или умение спрятаться где-нибудь под покровом темноты или иным образом избежать обнаружения, и *ё-нин* (светлое ниндзюцу) — проникновение у всех на виду, например замаскировавшись под монаха, чтобы избежать подозрений. Иногда синоби применяли оба метода сразу. Например, они могли проникнуть в город замаскированными, а затем ускользнуть от любопытных глаз и спрятаться во рву замка до момента нападения.

Каким бы ни было время суток, синоби отправлялся на задание, зная все возможное о цели, и использовал проверенные временем методы для сбора максимально подробной информации. Синоби изучали рельеф местности, где находилась их цель, обычаи, отношения, интересы и привычки ее жителей. Прежде чем пытаться проникнуть в замок, они проводили разведку, чтобы определить размер, расположение и назначение каждой комнаты, искали места проникновения, определяли, кто там живет и каков распорядок дня (включая даже график кормления домашних животных). Они запоминали имена, звания и должностные обязанности охранников неприятеля, а затем использовали вражеские флаги, эмблемы и униформу, чтобы открыто проникнуть внутрь (*ё-нин*) буквально рядом со своими ничего не подозревающими целями. Они собирали печати разных лордов, чтобы можно было подделывать их и с их помощью отдавать ложные приказы вражеской армии. Перед тем как вступить в бой, они исследовали размер, силу и возможности армии противника, а также пути ее снабжения, воинские приемы и боевой дух солдат. Если их целью был правитель, они стремились изучить его моральный кодекс и тайные страсти, которые могли помочь погубить его [5].

Синоби учили мыслить творчески с помощью философии «правильного ума». Обучение позволяло им больше узнать об окружающем мире и порождало новые способы действий в полевых условиях. Например, «Сёнинки» учит синоби развивать свои навыки, наблюдая за поведением животных в природе. Если он подходил к вражескому посту, то начинал думать как лиса или волк, то есть не проходил через заграждение, а проявлял терпение и огибал его, даже если приходилось идти много миль. В других случаях было уместно вести себя «как скот или лошадь» [5] на открытом пространстве, возможно, изображая посланника или эмиссара, чтобы приблизиться к врагу, который на человека низшего класса не обратил бы внимания. Независимо от того, как синоби чувствовали себя — даже если они были раскалены добела от гнева, — они выглядели безмятежно, «словно лебеди на водяной глади» [7]. Если им нужно было отвлечь охранника, стоящего на посту, они могли лаять или выть по-собачьи или трясти кимоно, имитируя звук отряхивающейся собаки [7].

Синоби привнесли в военное искусство новшества, которые военные и оперативники практикуют и по сей день, добиваясь успехов, так как именно разведка синоби и безупречное знание целей становились их оружием.

1

Карты сетей

Имея на руках карту, генерал может составить план защиты или атаки замка.

Выбирая время и день перемещения лагеря, необходимо соблюдать ряд принципов. Синоби обязан точно знать географию местности и расстояние до врага.

«Ёсимори хяку-сю», № 9

Раздобыв план замка или лагеря, необходимо как можно скорее вернуться, и именно так должен поступить хороший синоби.

«Ёсимори хяку-сю», № 24

Первый совет, который дается в «Руководстве для командиров» («Бансэнсюкай»), призывает создавать очень точные карты, которые военачальники могли бы использовать для планирования атак против врага [5]. «Ёсимори хяку-сю» в стихах № 6–10 и 24 также подчеркивает важность достаточной детализации карт, чтобы они были полезны и солдатам, и синоби.

Создавать карты командиры обычно поручали синоби. Из трактатов явно следует, что умение точно рисовать видимые объекты — горы, реки, поля — это не то же самое, что рисовать специальные подробные карты разведки объекта атаки, пригодные для целей военной стратегии или проникновения синоби. В трактатах говорится, какие детали важны для ведения войны и ремесла синоби и, следовательно, должны фигурировать на карте [5].

- **Все входы и ворота дома, замка или форта.** Какие используются замки́, защелки и механизмы открывания? Насколько сложно открыть ворота или двери, издают ли они шум при открытии или закрытии?

- **Подъездные дороги.** Прямые они или изогнутые? Широкие или узкие? Вымощены ли камнем? Ровные или под уклоном?
- **Внешний вид, схема и планировка здания.** Каковы размер и назначение каждой комнаты? Что хранится в каждой комнате? Скрипят ли в них половицы?
- **Обитатели строения.** Как зовут жителей? Практикуют ли они какие-нибудь примечательные виды искусства, имеют ли какие-либо навыки? Насколько осторожен или подозрителен каждый из жителей?
- **Топология замка и окрестностей.** Будет ли видно сигнал изнутри и снаружи помещения? Где хранятся еда, вода и дрова? Насколько широки и глубоки рвы? Насколько высоки стены?

Понятие о картах сети

Картами сети в кибербезопасности называют графы топологии сети, которые описывают физические и/или логические связи и конфигурацию *связей* (коммуникационные соединения) и *узлов* (устройств) сети. Чтобы лучше понять концепцию, посмотрите на дорожные карты или карты в атласе. Они описывают физическое местоположение, географические особенности, политические границы и природный ландшафт. Информация о дорогах (связях) — их название, ориентация, длина и пересечения с другими дорогами — может использоваться для прокладки маршрута между местами (узлами). Теперь рассмотрим следующий гипотетический сценарий.

Представьте, что вы живете в мире, где дороги и здания внезапно появляются или исчезают в мгновение ока. У вас есть GPS и координаты места, где вы находитесь и куда хотите пойти, но добраться туда можно лишь по запутанной сети постоянно меняющихся дорог.

К счастью, на каждом перекрестке есть специалисты по навигации (*маршрутизаторы*), помогающие путешественникам вроде вас найти путь. Эти маршрутизаторы постоянно обращаются к соседним маршрутизаторам и спрашивают у них, какие маршруты и местоположения открыты, чтобы обновить свою таблицу маршрутизации, хранящуюся в буфере обмена. Вам нужно останавливаться на каждом перекрестке и спрашивать у маршрутизатора, как проехать к следующему узлу, показывая проездной, на котором ваш предполагаемый пункт назначения закодирован в координатах GPS. Маршрутизатор проверяет свой буфер обмена на наличие открытых в данный момент маршрутов, делает определенные вычисления и указывает вам направление, записывая на вашем проездном адрес маршрутизатора, а также пробивает в нем отверстие, чтобы отследить количество маршрутизаторов, на которых вы отметились во время поездки, и отправляет вас

к следующему маршрутизатору. Этот процесс повторяется, пока вы не достигнете точки назначения. А теперь представьте себе лица картографов, которые, вероятно, бросили бы заниматься созданием карт, будучи не в состоянии уследить за постоянно меняющейся сетью. Составителям карт пришлось бы довольствоваться обозначением ключевых ориентиров и достопримечательностей, общими названиями и нечеткими линиями между этими точками, говорящими о том, что между ними существуют какие-то пути.

Эта гипотетическая для нашего мира ситуация на самом деле существует в киберпространстве, и именно поэтому сетевые карты не так точны, а их обслуживание не так приоритетно, каким должно было бы быть. Отсутствие качественной карты сети — это распространенная проблема организаций, занимающихся кибербезопасностью. Если у организации есть карта, она обычно предоставляется операционному центру безопасности (security operations center, SOC), чтобы его специалисты знали, где в потоке данных находятся датчики или устройства безопасности, и могли лучше понять маршрут пакетов, правила брандмауэра, сигналы тревоги и системные журналы. Кроме того, такая карта, скорее всего, довольно абстрактна и описывает только основные функции, такие как границы интернета, периметр сети и интрасети, общее расположение граничных маршрутизаторов или межсетевых экранов, но на ней не указываются сети, концептуальные схемы имеют вид простых кружочков и стрелочек. Пример плохо проработанного, но распространенного вида карты сети, которой пользуются специалисты в области кибербезопасности и ИТ, представлен на рис. 1.1.

Чтобы понять, почему на рис. 1.1 показана «плохая» карта, давайте еще раз рассмотрим приведенный в «Бансэнсюкай» совет по составлению карт, но применим кибераналогию.

- **Все точки доступа узла в сети.** Какие виды интерфейсов доступа присутствуют на устройстве (Ethernet [e], Fast-Ethernet [fe], Gigabit-Ethernet [ge], Universal Serial Bus [USB], Console [con], Loop-back [lo], Wi-Fi [w] и т. д.)? Есть ли фильтрация адресов управления доступом к сети (NAC) или управления доступом к среде (MAC)? Включен или заблокирован доступ к удаленной или локальной консоли? Какой вид физической безопасности реализован? Закрыто ли помещение с серверной стойкой на замóк или есть ли хотя бы USB-замки́? Ведется ли журнал доступа к интерфейсу? Где находится интерфейс управления сетью и сама сеть? Каков IP-адрес и MAC-адрес каждой точки доступа?
- **Граничные шлюзы, переходы и точки выхода.** Сколько интернет-провайдеров (internet service provider, ISP) у сервера — один или больше? Используется надежное подключение к интернету (Trusted Internet Connection, TIC) или управляемая служба интернета (Managed Internet Service, MIS)? Какова пропускная способность интернет-соединения? Применяется оптоволокно,

Ethernet, коаксиальный кабель или другой канал? Какие переходы ведут к сети? Существуют ли способы входа в сеть или выхода из нее через спутник, микроволновую печь, лазер или вайфай?

- **Структура и схема сети.** Каковы имя, назначение и размер каждой подсети, например используется ли бесклассовая междоменная маршрутизация (Classless Inter-Domain routing, CIDR)? Задействуются ли виртуальные локальные сети (virtual local area networks, VLAN)? Заданы ли лимиты пула подключений? Является ли сеть плоской, иерархической или разделена на структуры, защитные слои и/или функции?

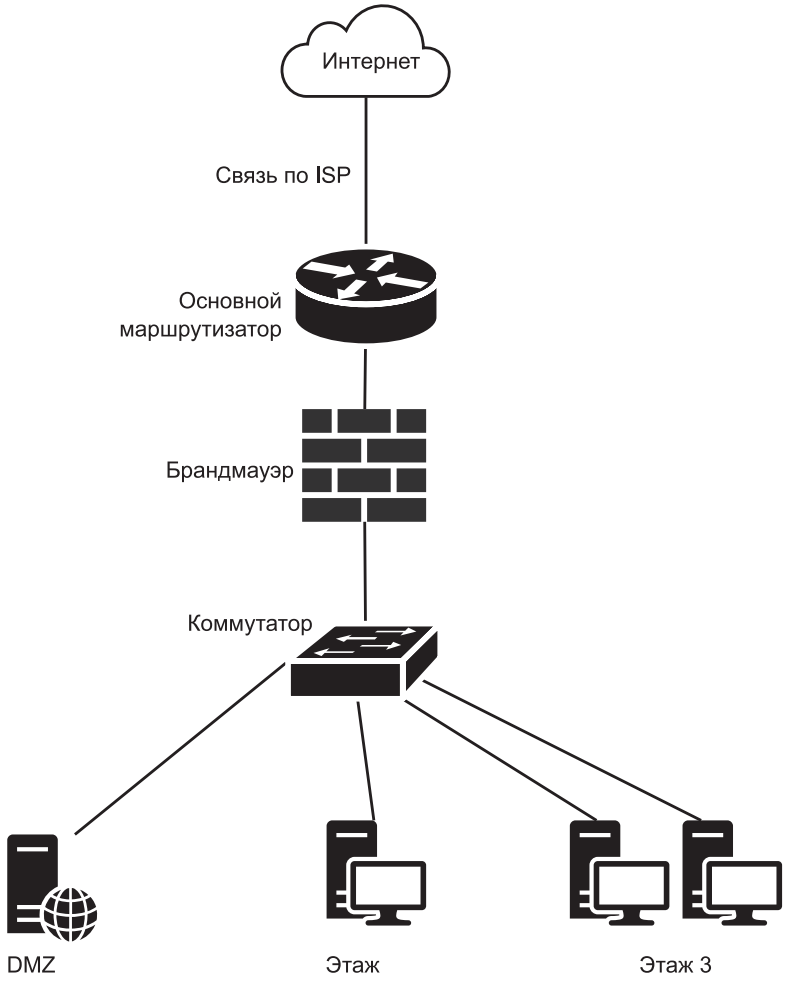

Рис. 1.1. Упрощенная карта сети

- **Хосты и узлы сети.** Как они называются? Какая у них версия операционной системы (ОС)? Какие службы/порты используются, какие из них открыты? Какие на них запущены средства безопасности, которые позволят обнаружить атаку? Есть ли у них общеизвестные уязвимости (common vulnerability exploit, CVE)?
- **Физическая и логическая архитектура сети и здания. Где находится датацентр?** Есть ли в холле разъемы Ethernet? Можно ли поймать вайфай за пределами здания? Видны ли экраны компьютеров и терминалы снаружи здания? Используется ли в офисе безопасное стекло? Правильно ли сегментированы сети гостевых или конференц-залов? Каковы основные списки управления доступом (access control list, ACL) и правила брандмауэра в этой сети? Где разрешается DNS? Что доступно в периметре сети или DMZ (demilitarized zone)? Существуют ли внешние поставщики электронной почты или другие облачные сервисы? Как устроена архитектура удаленного доступа или виртуальной частной сети (VPN)?

Организации, не имеющие действующей карты сети, иногда используют электрические схемы или схемы, составленные их ИТ-отделом. На таких упрощенных рисунках отражено относительное расположение систем, сетевого оборудования и подключения устройств, и они могут служить справочными материалами для устранения технических или эксплуатационных проблем в сети. Но у множества организаций нет даже таких приблизительных схем, зато есть электронные таблицы, в которых перечислены имена хостов, их модели и серийные номера, IP-адреса, а также расположение всего оборудования на стойке в центре обработки данных. При этом если заинтересованные стороны могут использовать такую таблицу для поиска нужных ответов и серьезных сетевых проблем или сбоев не возникает, то даже само наличие такой документации может препятствовать созданию карты сети. Это ужасно, но у некоторых компаний есть архитектор или специалист, который держит карту сети в голове, и ни в каком другом виде ее не существует.

Справедливости ради стоит сказать, что бывают и разумные причины отсутствия полезных сетевых карт. Создание, совместное использование и обслуживание карт отнимает драгоценное время и другие ресурсы. Карты могут часто меняться. Добавление систем в сеть или их удаление, изменение IP-адресов, переделка кабелей или задание новых правил маршрутизатора или брандмауэра — все это может значительно повлиять на точность карты, даже если изменение произошло всего несколько минут назад. Кроме того, современные компьютеры и сетевые устройства используют протоколы динамической маршрутизации и конфигурации хоста, которые автоматически отправляют информацию в другие системы

и сети, не нуждаясь в картах вообще, что означает: сети могут автоматически настраиваться сами.

Разумеется, существует множество программных инструментов для создания карт, например программа Nmap [24], которая сканирует сеть, определяя в ней хосты, визуализирует сеть по количеству переходов от сканера, использует простой протокол управления сетью (Simple Network Management Protocol, SNMP) для обнаружения и отображения топологии сети или задействует файлы конфигурации маршрутизатора и коммутатора для быстрого создания сетевых диаграмм. Сетевые диаграммы, генерируемые программами, удобны, но они редко отражают все подробности и в целом контекст, необходимый для создания по-настоящему качественной карты, которую хотел бы иметь под рукой защитник. Идеальным решением было бы одновременное использование программ для картографии, сетевого сканирования и человеческого опыта, но даже этот подход требует значительных затрат времени сотрудника со специальными навыками, иначе полученные карты не будут достаточно точными или полезными.

Несмотря на эти ограничивающие факторы, чрезвычайно важно, чтобы защитник сети при составлении карты был очень внимателен. Примерная карта, показанная на рис. 1.2, иллюстрирует детали, которые должны быть указаны на составляемой защитником карте сети.

Для представления устройств в сети используют геометрические фигуры, а не пиктограммы. Для схожих типов устройств применяют схожие фигуры. Например, круги на рис. 1.2 обозначают рабочие станции, квадраты — маршрутизаторы, а прямоугольники — серверы. В продолжение этой мысли, треугольники, если бы они были, представляли бы ретрансляторы электронной почты или контроллеры домена. Кроме того, на фигурах отсутствует текстура или фон, потому что информация, размещенная внутри, должна быть хорошо читаемой.

Каждый интерфейс, как виртуальный, так и физический, имеет свой тип и номер. Например, может быть указан тип интерфейса Ethernet, а номер интерфейса будет таким же, как и физически указанный на устройстве, eth 0/0. Также помечаются неиспользуемые интерфейсы. Каждому интерфейсу приписывается назначенный ему IP-адрес и подсеть, если они известны.

Открытая информация об устройстве: имя хоста, марка, модель устройства и версия ОС — указывается в верхней части устройства. Уязвимости, учетные данные по умолчанию, известные учетные данные и другие важные слабости обозначаются в центре устройства. Аналогичным образом документируются запущенные службы, программное обеспечение и открытые порты. На карте также указываются сети VLAN, сетевые границы, макет и структура сети. Рядом с ними записывается любая заслуживающая внимания информация.

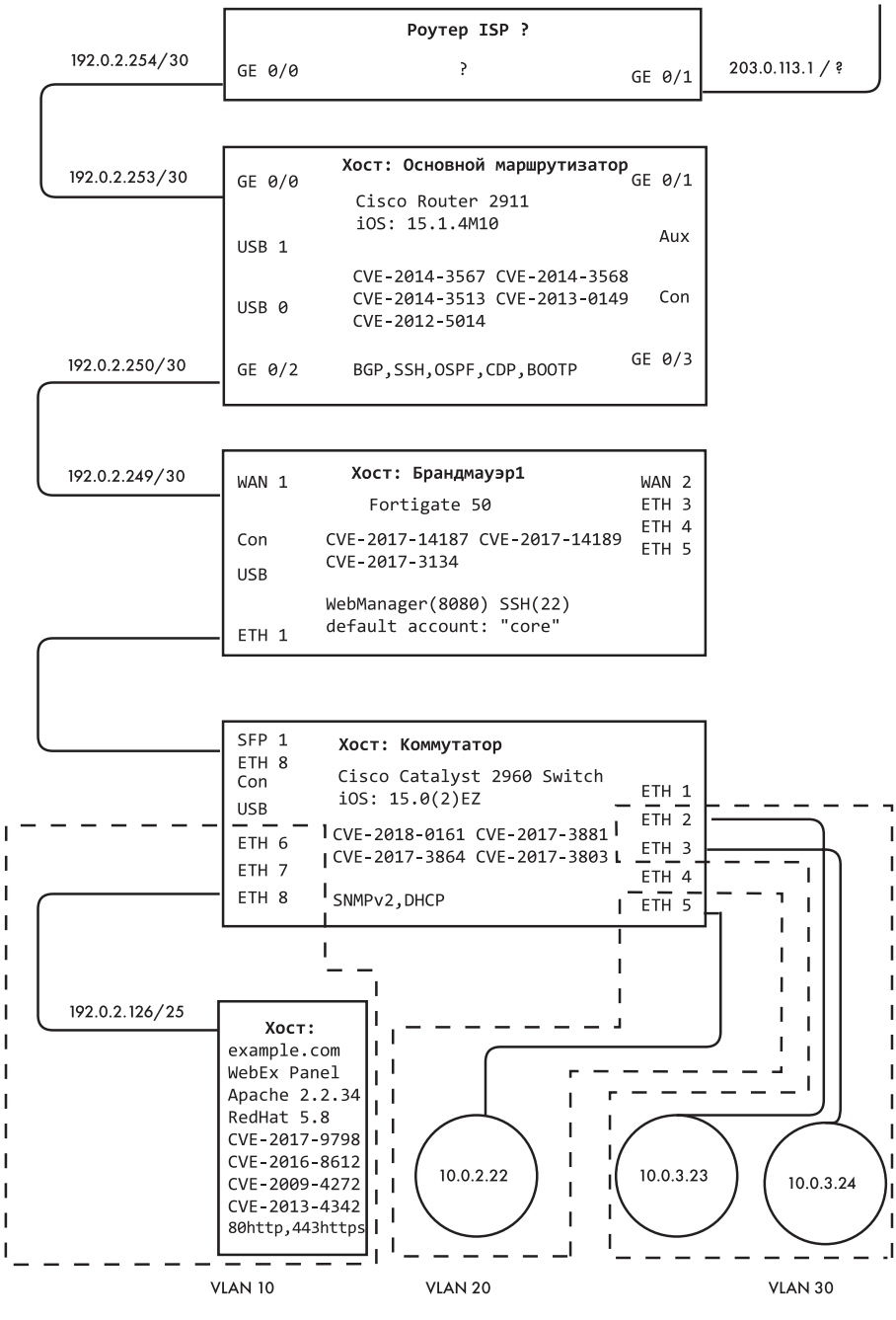

Рис. 1.2. Подробная карта сети

Тайный сбор информации

Высшим пилотажем у синоби считалось умение собрать разведданные, не обнаружив себя. Если он будет прогуливаться возле за́мка и замерять длинной линейкой его размеры, то жители наверняка заподозрят, что тут работает вражеский шпион. Следовательно, старательные синоби составляли карты в мирное время, когда обитатели замка были менее бдительны и можно было более свободно ходить там, где нужно, вызывая во время сбора данных меньше подозрений [5].

Часто синоби приходилось придумывать способы выполнять измерения, отмечать топографические особенности и собирать другую информацию втайне от посторонних глаз. Что характерно, в разделе о методах открытой маскировки трактата «Бансэнсюкай» приведено описание того, как точно создавать карты, и там говорится, что синоби умели создавать карты прямо на глазах у врага. В трактате описывается техника под названием *урамитцу но дзюцу* [5], предназначенная для определения расстояния до знакомого объекта, если известны размеры объекта для масштабирования. *Урамитцу но дзюцу* также рассматривает хитрые приемы из тригонометрии. Например, синоби может лечь ступнями к цели и использовать их известные размеры для измерения расстояния, при этом со стороны кажется, что человек просто дремлет под деревом.

Сбор информации о сетевых узлах — одно из первых действий, которое выполняет злоумышленник перед совершением атаки на сеть или хост. Карты, созданные противником, предназначены для того же, что и карты ниндзя, — идентификации и документирования информации, необходимой для проникновения на объект. К этой информации могут относиться все точки входа в сеть и выхода из нее: подключения к интернет-провайдеру, точки беспроводного доступа, УВЧ, микроволновые, радио- или спутниковые точки, облачные, взаимосвязанные и внешние сети.

Злоумышленники также находят шлюзы протокола пограничного шлюза (BGP) и маршруты или переходы к сети. Определяют репрезентативную структуру, расположение и дизайн сети, оборудование в ней, включая имена хостов, модели устройств, операционные системы, открытые порты, запущенные службы и уязвимости, а также топологию сети, включая подсети, VLAN, ACL и правила брандмауэра.

Многие из инструментов, предназначенные для отображения сети и используемые злоумышленниками, являются «шумными», поскольку они обмениваются данными с большим количеством хостов, применяют специально собранные пакеты и могут быть обнаружены внутренними устройствами безопасности. Но злоумышленники могут обойти этот недостаток за счет замедления или настройки картографа, использования нестандартных (неподозрительных) пакетов и даже ручной разведки с помощью стандартных инструментов, работающих на хосте жертвы, таких как

команды `ping` или `net`. В атаках также могут задействоваться безобидные методы разведки, когда злоумышленник не трогает и не сканирует цель, а лишь собирает информацию с помощью сервиса Shodan или других ранее проиндексированных данных, хранящихся в поисковых системах в интернете.

Более хитроумные злоумышленники пользуются тактикой *пассивного отображения сети*, когда злоумышленник собирает информацию о цели, не взаимодействуя с ней напрямую (без активного сканирования с помощью инструментов вроде Nmap). Еще одна тактика пассивного отображения сети — это интерпретация пакетов, перехваченных с сетевого интерфейса в *беспорядочном режиме*, то есть настройка сетевого интерфейса на запись и проверку всех сетевых коммуникаций. Этот режим противоположен *упорядоченному режиму*, при котором записывается и проверяется только связь внутри сети. Беспорядочный режим позволяет получить представление об используемых сетью соседних хостах, потоках трафика, службах и протоколах, не взаимодействуя с ними активно.

Методами отображения сети без прямого взаимодействия с ней являются также перехват электронных писем администратора сети на выходе из нее, поиск сетевых карт цели во внешнем хранилище файлов или поиск на форумах, где администратор просит помощи в устранении неполадок, для чего может публиковать журналы или ошибки, конфигурации маршрутизатора, информацию о сетевой отладке или другие технические подробности, позволяющие понять структуру и конфигурацию сети. Как и в *урамитцу но дзюцу*, использование наблюдаемой информации из сети цели позволяет составить карту, не обращаясь к сети. Пассивное отображение может включать в себя измерение задержки трассировщиков для определения спутниковых переходов (например, наличие спутника обычно сопровождается внезапным увеличением задержки связи на 500 мс) или обнаружения глубокой обработки пакетов системой брандмауэра (например, препроцессор распознает потенциальную злонамеренную атаку и добавляет ощутимые задержки связи). Пассивное отображение может включать также раскрытие информации внутренней сети из внешних зон DNS и записей ответов. Это могут быть заказы на государственные закупки и запросы на закупку определенного программного либо аппаратного обеспечения, объявления о вакансиях сетевых или системных администраторов с опытом работы в конкретной технологии, сетевом оборудовании или аппаратном/программном обеспечении.

Если злоумышленник тратит так много времени на разработку карт, они в конечном итоге могут оказаться более полными, чем собственные карты цели, и тогда противник будет знать о сети цели больше, чем сама цель. Чтобы не отставать в этой битве, защитники сети должны разрабатывать и поддерживать лучшие карты и обеспечивать высокую степень защиты.

Создание карты

Создание карты может состоять из трех основных этапов.

1. Выделите средства для создания полной и точной карты, которую было бы легко обновлять и надежно хранить. Карта должна содержать информацию, необходимую для нужд определенного отдела, например отдела ИТ, центра сетевых операций (network operations center, NOC) и SOC. Рассмотрите возможность найма специального человека, команды или подрядчика, который бы составил и проанализировал такую карту.
2. Создайте саму карту, указав на ней все подробности, перечисленные в начале этой главы.
3. Попросите коллег проверить эту карту в рамках процесса управления изменениями и делайте это всякий раз, когда кто-либо замечает расхождение карты с действительностью.

Давайте подробнее рассмотрим второй шаг — создание карты.

Когда вы определили все ключевые заинтересованные стороны и убедили их в том, что этот проект совершенно необходим, первый шаг — собрать все, что есть в вашей организации, что может помочь создать его. Сюда входят схемы подключения, планы проектов старой сетевой архитектуры, результаты сканирования уязвимостей, инвентаризации активов и центра обработки данных, данные об аренде DHCP, записи DNS, сведения об управлении сетью SNMP, записи агентов конечных точек, данные о захвате пакетов (packet captures, PCAP), журналы SIEM (security information and event management), настройки маршрутизаторов, правила брандмауэра и результаты сканирования сети. Настройка маршрутизатора лежит в основе построения базовой архитектуры и компоновки вашей сетевой карты. К примеру, можете начать с размещения вашего ядра или центрального маршрутизатора(ов) в середине карты и затем рисовать ответвления от него. Перехват PCAP поможет выявить в сети конечные точки, которые могут не отвечать на сканирование сети или вообще быть недоступными для сканеров из-за сетевой фильтрации. Разрешив выбранным системам собирать PCAP в течение длительного периода в беспорядочном режиме, вы получите список конечных точек, как показано на рис. 1.3.

В идеале собирать PCAP нужно во время сканирования сети, чтобы проверить, куда дотягивается сканер. Кроме того, следует провести несколько сканирований сети, при этом минимум одна конечная точка в каждой подсети должна сканировать свою подсеть. Эти сканирования можно вручную объединить в топологию карты сети, как показано на рис. 1.4. Определите элементы, которые можно автоматизировать, чтобы этот процесс было легче повторить в будущем.

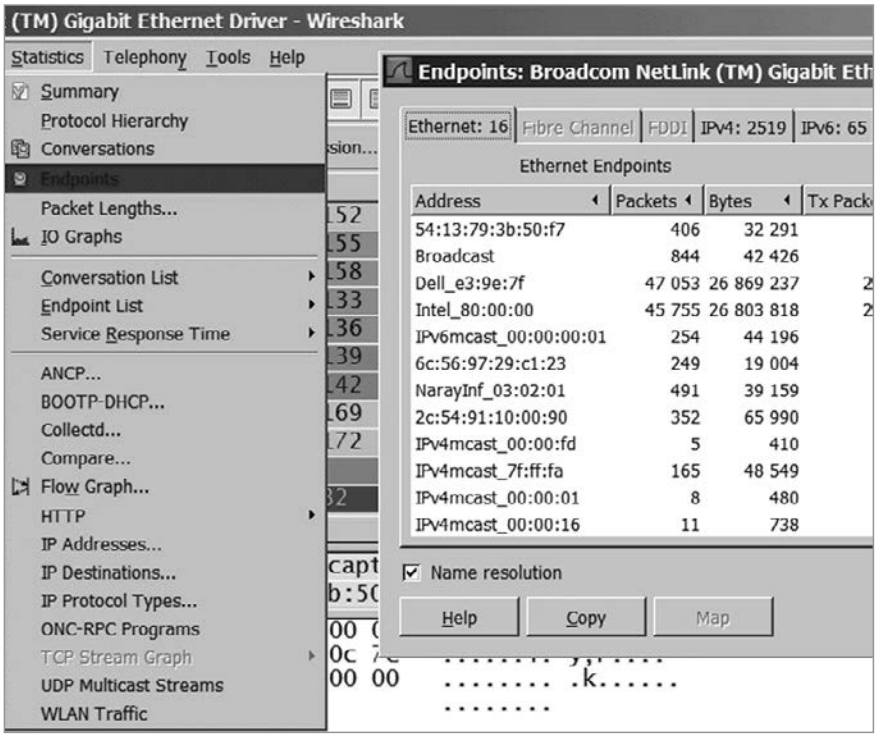

Рис. 1.3. Скриншот Wireshark со списком конечных точек, обнаруженных во время сбора PCAP

Собранные данные нужно обработать, проанализировать и объединить. Перед объединением данных полезно выяснить, какой источник данных наиболее точен, а также определить источники, предоставляющие уникальную и полезную информацию, например время последнего посещения устройства. Также следует проанализировать все найденные несоответствия. Это могут быть устройства, которых на самом деле нет в сети, несанкционированные устройства, странное сетевое поведение или соединения. Если вы обнаружите, что ваши сетевые сканеры не смогли проникнуть в какие-то части подсети из-за правил IP-адресов или работы системы предотвращения вторжений (intrusion prevention system, IPS), рассмотрите возможность изменения настроек, чтобы можно было выполнить более глубокое и всестороннее сканирование.

Рассмотрите различные инструменты для составления карт сети, которые могут автоматически принимать данные SNMP, сканировать сеть и уязвимости, а также позволяют выполнять ручное редактирование и добавление данных. Выбранный вами инструмент должен создавать исчерпывающую, точную и подробную карту

сети, отвечающую потребностям заинтересованных сторон. Выберите лучшее решение, которое будет обрабатывать ваши данные и соответствовать вашему бюджету.

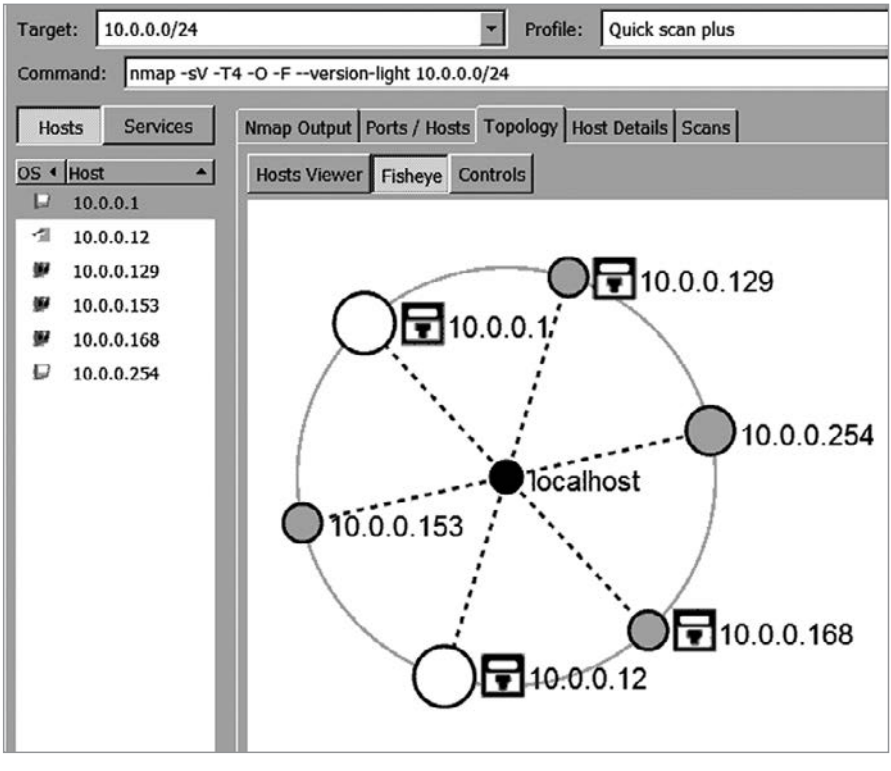

Рис. 1.4. Топология подсети 10.0.0.0/24 по результатам сканирования в Zenmap

Создайте карту и протестируйте ее. Проверьте ее полезность во время совещаний либо инцидентов в сфере безопасности и сбоев/отладки сети. Помогает ли карта решать проблемы и быстрее находить их источник? Проверьте точность карты с помощью трассировки маршрута и выполнения tcpdump через интерфейсы. Чтобы проверить точность с помощью трассировки, нужно провести ее изнутри и снаружи из разных сетевых местоположений и посмотреть, указаны ли на карте точки перехода (маршрутизаторы) и соответствуют ли они структуре сети. Пример трассировки маршрута показан на рис. 1.5.

Посмотрите, насколько полезна будет ваша карта для красной и синей команд. Соберите отзывы, повторите процесс составления и получите карту лучшего качества за меньшее время.

```
C:\Users\benm>tracert -4 example.com

Tracing route to example.com [93.184.216.34]
over a maximum of 30 hops:

  1     2 ms     1 ms     1 ms  10.0.0.1
  2    18 ms    10 ms     9 ms  96.120.106.61
  3     9 ms    10 ms     9 ms  xe-5-2-0-sur01.newmexiconw.dc.bad.comcast.net [162.151.98.145]
  4    18 ms    10 ms    11 ms  ge-1-21-ur02.waldorf.md.bad.comcast.net [68.87.135.97]
  5    41 ms    11 ms    10 ms  ae-13-ar01.capitolhghts.md.bad.comcast.net [68.87.168.61]
  6    13 ms    14 ms    14 ms  be-33657-cr02.ashburn.va.ibone.comcast.net [68.86.90.57]
  7    11 ms    12 ms    12 ms  be-10142-pe01.ashburn.va.ibone.comcast.net [68.86.86.34]
  8    12 ms    12 ms    12 ms  as27471-2-c.350ecermak.il.ibone.comcast.net [173.167.57.50]
  9    11 ms    11 ms    13 ms  152.195.64.133
 10    11 ms    10 ms    11 ms  93.184.216.34

Trace complete.

C:\Users\benm>
```

Рис. 1.5. Трассировка в Windows адреса example.com

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Рассмотрим сценарий, в котором вы — правитель средневекового замка, у вас есть ценная информация, сокровища и люди. Вам стало известно, что ниндзя тщательно нанесли на карту ваш замок и его окрестности, но при этом неясно, выбрали вас в качестве цели или это просто пассивная разведка. Вы не знаете, как выглядит карта и насколько она детализирована. У вас же есть лишь архитектурный план замка, который использовался во время его возведения и был разработан для строителей, а не для других пользователей, к тому же с тех пор устарел.

Что может быть отражено на карте ниндзя, чего нет на вашей карте? Что ниндзя знает о вашем замке, чего не знаете вы, и как эту информацию можно применить для проникновения в него? Кому в замке был бы полезен доступ к карте ниндзя? Кому вы доверили бы нанести на карту свой замок так же, как это делали ниндзя, чтобы увидеть то, что увидели они?

Рекомендуемые меры безопасности и предосторожности

Все рекомендации, если это возможно, здесь и далее сопровождаются мерами безопасности из стандарта NIST 800-53.

1. Распределите обязанности по документированию карты сети. Внедрите политики и процедуры для координации обновлений карты между командами.

(Разделы CM-1. Политика и процедуры управления конфигурацией; CM-3. Контроль изменений конфигурации | (4) Представитель службы безопасности; CM-9. План управления конфигурацией.)

2. Чтобы было с чего начать, документируйте конфигурацию топологии сети, архитектуры, логическое размещение и информационные системы. (CM-2. Базовая конфигурация.)
3. Добавьте идентификацию дефектов, например неточностей карты, и процедуру устранения, допустим, уязвимостей, сетевой архитектуры, в процесс составления карты. (SI-2. Устранение дефектов.)

Резюме

В этой главе мы рассмотрели цели создания карт синоби, стандарты этого процесса и методы картографирования, а также привели обзор современных практик и технологий картографирования сетей. Беседы о важности сетевых карт, о том, как создавать хорошие карты и как злоумышленники собирают информацию о вашей системе, возможно, подогрели ваше воображение и вы хотите найти больше источников данных или методов, которые можно было бы использовать для построения карты своей и любой другой сети.

В следующей главе мы попробуем задействовать карту сети в качестве диаграммы потока данных (data flow diagram, DFD) для моделирования угроз. Это означает, что вы определите в своей сети области, в которых злоумышленник может провести атаку или обойти защиту. Я расскажу о новой защитной технике ниндзя, которую можно использовать для защиты слабых мест в вашей сети.

2

Особое внимание к защите

Даже замки с самыми мощными укреплениями следует охранять, уделяя особое внимание темным переулкам.

Пробираясь в замок или лагерь, синоби должен
держать в уме естественно укрепленные
и труднопреодолимые направления,
деревья и слепые зоны.
«Ёсимори хяку-сю», № 10

Синоби всегда были опытными лазутчиками. Древние трактаты описывают, как быстро идентифицировать и использовать слабые места в укреплениях противника. В них также подчеркивается, что во время организации собственной защиты синоби должны широко мыслить и творчески применять свои знания. «Бансэнсюкай» советует командирам, которым поручено защищать лагерь или замок, с особым вниманием относиться к тем местам, через которые синоби, скорее всего, попытается проникнуть, — это углы каменных стен замка, места вывоза мусора, канализация, а также деревья или кусты [5].

Понятие вектора атаки

Представим, что стена замка — это *плоскость атаки*, а слабые места в стене, например канализация или выпирающие камни, по которым можно забраться на стену, — это *векторы атаки*. Термин *«плоскость атаки»* обозначает любое программное обеспечение, сеть или систему, которую злоумышленник может захотеть атаковать. Любая точка на плоскости атаки может быть вектором атаки или средством, которое злоумышленник использует для получения доступа. В кибербезопасности всегда рекомендуется уменьшать плоскость атаки. Но хотя сокращение площади

замка уменьшает пространство, которое необходимо защищать, оно не позволяет уменьшить ущерб, который может нанести противник, равно как и запретить ему применять тот или иной вектор атаки. А вот уменьшение плоскости атаки вполне может облегчить защиту цели.

В томе «Бансэнсюкай» о скрытом проникновении описываются техники защиты, оружие и способы мышления, которые несут угрозу защищаемому месту. Трактат призывает командиров думать о том, как любой элемент окружения можно использовать против них. Например, он предписывает злоумышленникам искать вокруг замка *синоби-гаэси* — специальные шипы, которые разбрасывают вокруг лагеря, чтобы затруднить нападение [5]. Когда защитники размещали шипы в местах, которые считали уязвимыми, само их наличие подсказывало вражеским синоби, что именно тут в замок проникнуть легче. Фактически защитники сами выдают свои опасения. Синоби мог довольно легко избавиться от шипов и проложить путь через самое слабое место в периметре цели [5].

Небольшой пример меры безопасности, которая была «прикручена» с запозданием, можно найти в Microsoft Windows PowerShell. Многие функции безопасности, добавляемые в платформу .NET с каждой новой версией PowerShell, не устранили основные недостатки продукта и, по сути, позволили злоумышленникам создать арсенал инструментов, которые можно использовать для проникновения в системы, поддерживающие PowerShell. Это отличный пример для любого исследователя безопасности, желающего изучить технику *синоби-гаэси*.

Древние замки, все еще стоящие в Японии, обычно не защищены шипами, но зато водопроводные трубы в них слишком малы для человека, периметры очищены от растительности и на внешних стенах нет утопленных углов. Все это свидетельствует о том, что правители, следуя указаниям синоби, сознательно устранили все уязвимости. В идеале стоило бы устранить вообще все слабые места, но это не всегда возможно.

В этой главе мы обсудим концепцию охраны и ее предполагаемое место среди пяти функций кибербезопасности. Затем поговорим о том, как определить уязвимые места, требующие защиты, с помощью моделирования угроз.

Концепция охраны

Охрана — это защитный контроль над активами путем наблюдения за окружающей средой, обнаружения угроз и принятия превентивных мер. Предположим, хозяин замка считает довольно большую водосточную трубу в его стене слабым местом. Убирать трубу нельзя, так как она необходима для отвода воды, но рядом должен стоять охранник, не позволяющий злоумышленникам использовать ее для проникновения.

Как правило, организации держат сотрудников службы безопасности в неведении относительно слабых мест, слепых зон сети или уязвимых векторов атак, которые следует защищать с особой тщательностью. Некоторые организации считают, что обнаружение уязвимостей в сети целиком и полностью является прерогативой службы кибербезопасности. Многие заинтересованные стороны не определяют векторы атак заранее, и если нет общепринятого или легкодоступного решения для защиты слабого места, они просто игнорируют последние и надеются, что об этом не придется пожалеть в будущем.

Иногда руководство прямо указывает сотрудникам службы безопасности *не выполнять* базовую регистрацию, сканирование или исправление устаревших систем, чтобы ненароком не нарушить бизнес-процесс. У многих организаций, утонувших в бюрократии, угроза вообще не считается реальной проблемой, если она не была задокументирована ранее. Представьте, вы видите, что у замка нет западной стены, и докладываете об этой уязвимости королю, а тот говорит, мол, неправда это, так как в отчете ничего такого не сказано.

Охрана с точки зрения фреймворка кибербезопасности

Фреймворк кибербезопасности Национального института стандартов и технологий (National Institute of Standards and Technology, NIST) [17] ставит своей целью предотвратить распространенные ошибки и повысить защищенность организаций от киберугроз с помощью пяти основных этапов кибербезопасности: идентификации, защиты, обнаружения, реагирования и восстановления. Эти этапы помогают выявлять уязвимости в сетях и системах с помощью общепринятых инструментов и процессов защиты информации.

Например, большинство организаций начинает выявление слабых мест со сканирования уязвимостей или приложений в своей сети — это этап *идентификации*. Подобное сканирование позволяет эффективно и надежно выявить очевидные проблемы безопасности, такие как необновленное программное обеспечение, активные учетные записи с отсутствующими паролями, заводские учетные записи, непараметризованный ввод и порты SSH, открытые для доступа в интернет. Следующий этап — *защита*. При обнаружении незащищенной системы сканер документирует проблему, а затем сотрудники службы безопасности исправляют или смягчают уязвимость с помощью обновлений, изменений конфигурации или архитектуры, систем безопасности или программного обеспечения.

Если сотрудники службы безопасности не могут защитить систему, которая считается возможным вектором атаки, такие системы придется *охранять* силами людей. Однако в структуре NIST не предусмотрен этап охраны. Вместо этого мы переходим

прямо к *обнаружению*: на этом этапе сотрудники службы безопасности пытаются обнаружить злоумышленника путем отслеживания и расследования аномальных событий. Лишь в тот момент, когда будет обнаружено проникновение, наступает этап *реагирования*, в рамках которого сотрудники должны сдержать угрозу, нейтрализовать ее и доложить о ней.

Последний этап — это *восстановление* систем и данных до рабочего состояния с одновременным улучшением их способности противостоять будущим атакам.

Все перечисленные меры необходимы для создания надежной системы безопасности и выполняют функции предотвращения, защиты или реагирования. В сфере кибербезопасности редко применяется концепция *охраны*, то есть надзора над системой со стороны человека, потому что защитник-человек не может вручную проверять каждое электронное письмо, веб-страницу, файл или пакет, который входит в среду и выходит из нее. Это не то же самое, что работа охранника, который может наблюдать за людьми, входящими в здание.

Дело в том, что компьютеры с пропускной способностью канала связи 1 Гбайт могут обрабатывать более 100 000 пакетов в секунду, что превышает возможности любого человека. Вместо того чтобы использовать людей-охранников, защитники либо в основном полагаются на автоматизированные средства безопасности, либо просто принимают или игнорируют какую-то долю риска. Тем не менее концепция охраны в современной цифровой сети все же может применяться, но лишь в тех областях, которые требуют особого внимания, например в наиболее вероятных векторах атаки. И здесь становится понятна польза моделирования угроз, которое позволяет выявить такие области.

Моделирование угроз

Охрану в кибербезопасности можно описать как *охоту за угрозами*, то есть активный поиск признаков проникновения в журналах, данных расследований и других наблюдаемых источниках. Не многие организации занимаются охотой за угрозами, и даже там, где это делается, задача охотника — обнаруживать, а не охранять.

Важно понимать, что в процессе охоты специалисты выходят за рамки обычных методов, постоянно придумывают новые способы атак на сети и информационные системы и внедряют необходимые средства защиты. Для этого защитники могут использовать моделирование угроз, позволяющее реализовать средства управления информационными потоками и разработать меры защиты от угроз, а не просто реагировать на них.

Моделирование угроз, как правило, выполняется только зрелыми организациями и реализуется в виде *диаграммы потока данных (DFD)*, которая описывает потоки

данных и процессы внутри систем. DFD обычно документируется в виде блок-схемы, но также может иметь вид подробной сетевой карты. DFD можно использовать в качестве инструмента для структурированного анализа плоскости атаки, который позволяет рассматривать сценарии атаки в рамках параметров задокументированных информационных систем. В этом случае не требуется сканирования уязвимостей, подтверждения сценария атаки «красной командой» или проверки со стороны системы соответствия, и организациям не приходится ждать инцидента, чтобы модель угрозы и примененные меры считались оправданными.

Понимание того, где в современных системах находятся «утопленные углы замка, места для вывоза мусора, водопроводные трубы и близлежащие кусты», может помочь вам определить векторы атак, которым требуется повышенная защита.

Рассмотрим пример: во время ночного дежурства охранник дергает за каждую дверную ручку в офисе, чтобы убедиться, что двери заперты. Найдя незапертую дверь, он запирает ее, забирает ключи и пишет доклад об инциденте.

Позже выясняется, что инцидент безопасности произошел из-за того, что дверные ключи были скопированы или украдены, поэтому организация добавляет к дверям метод аутентификации второго уровня, например кнопочную клавиатуру или считыватель бейджей, меняет замки и выдает новые ключи. Эти превентивные меры безопасности удовлетворяют аудиторов, отвечающих за соблюдение нормативных требований, и инцидент безопасности считается исчерпанным. Также директор по информационной безопасности (chief information security officer, CISO) нанимает «красную команду» для проведения узкоспециализированного теста на физическое проникновение через новые механизмы запирания, и ее участники подтверждают, что благодаря новым мерам безопасности им не удалось войти в помещение.

Однако, смоделировав угрозы, мы выяснили, что можно отодвинуть незакрепленную потолочную плитку и перелезть через стену офиса, тем самым полностью игнорируя новые меры безопасности. Для предотвращения угрозы мы могли бы добавить элементы управления, такие как камеры видеонаблюдения или датчики движения в подвесном потолке, либо установить другие потолки и полы, не дающие возможности никуда пролезть. Можно даже нанять охранников и научить их определять места сдвига потолочной плитки, обнаруживать на потолке, стенах или полу следы преступников. При этом нужно, чтобы охранники находились внутри комнаты или вообще внутри потолка, и у них должны быть полномочия и средства для защиты помещения от злоумышленников.

Возможность реализации таких контрмер невелика — за одно лишь подобное предложение вас поднимут на смех. Нетрудно понять, почему организация скорее посчитает определенные угрозы допустимым риском, чем будет пытаться отразить их. Вероятно, именно поэтому NIST Cybersecurity Framework не включает этап

охраны. Однако сам образ мышления, основанный на детальном моделировании угроз, и последующая вдумчивая и креативная реализация мер безопасности могут повысить безопасность информационных систем и сети.

В качестве примера сценария, подходящего для реализации охранной функции, рассмотрим *блоки перехода*. Блок перехода — это система, которая охватывает две границы сети или более, позволяя администраторам удаленно входить в систему в блоке перехода одной сети и переходить в другую сеть, получая к ней доступ. Традиционные меры кибербезопасности требуют повышения защищенности блоков перехода путем исправления всех известных уязвимостей, ограничения доступа с помощью правил брандмауэра и мониторинга журналов аудита на предмет аномальных событий, таких как несанкционированный доступ. Однако такие технические средства контроля часто атакуют или обходят. В то же время охранник может физически отсоединить внутренний сетевой кабель от другой сети и подключить его напрямую только после проверки того, что у пользователя есть разрешение на выполнение удаленных команд в данной системе. Охранник также может активно отслеживать действия на машине в режиме реального времени и принудительно завершать сеанс сразу же, как только обнаружит злонамеренные или несанкционированные действия. Таким образом, реализация функции охраны может означать найм человека-охранника, который будет сидеть в дата-центре и предотвращать как физический, так и удаленный доступ к защищаемой системе.

Использование модели угроз для поиска потенциальных векторов атак

При определении векторов атак необходимо придерживаться процедуры моделирования угроз, начиная с создания DFD. Как только потенциальные векторы атаки определены, трактаты синоби рекомендуют проверить их и определить, какие технические меры безопасности можно реализовать для организации защиты. Затем, если есть нужда, для защиты этих областей можно задействовать охранников. Вы можете использовать карту сети, составленную в предыдущей главе, чтобы на ее основе создать DFD, или непосредственно по ней найти векторы атак.

1. **Смоделируйте свои информационные системы.** Создайте точную DFD на основе информации о сети вашей организации при содействии отделов безопасности, разработки, бизнеса, других заинтересованных лиц и экспертов по ИТ-системам. Необязательно использовать унифицированный язык моделирования (Unified Modeling Language, UML) или другой сложный инструмент. Достаточно лишь точно представить систему и информацию о ней. Обратите внимание на то, что создание схем больших и сложных систем иногда может занять у команды более шести месяцев.

2. **STRIDE и защита.** STRIDE — это методология моделирования угроз, разработанная Microsoft [1] для описания того, что в информационной системе может пойти не так. Аббревиатура составлена из названий того, что злоумышленник может совершить с вашей системой.

Spoofing identify (подделка идентичности)	=	Аутентификация
Tampering with data (порча данных)	=	Целостность
Repudation/deniability (отказ)	=	Безотказность
Information disclosure (раскрытие информации)	=	Конфиденциальность
Denial of service (отказ в обслуживании)	=	Доступность
Elevetion of privilege (получение привилегий)	=	Авторизация

Чтобы задействовать методологию STRIDE, посмотрите на составленную DFD и предположите, как злоумышленник может навредить в каждой точке, где происходит ввод, обработка и вывод данных или имеются другие потоки данных либо правила. Например, если для проверки личности пользователя системе требуется отпечаток большого пальца, то прежде чем разрешить доступ к системе, подумайте, как злоумышленник может подделать этот отпечаток, чтобы выдать себя за другого пользователя. Или можете подумать о том, как злоумышленник может проникнуть в базу данных отпечатков пальцев и загрузить туда свой отпечаток. Вы можете изучить сценарий, в котором злоумышленник отключает сканер отпечатков пальцев, а затем получает доступ через более слабый процесс аутентификации.

Можете применить предложенный фреймворк для проверки любых предполагаемых моделей угроз, которые неточно представляют ваши системы, или сценариев, которые не описывают, как та или иная угроза повлияет на конкретные компонент, поверхность или вектор. Для этого может потребоваться содействие технических экспертов в области моделирования угроз.

Предположим, что после моделирования угроз в организации создается сценарий «Угроза вредоносного ПО нарушает целостность внутренних баз данных». Эта угроза не смоделирована должным образом. В числе прочей важной информации полученный сценарий не описывает, как вредоносное ПО может попасть и установиться в систему. Он также не описывает, как вредоносная программа может нарушить целостность базы данных и что

именно она делает: шифрует, удаляет или повреждает данные? Сценарий не описывает, через какие векторы угроза может воздействовать на систему, не учитывается поток информации и имеющиеся средства контроля, не предоставляются реалистичные меры противодействия. Если, например, мы определили, что наиболее вероятным способом заражения внутренней бизнес-базы данных вредоносным ПО будет USB-накопитель, то отдел безопасности может разработать политику, подробно описывающую, как сотрудники должны использовать USB-накопители, или установить камеры для отслеживания доступа к USB-портам. Организация может дать отделу безопасности возможность включать или выключать USB, определять, какие диски могут взаимодействовать с USB, управлять потоком информации через USB-порты, проверять файлы на USB-накопителях перед предоставлением доступа, управлять доступом с помощью аппаратной или программной блокировки или вообще залить порты USB эпоксидной смолой. Такие меры, будучи результатом тщательного моделирования угроз, позволяют сотрудникам службы безопасности полноценно защищаться от конкретных угроз, а не считать риск допустимым и не ограничиваться функциями защиты и обнаружения.

3. **Не распространяйтесь о предпринимаемых мерах безопасности.** Моделирование угроз — это итеративный бесконечный процесс оценки новых угроз и разработки защитных контрмер. Разрабатывая способы защиты систем, избегайте использования *синоби-гаэси*, то есть того, что явно привлекает внимание к уязвимым областям. Часто из-за ограничений во времени, ресурсах или из-за общей занятости вводится лишь часть мер безопасности, которые мотивированный и хитроумный злоумышленник способен обойти. Например, эпоксидную смолу из USB-порта можно удалить с помощью изопропилового спирта. По возможности оцените жизнеспособность ориентированного на безопасность защитного подхода.

   В примере с атакой через USB сам интерфейс USB работает на аппаратном уровне абстракции (hardware abstraction layer, HAL), который находится ниже ядра ОС. Этот уровень нельзя полностью защитить с помощью программного обеспечения и программных политик, поскольку они существуют над ядром и их можно обойти. Следовательно, комплексным решением может быть использование материнской платы и корпуса, в которых USB-портов вообще нет. Эпоксидная смола в USB-порте напрямую сообщает мотивированным злоумышленникам, что вы недостаточно хорошо поразмыслили над должной безопасностью USB-устройств и, вероятно, здесь легко провести атаку, удалив смолу. Это работает так же, как если синоби извлекает прикрепленные к трубам шипы и пробирается в замок.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Рассмотрим сценарий, в котором вы — правитель средневекового замка, а в нем хранятся разные ценности. Вам стало известно, что ниндзя планирует проникнуть в замок и поджечь запасы провизии в подвале. В нем есть несколько точек входа/выхода, через которые слуги перевозят провиант, и при этом за ними никто не следит.

Подумайте, какие меры могут предпринять охранники, чтобы уберечь провиант от пожара. Какие кадровые изменения вы можете осуществить, чтобы проконтролировать взаимодействие людей с провизией и не допустить нанесения ей вреда? Какие меры позволят охранникам сразу все увидеть, быстро сообщить о пожаре и отреагировать на него? Как охранники могут обнаружить ниндзя, проникающего в подвал, и какие архитектурные изменения можно было бы внести, чтобы слепых пятен на подходе к подвалу стало меньше?

Разумеется, было бы целесообразно хранить запасы провизии в разных местах, а еще лучше — в огнеупорном материале, но в рамках этого упражнения стоит подумать именно о том, как охранники могут контролировать и защищать провизию, а не напрямую устранять угрозу пожара.

Рекомендуемые меры безопасности и предосторожности

1. Проанализируйте результаты аудита, оценки «красной команды», данные сканирования уязвимостей и отчеты об инцидентах, чтобы найти в среде уязвимости, которые нельзя легко исправить или устранить с помощью мер контроля, то есть тех, которые требуют особой защиты. (CA-2. Оценка безопасности; CA-8. Тестирование на проникновение; IR-6. Отчеты об инцидентах | (2) Уязвимости, связанные с инцидентами; RA-5. Сканирование уязвимостей.)
2. Выполните моделирование угроз вашей среды для выявления уязвимостей. Определите, какие из них можно разработать за пределами среды. Изучите концепцию охранных функций безопасности и примените эти средства контроля к угрозам, которые сложно устранить. (SA-8. Принципы обеспечения безопасности; SA-14. Анализ критичности; SA-15. Процесс разработки, стандарты и инструменты | (4) Моделирование угроз/анализ уязвимостей; SA-17. Архитектура и дизайн безопасности для разработчиков.)
3. Чтобы сдержать распространение угроз, защищаться от них и обеспечить быстрое реагирование на них, наймите сотрудников службы безопасности,

которые будут охранять систему в режиме реального времени, и посадите их следить за уязвимыми областями бизнес-операций. (IR-10. Группа комплексного анализа информационной безопасности.)

Резюме

Эта глава помогла вам подумать о том, какие точки в вашей сети злоумышленник может атаковать с целью проникновения. Мы также рассмотрели концепцию защиты, при которой человек контролирует информационные системы и процессы. Возможно, вы использовали карту сети из предыдущей главы или создали собственную диаграмму потока данных для определения вероятных векторов атак и потенциальных угроз из парадигмы STRIDE, которые можно нейтрализовать с помощью средств защиты.

В следующей главе рассмотрим «ксенофобскую» концепцию безопасности, используемую древними ниндзя. Эта концепция помешает противникам найти какие-либо точки соприкосновения с вашей средой или точки опоры в ней и тем самым помешает вообще предпринять какую-либо атаку.

3

Ксенофобская безопасность

Если вы без особых раздумий впускаете к себе незнакомцев, вражеские синоби могут проникнуть к вам под видом незнакомца и найти нужную информацию.

Если рядом с постом снуют попрошайки или нищие,
следует жестко разогнать их.
«Ёсимори хяку-сю», № 91

В этой главе мы исследуем концепцию ксенофобской безопасности (безопасности, основанной на недоверии к посторонним) и ее применение в качестве меры защиты от привилегий. Чтобы проиллюстрировать эту идею, рассмотрим враждебную среду, в которой перемещаются синоби.

Синоби, пытающиеся проникнуть в деревню и собрать информацию у всех на виду, сталкивались с проблемой невероятной ксенофобии средневековых японцев. Изоляция деревень страны привела к появлению уникальных диалектов, причесок, одежды и других обычаев, из-за которых каждая деревня превращалась в обособленную экосистему [6]. В таких поселениях жителей было немного, все знали друг друга, а посторонние сразу бросались в глаза [6]. Поэтому на чужаков-синоби обычно смотрели с подозрением и следили за ними. Они не могли свободно передвигаться по деревне, часто не могли снять комнату и даже купить еду. И разумеется, сельчане не горели желанием делиться с чужаками информацией. Ксенофобия привела к тому, что синоби стали *антипривилегированными*.

Понятие антипривилегии

Чтобы понять концепцию антипривилегии, рассмотрим сначала концепцию *привилегии*, под которой в кибербезопасности обычно понимаются разрешения, которые пользователь получает для работы, например разрешение на чтение или удаление

файла. Современные компьютерные системы имеют кольцевую архитектуру с разными уровнями привилегий:

- **уровень 4** — по умолчанию (непривилегированный пользователь);
- **уровень 3** — обычный пользователь (с минимальными привилегиями);
- **уровень 2** — суперпользователь (админ);
- **уровень 1** — root-пользователь (повышенные привилегии);
- **уровень 0** — ядро (система).

Например, простой сельский житель (минимально привилегированный) или кошка (непривилегированный) могут покинуть город в любой момент. Староста села, имеющий повышенные привилегии, дополнительно имеет право запереть городские ворота. А иностранец, подозреваемый в причинении вреда (антипривилегия), может иметь еще меньше разрешений, чем бездомная кошка (непривилегированная), и поэтому ему не разрешат покинуть деревню.

Важно понимать различие между антипривилегиями и отсутствием привилегий. В некоторых компьютерных системах такие действия, как выход из системы, считаются непривилегированными и по умолчанию разрешены субъектам на всех уровнях. Ненадежные процессы/пользователи могут задействовать непривилегированные возможности для совершения злонамеренных действий или относительно свободно делать свои дела, преследуя злые цели. А запретив антипривилегированному процессу выйти из системы, вы можете помешать ему подчищать историю сеансов и следы своего присутствия. Представьте, что компьютерная система поддерживает пятый уровень безопасности (антипривилегированный). Если мы вернемся к примеру с деревней, то жители могут заставить подозреваемого синоби пройти обыск и допрос и лишь потом выпустить из деревни. Таким образом в деревне можно было поймать воров и шпионов.

Более того, делая работу лазутчиков намного более рискованной и дорогой, деревни, несомненно, сдерживали враждебную активность. Чтобы проникнуть в деревни, где враждебно относились к чужакам, синоби сначала приходилось запомнить и отработать несколько подходящих для данной культуры приемов маскировки: начать носить одежду, обычную для этой местности, сделать нужную прическу, освоить местный диалект, узнать обычаи и социальные правила, характерные для этого места.

Когда культурная маскировка выполнена, синоби нужно придумать убедительный повод оказаться в деревне, обычно связанный с работой. «Нимпидэн» описывает, как синоби придумывали истории прикрытия и притворялись странствующими монахами, торговцами, нищими или даже самураями, путешествующими по приказу

своего господина (самурай, даже если был чужаком, не вызывал такого же уровня недоверия, как потенциальный беглец или бандит).

Находясь замаскированным в окружении людей той же профессии, класса или касты, синоби должны были демонстрировать достаточно знаний, чтобы казаться реальными представителями профессии, а также «не уметь» выполнять другие общепринятые вещи. Имитация незнания позволяла обмануть цель относительно истинного интеллекта синоби, а заодно служила инструментом лести, снижала уровень бдительности цели и развязывала ей язык. В «Нимпидэн» описаны те, кого синоби могли победить с помощью этой тактики: местные чиновники, сотрудники магистрата, врачи, монахи и другие лица, работающие в контакте с местным властителем или знатью. Эти цели обычно обладали ценной для миссии информацией [6].

Обратите внимание на то, что социальная иерархия средневековой японской деревни напоминает кольцевую структуру привилегий в современных компьютерных системах или даже многоуровневую сегментацию компьютерных сетей, в которой внешние уровни, такие как DMZ, вызывают наименьшее доверие. Точно так же обычные сельские жители (наименее привилегированные) не могут взаимодействовать с господином, который находится в центре, то есть на уровне 0.

Мы можем применить метод определения вероятных целей синоби в контексте кибербезопасности. Подобно тому как синоби нацелены на тех, кто, образно говоря, находится поближе к уровню 0 или имеет к нему доступ, современные злоумышленники нацеливаются на привилегированные классы систем или пользователей. Таким образом, защитники должны понимать, что является компьютерным эквивалентом высокопоставленных жителей деревни. Кроме того, следует продумать, какую маскировку может использовать современный злоумышленник, чтобы приблизиться к более привилегированным системам или пользователям.

Проблема взаимодействия и универсальных стандартов

Даже если сознательно об этом никто не думает, *совместимость* является высшим приоритетом для потребителей технологий: люди ожидают, что их устройства, приложения, системы и программное обеспечение будут без проблем работать с новыми и старыми версиями и на разных платформах, а также будут взаимозаменяемыми с другими марками и моделями. Международная организация по стандартизации (International Electrotechnical Commission, ISO), Международная электротехническая комиссия (International Organization for Standardization, IEC), Инженерный совет интернета (Internet Engineering Task Force, IETF), Общество интернета (Internet Society, ISOC) и другие руководящие органы установили согласованные стандарты того, как технологии должны разрабатываться, функционировать и интегрироваться.

В результате появилось много стандартов ISO, запросов на комментарии (Request for Comments, RFC) и других протоколов взаимодействия, которые делают компьютеры более доступными, не говоря уже о том, что стало легче их создавать, диагностировать, ремонтировать, программировать, подключать к сети и запускать, а также управлять ими. Ярким примером является стандарт Plug and Play (PnP), представленный в 1995 году, который предписывает хост-системе обнаруживать и принимать любое постороннее устройство, подключенное к ней через USB, PCI, PCMCIA, PCIe, FireWire, Thunderbolt или другие средства, а затем автоматически настраивать его и настраивать интерфейс.

К сожалению, когда во главу угла ставится функциональность и работоспособность, безопасность почти никогда не оказывается приоритетом. Фактически стандарт PnP, который способствует доверию и принятию незнакомых сущностей, являет собой полную противоположность ксенофобскому стандарту безопасности, которого придерживались средневековые японцы. Например, незнакомая система может подключиться к сети, запросить IP-адрес из протокола динамической конфигурации хоста (Dynamic Host Configuration Protocol, DHCP), направление от локального маршрутизатора, полномочный DNS-сервер и имена других устройств и получать локальную информацию из протокола разрешения адресов (Address Resolution Protocol, ARP), блока сообщений сервера (Server Message Block, SMB), автоматического обнаружения веб-прокси (Web Proxy Auto Discovery, WPAD) и других протоколов, обеспечивающих совместимость. Вы подключаете систему к сети, и она работает, демонстрируя именно то поведение, которого пользователи от нее ожидают.

Чтобы выявить слабые места, связанные с доступностью протокола PnP, были введены средства управления безопасностью, такие как контроль доступа к сети (Network Access Control, NAC) и объекты групповой политики (Group Policy Objects, GPO). В хост-системах эти технологии защищают от потенциально вредоносных посторонних устройств, которые физически подключаются к внутренним сетям или системам.

NAC обычно блокируют DHCP, определяя неопознанные компьютеры в гостевые IP-подсети или непривилегированные VLAN. Это позволяет посторонним системам подключаться к интернету, но отделяет их от заслуживающей доверия части сети. Такое поведение полезно для конференц-залов и вестибюлей, в которых посторонние деловые партнеры и поставщики могут работать, не подвергая сеть угрозам.

GPO на локальных хостах определяет, какие типы устройств — внешние жесткие диски, USB-накопители, устройства чтения мультимедиа и т. д. — могут подключаться к системе. GPO может даже занести в белый список известные в организации приложения, блокируя загрузку или установку всего незнакомого программного обеспечения в хост-системе.

Однако эти меры безопасности — скорее исключение. Большая часть технологий, от разъемов RJ45 Ethernet с использованием стандартов EIA/TIA-561 и Yost до пакетных сетей с применением стандартов IEEE 802, построены на прозрачных, широко известных стандартах, обеспечивающих быстрое и легкое использование в разных системах и сетях, что делает их уязвимыми для систем злоумышленников, которые могут обнаруживать сеть и выполнять разведку, анализ и связь.

Разработка уникальных характеристик для вашей среды

Благодаря уникальным свойствам и характеристикам вашего технического оснащения вы сможете отличить оборудование вашей системы от мошеннического и даже защитить сеть от взлома. Эти характеристики можно наблюдать и анализировать, но их использование не должно широко разглашаться, поскольку это сводит на нет всю защиту. Большинство элементов современных ИТ-систем и программного обеспечения можно настраивать, и такие изменения конфигурации, по сути, создают ксенофобскую ИТ-модель системы.

Недавно появившиеся коммерческие продукты, использующие модель нулевого доверия, могут помочь сделать вашу сеть или системы подозрительными по отношению к незнакомым системам, программному обеспечению и устройствам за счет сочетания технических протоколов и недоверия. Строгие белые списки и процедуры аутентификации/авторизации дают тот же результат, но правильнее было бы ввести компьютерный аналог «диалектов», то есть настроек, приемов и других уникальных характеристик, отличающихся от универсальных компьютерных стандартов. Системы или устройства, подключающиеся к вашей внутренней сети, должны быть «обучены» уникальной культуре вашей организации, а посторонние серверы, компоненты, сетевые устройства и протоколы будут отвергаться, причем служба безопасности предупредит о вторжении.

Применив креативность и технические знания, можно реализовать такие культурные идентификаторы на любом уровне модели взаимодействия открытых систем (Open Systems Interconnection, OSI) (приложение, представление, сеанс, транспорт, сеть, канал передачи данных, физический уровень) для идентификации внешних нарушителей сети и обеспечения дополнительного уровня защиты от злоумышленников. Каким бы ни было ксенофобское решение — перестановка определенных контактов в скрытых адаптерах разъемов RJ45, выполнение «секретных рукопожатий» (SYN, SYN ACK, ACK-PUSH) на уровне TCP/IP или использование зарезервированных битов в заголовке Ethernet, — оно должно быть модульным, настраиваемым и уникальным для каждого экземпляра.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Рассмотрим сценарий: вы управляете средневековым замком, в котором хранится что-то ценное. Вы замечаете, что один из местных рыбаков, продающий рыбу вашим поварам, консервирует ее по незнакомой технологии и говорит на странном диалекте. Когда его спрашивают, почему он так делает, он утверждает, что рыба при такой консервации получается вкуснее. Его фамилия вам незнакома.

Какие уникальные культурные идентификаторы вы могли бы использовать, чтобы определить, является ли рыбак посторонним, и как их применить? Если рыбак говорит, что родился в вашей деревне, но какое-то время жил в другом месте, как проверить сказанное? Если не удалось проверить его историю и вы подозреваете его в шпионаже, как устранить угрозу, не изгнав или не казнив потенциально невиновного рыбака? Чтобы ответить на эти вопросы, вам нужно рассмотреть три сценария: рыбак действительно шпион, рыбак не шпион и цель рыбака неясна. Вы можете попросить напарника сыграть роль такого рыбака, предварительно тайно выбрав одну из ролей, а можете мысленно отыграть роли и рыбака, и следователя.

Это упражнение помогает подумать об идентификации активов с использованием ксенофобских моделей, избегая при этом технических вопросов, касающихся компьютерных стандартов и инвентаризации. Хотя сценарий этот вымышленный, синоби, вероятно, иногда маскировались под рыбаков, поскольку такое прикрытие давало им возможность ходить туда-сюда, болтать с местными жителями и проводить разведку.

Рекомендуемые меры безопасности и предосторожности

1. Проанализируйте системы и определите, соответствуют ли их спецификации и требования ранее согласованной базовой конфигурации. (CM-2. Базовая конфигурация.)
2. Поддерживайте документирование всех информационных систем в своей организации, что позволяет быстрее и проще идентифицировать чужие системы в вашей среде. (CM-8. Инвентаризация информационной системы.)
3. Используйте зашифрованную информацию, встроенные данные, специальные типы данных или метаданные (например, заполнение всех пакетов до определенного размера) в качестве специальных идентификаторов при обмене данными, чтобы настроенные фильтры могли выявлять и отсекать

незнакомый трафик. (AC-4. Настройка информационного потока; SA-4. Процесс перехвата.)

4. Ограничьте внедрение и передачу информации о ксенофобских идентификаторах вновь обнаруженным системам и устройствам. (SA-4. Процесс обнаружения.)
5. Используйте ксенофобский анализ как средство безопасности в процессе идентификации и аутентификации систем и устройств в своей организации. (IA-3. Идентификация и аутентификация устройства.)

Резюме

В этой главе мы описали исторически сложившуюся ксенофобскую среду, в которой действовали синоби, для чего им требовалось немало времени и усилий, а также знание передовых методов подготовки к разведке и применение тактики открытой маскировки до начала непосредственной разведки. Вы узнали о концепции антипривилегий и о том, как создавать уникальные внутренние характеристики для идентификации несанкционированных ресурсов или пользователей в своей среде. Теперь вы можете определить ключевые ресурсы или людей, которые являются вашими вероятными целями, хоть их можно и не счесть вектором атаки по результатам предыдущих упражнений по моделированию угроз. Затем вы можете рассмотреть системы или учетные записи, которые тесно связаны с потенциальными целями.

Используя правильные знаки отличия, одежду, прическу, акцент и другие характеристики жителей, синоби могли избегать проверок, подробно описанных в этой главе. В следующей главе мы исследуем технику безопасности «согласованная пара», издавна применявшуюся японскими военачальниками для обнаружения замаскированных синоби, которые могли проникнуть в замок.

4

Задача идентификации

Еще в древности были придуманы способы идентификации знаков, паролей и сертификатов, и если вы не изобретаете новые или не меняете существующие, враг сможет подделать их и проникнуть к вам.

Во время ночной атаки враг может проникнуть
в ряды ваших союзников. Чтобы предотвратить это,
имейте заранее определенный способ отличить своих
от чужих.

«Ёсимори хяку-сю», № 27

Представьте себе следующий сценарий из прошлого: большая группа войск совершает ночной набег и возвращается домой, а военачальник должен открыть ворота, чтобы впустить их в замок. Ночные рейды помогали выигрывать битвы, но они же создавали возможности для контратаки. Вражеские синоби могли скопировать или украсть униформу атакующих и влиться в их строй во время возвращения в лагерь.

Чтобы обезопасить себя, командиры вводили одноразовый пароль, который бойцы должны были знать, чтобы пройти через ворота. Но такой пароль легко было взломать, так как замаскированные синоби могли подслушать его, если солдат, стоявший впереди, произносил слово вслух. Тогда командиры пробовали другие способы опознавания. Некоторые требовали, чтобы все воины носили нижнее белье определенного заранее цвета, которое можно было проверить по их возвращении, но умные синоби носили несколько предметов белья, а затем во время осмотра выборочно стягивали слои, чтобы был виден только правильный цвет. Некоторые практиковали смену паролей несколько раз в день (что по-прежнему не мешало синоби подслушать действующий в данный момент), вводили уникальную униформу или жетоны (их синоби мог украсть с трупа мертвого солдата после рейда).

Синоби классифицировали эти техники как искусство открытой маскировки (*ё-нин*, что буквально переводится как «светлое ниндзюцу») в противоположность искусству скрытого проникновения (*ин-нин*, что переводится как «темное ниндзюцу»).

Под *открытой* маскировкой понимается, что синоби явно видим, но переодет, например, в форму защитника замка, так как его обязательно заметят. Под *скрытой* техникой понимается нежелание быть увиденным, например использование камуфляжа или слияние с тенями. Многие приемы открытой маскировки, описанные в «Бансэнсюкай», можно применять и в нападении, и в обороне. Синоби умели применять их не только для атак, но и для обнаружения вражеских лазутчиков. Для шпионов было обычным делом копировать униформу и эмблемы или подслушивать пароли, поэтому синоби разработали специальные методы, позволяющие отличать союзников от врагов.

Одним из таких методов идентификации был *метод согласованной пары*, то есть сочетания слов, используемые для аутентификации союзников [6]. Этот метод известен также как *парный пароль* или *вопрос — ответ*. Метод работал следующим образом: допустим, у ворот замка появился неизвестный человек, который хочет войти. Охранник видит, что незнакомец одет в свою форму и носит герб союзника. Тогда охранник произносил слово, например «дерево». Если незнакомец не назвал в ответ нужную пару, например «лес», охранник знал, что перед ним чужак. В «Бансэнсюкай» отмечается, что парные пароли должны быть довольно простыми, чтобы люди низшего ранга могли их запомнить, но не рекомендуется использовать общие ассоциации, которые легко угадать. Например, вместо пары «снег» и «гора» стоит взять пару «снег» и «гора Фудзи». Трактат рекомендует командирам придумать 100 различных пар слов на 100 дней и каждый день вводить новую пару [6]. Такое большое количество пар позволит часовому при необходимости выбирать из списка новую пару для каждого проходящего через ворота отряда, что снижает вероятность того, что противник подслушает пароль.

Парные пароли использовались для выявления возможных лазутчиков. Если незнакомец отвечал неправильно, его быстро задерживали, допрашивали и, возможно, убивали. Зная об этих последствиях, «Бансэнсюкай» рекомендует, чтобы синоби, пытающиеся проникнуть во вражеский лагерь, вели себя и выглядели как неряшливые солдаты или солдаты низшего класса. В этом случае, если синоби не знает пары к названному паролю, можно убедить охранника, что ты просто не знал такого пароля, но на самом деле свой [6]. Вы могли заметить, что финансовые учреждения начали внедрять методы сопоставленных слов или изображений для онлайн-аутентификации, но на таких сайтах не используется 100 пар, а те, которые есть, обновляются крайне редко. Малое количество пар позволяет злоумышленнику запомнить все пары, а затем воспользоваться ими в своих целях.

Приведенные исторические примеры позволяют понять, как трудно защитить свои механизмы аутентификации от умного и изворотливого противника. В этой

главе мы коснемся того, насколько сложным может быть процесс аутентификации, а также рассмотрим факторы, используемые в информационном обеспечении (information assurance, IA) для проверки личности. Я упомяну некоторые методы, которые задействуются в современных киберпреступлениях для того, чтобы обойти механизмы аутентификации, и приведу аналогичные тактики синоби, которые показывают, почему аутентификация в обозримом будущем станет проблемой. Также я расскажу читателям, как применять методы аутентификации синоби в современных приложениях. Цель этой главы состоит в том, чтобы помочь им понять основные вопросы идентификации и при этом не потеряться в обширной области знаний, в которую превратились аутентификация и криптография.

Понятие аутентификации

Аутентификация — процесс подтверждения личности пользователя перед предоставлением ему доступа к информационным системам, данным, сетям, помещениям и другим ресурсам. В процессе аутентификации система подтверждает идентичность пользователя, запрашивая что-то, что он знает, что-то, что у него есть, или что-то, чем он является. Например, аутентификатор может запросить пароль (то, что пользователь знает), токен (то, что у него есть) или биометрические данные (то, чем он является). В зависимости от необходимого уровня безопасности организациям может требоваться *однофакторная*, *двухфакторная* или *многофакторная* аутентификация.

В сложившихся организациях используется также *строгая аутентификация*, в которой задействуется несколько уровней многофакторных учетных данных. Например, на первом этапе строгой аутентификации могут потребоваться имя пользователя, пароль и отпечаток пальца, а на втором этапе — токен и одноразовый код, отправленный по SMS. Все чаще специалисты думают о возможности введения четвертого фактора, а именно доверенного сотрудника организации, который мог бы подтвердить личность пользователя. Интересно, что сценарий с парным паролем начинается именно с этого теста, так как пароль применяется только в том случае, если никто поблизости не может подтвердить личность незнакомца.

Сбой аутентификации — это критическая проблема безопасности. Идентификационные данные пользователей определяют разрешения, которые позволяют им выполнять определенные, зачастую привилегированные, действия. Злоумышленник, которому удается выдать себя за реального пользователя, прошедшего проверку подлинности, получает свободный доступ к ресурсам пользователя и может совершать злонамеренные действия в информационных системах, данных и сетях.

К несчастью, процесс аутентификации несовершенен. Несмотря на множество способов кибераутентификации, все равно невозможно со стопроцентной точностью

установить личность пользователя или процесса, поскольку почти каждую проверку можно обойти (например, с помощью подделки — применения ложных данных с целью выдать себя за другое лицо) или скомпрометировать. Злоумышленники используют разнообразные методы кражи паролей, перехвата токенов, копирования хешей аутентификации или токенов, а также подделки биометрических данных. Если злоумышленник получает неавторизованный доступ к системе управления идентификацией, например к контроллеру домена, он может сам создавать поддельные учетные записи и проходить с их помощью аутентификацию. После успешной аутентификации личность пользователя редко подвергается сомнению, кроме случаев, когда для выполнения привилегированных действий требуется повторный ввод пароля. Аналогично, замаскированные синоби могли свободно разгуливать по замку, так как предполагалось, что их личность уже проверена на входе.

Развитие технологий безопасности нацелено на борьбу с угрозами аутентификации. Одно из новых решений в этой сфере называется *непрерывной аутентификацией*, или *активной аутентификацией*. В этом случае система проверяет личность пользователя постоянно с момента его входа в систему. Однако поскольку обмен данными в процессе непрерывной аутентификации может затруднять взаимодействие с пользователем, разрабатываются и другие методы мониторинга аутентификации с помощью приемов набора текста, движения мыши или других поведенческих характеристик, которые позволяют определить личность человека. Такие методы позволяют выявить злоумышленников, которые получают доступ к оставшейся без присмотра системе, и блокируют их работу. Эти же методы можно применять к неавторизованным пользователям, работающим через удаленный доступ, например по протоколу удаленного рабочего стола (Remote Desktop Protocol, RDP). Поведенческие методы позволяют выявлять злоумышленников, даже если они авторизованы с помощью настоящих учетных данных. Разумеется, поведение человека может измениться. Более того, наиболее изощренные злоумышленники могут имитировать или моделировать поведение другого человека, включив в свои атаки рекогносцировку поведения пользователей.

Модель парного пароля может быть реализована через человеко-машинный интерфейс, в котором задействуются пассивные датчики мозговых волн, подключенные к системе, проверяющей личность на основе мысленных импульсов пользователя. Исследования показывают, что люди генерируют уникальные мозговые паттерны или мыслительные ассоциации, когда смотрят на объект, с которым они взаимодействовали раньше. Таким образом, отображение управляемых пользователем воздействий, таких как парные слова или комбинации изображений, мониторинг электрических импульсов мозга и их сопоставление с профилем пользователя позволяют точно аутентифицировать его. При достаточном количестве уникальных пар задач, генерируемых динамически, сводится к нулю вероятность того, что злоумышленники смогут воспроизвести или смоделировать активность мозговых волн пользователя при появлении соответствующего запроса.

В следующем разделе мы обсудим методы, которые можно применять для реализации аутентификации методом согласованной пары.

Разработка аутентификаторов методом согласованной пары

В этом разделе мы рассмотрим несколько предложений по разработке аутентификаторов методом согласованной пары и идей по их применению.

- **Работайте с правильными поставщиками средств аутентификации.** Найдите поставщиков, которые используют аутентификацию с помощью ключевой фразы, не совпадающей с паролем пользователя, именем учетной записи или другой связанной с пользователем информацией, которую злоумышленник может скомпрометировать. Некоторые финансовые организации не разрешают менять учетную запись без прохождения такой аутентификации, но, к сожалению, гораздо чаще этот метод применяется лишь тогда, когда пользователь пытается восстановить забытый пароль, а контрольные фразы при этом не меняются.
- **Разработайте новые системы аутентификации.** Ваше средство аутентификации может интегрироваться с элементами управления и запрашивать согласованную пару у аутентифицированного пользователя всякий раз, когда он пытается выполнить привилегированные действия, такие как команды от имени администратора, или root-пользователя, или системы. Согласно этому протоколу, даже если злоумышленник сумел разведать одну или несколько запрашиваемых пар, запрос на выполнение привилегированных действий будет отклонен.

  В идеальном продукте применяются две формы согласованных пар: ежедневные и пользовательские. Ежедневная проверка выполняется в нецифровом формате и только для авторизованного персонала. Например, для доступа в помещения могут использоваться пары слов или изображений. Все остальные сотрудники, включая работающих удаленно, создают большой набор пар слов, которые вряд ли будут забыты или неверно истолкованы. Организация выбирает пары случайным образом или меняет их, чтобы быстро выявить неавторизованных пользователей, прошедших аутентификацию в сети. (Обратите внимание на то, что злоумышленник может добавить собственные пары в скомпрометированные или поддельные учетные данные, и для защиты от этого должны быть обеспечены безопасные передача, хранение и аудит новых пар в активной системе проверки.) Рассмотрите возможность использования одностороннего интерфейса добавления новых пар в защищенном контролируемом информационном объекте (secure controlled information

facility, SCIF) или сегментированной области, где нужна была бы ручная аутентификация и авторизация. Существуют и другие механизмы, которые могут позволить организациям вылавливать неопознанных пользователей с помощью запроса доступа к микрофону, камере, местоположению, запущенным процессам, оперативной памяти или кэшу, снимка экрана рабочего стола и другой информации о системе подключения, что позволяет лучше определить источник и личность угрозы.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Рассмотрим сценарий, в котором вы — правитель средневекового замка, где хранятся некоторые ценности. Вы успешно совершили набег на вражескую армию и вернулись домой. Солдат из вашей армии согласно обычаю желает подойти к вам и преподнести отрубленную голову вражеского командира. Воин носит вашу униформу, правильный герб, знает пароль, хорошо ориентируется внутри вашего замка и ждет разрешения войти во внутреннюю цитадель, чтобы засвидетельствовать вам свое почтение.

Подумайте, как быть с подозрительными людьми, которые проходят стандартную проверку подлинности и запрашивают привилегированный доступ. Какие из существующих протоколов безопасности или процессов аутентификации помогут вам определить, свой это воин или замаскированный синоби, желающий вашей смерти? Как снизить риск, если вы не можете определить личность воина (помимо прямого отказа в доступе)?

Рекомендуемые меры безопасности и предосторожности

Все предложенные методы следует рассматривать в контексте идентификации и аутентификации методом согласованной пары.

1. Реализуйте для привилегированных учетных записей разрыв сессии через определенные промежутки времени, по запросу привилегированных пользователей или в ответ на подозрительное поведение. Доступ должен восстанавливаться только после того, как пользователь пройдет проверку методом согласованной пары (блокировка сеанса предпочтительнее, чем обычная блокировка паролем, поскольку задачу на согласованную пару решить легче, чем ввести пароль). (AC-11. Блокировка сеанса; IA-2. Идентификация и аутентификация (пользователи в организациях) | (1) Сетевой доступ к привилегированным учетным записям | (3) Локальный доступ

к привилегированным учетным записям; IA-10. Адаптивная идентификация и аутентификация; IA-11. Повторная аутентификация.)

2. Идентифицируйте, документируйте и применяйте меры безопасности в отношении тех действий пользователей, которые можно выполнять без решения согласованной пары (например, обращение в техподдержку или вызов службы экстренной помощи). (AC-14. Разрешенные действия без идентификации или аутентификации.)
3. Разработайте аутентификацию методом согласованной пары, устойчивую к атакам повторного воспроизведения, путем создания больших наборов аутентификаторов одноразового запроса — ответа. (IA-2. Идентификация и аутентификация (пользователи в организациях) | (8) Сетевой доступ к привилегированным учетным записям — устойчивость к повторному воспроизведению.)
4. Перехватывайте информацию, которая однозначно идентифицирует запрашивающее аутентификацию устройство, чтобы получить сведения о неопознанных лицах, не прошедших проверку согласованной пары. (IA-3. Идентификация и аутентификация устройства | (4) Аттестация устройства.)
5. Требуйте личного ввода согласованной пары для предотвращения компрометации системы идентификации ответа. (IA-4. Управление идентификаторами | (7) Личная регистрация.)
6. Физически и логически изолируйте систему ответов на запрос согласованной пары и обеспечьте строгий контроль доступа, чтобы защитить систему от взлома. (IA-5. Управление аутентификатором | (6) Защита аутентификаторов.)

Резюме

В этой главе мы рассмотрели проблемы, с которыми сталкиваются командиры, когда им требуется проверить личность солдат и не позволить замаскированным синоби проникнуть в замок. Вы узнали о технике идентификации методом согласованной пары и о том, как синоби использовали ее для обнаружения врага и как обходили во время проникновения. Мы также обсудили современные аналоги этого метода в области компьютерной безопасности, аутентификации и идентификации.

В следующей главе мы поговорим о том, чем двухэтапная аутентификация отличается от согласованных пар, а чем дополняет их.

Я расскажу о скрытой технике аутентификации синоби — двойном пароле, который можно использовать для обнаружения особо хитрых злоумышленников.

5

Двойной пароль

Иногда в качестве пароля можно использовать знаки и жесты, например зажать нос или коснуться уха.

Техника Aikei включает методы татисугури
исугури — передачи паролей жестами.
«Бансэнсюкай», ё-нин II

Трактаты «Бансэнсюкай» и «Гумпо дзиёсю» описывают протокол обнаружения с применением открытой маскировки, предположительно, разработанный самураем Кусуноки Масасигэ [6], жившим в XIV веке. Сигнальные техники татисугури исугури описывают использование жестов, поз или положения тела в качестве секретного механизма аутентификации, повышающего безопасность проверки пароля.

Эти методы в совокупности образуют систему *двойного пароля*, или *двойной печати* [6], предназначенную для выявления замаскированных вражеских синоби, прошедших проверку с помощью украденных паролей, опознавательных знаков и правильных ответных слов.

Рассмотрим классический пример татисугури исугури: к воротам подходит человек в правильной форме и с правильным гербом и желает войти. Не узнав незнакомца, охранник подходит к нему и произносит первую часть парного пароля. Если посетитель свой и знает протокол идентификации татисугури исугури, в ответ он выполнит заранее оговоренное действие — неочевидный сигнал вроде прикосновения к носу или уху, а затем произнесет кодовое слово. Охранник разрешит ему войти только в том случае, если незнакомец отвечает и правильным кодовым словом, и правильным движением (при этом может быть несколько способов реализовать татисугури исугури в зависимости от того, будет охранник стоять или сидеть, но, к сожалению, считается, что эти методы описаны в утерянном трактате «Тейкаирон») [5].

Изящество этой техники состоит в том, что на позу человека обычно никто не обращает внимания. Даже злонамеренный наблюдатель, пытающийся выдать себя за своего, скорее всего, не заметит тайного беззвучного знака. Наблюдатель может увидеть, как 100 человек входят в ворота, используя один и тот же пароль, пока охранник сидит (потому что он их всех узнает), но не заметит, чем отличается взаимодействие, когда охранник стоит. Техника татисугури исугури оказалась довольно успешной, и даже у других синоби не нашлось способов бороться с ней, хотя текст «Бансэнсюкай» гласит, что синоби должен повторять за охранниками все их действия на всех пропускных пунктах, даже если они кажутся бессознательными [5]. По крайней мере, это позволит сбить охранника с толку, и он может подумать, что синоби слегка не в себе или просто глуп. В трактатах также содержится полезный совет для синоби, который не сумел пройти проверку татисугури исугури: «Либо быстро думай и быстро говори, либо беги, спасая свою жизнь» [7].

В трактатах синоби нет явного определения концепции *двойного пароля*, и у меня нет оснований заявлять, что приведенный далее гипотетический пример действительно имел место, но такая иллюстрация мне кажется правдоподобной.

С древних времен для защиты содержимого письма или трактата использовались оттиски печати на воске. В идеале у каждого отправителя сообщения должен был быть уникальный металлический штамп, что позволяло ему оставлять уникальную отметку, тем самым подтверждая подлинность документа. Кроме того, если кто-либо, кроме предполагаемого получателя, откроет письмо или трактат, печать сломается, и это будет расцениваться как вмешательство.

Но шпионы узнали, что с помощью специальных методов нагрева можно слегка размягчить печать, снять ее, не повредив самой печати и бумаги, прочитать содержимое письма, а затем повторно запечатать его или вовсе переставить печать на поддельный документ, содержащий дезинформацию. Для борьбы с нагревом печати со стороны, прилегающей к бумаге, можно было применять двойное запечатывание. Представьте себе, что вместо одного штампа автор письма использует тиски с двумя штампами. Тогда на нижней стороне восковой пластины будет расположена скрытая печать, которую можно будет увидеть, лишь разорвав документ. Если расплавить печать со стороны бумаги, можно сохранить лишь верхнее изображение, но скрытая печать в этом случае будет повреждена, поэтому техника и называется двойной печатью.

Нетрудно понять, почему на случай снятия одиночной печати применялась техника двойной печати и как она помогала обнаружить активность вражеских синоби. В этой главе мы подчеркнем разницу между двухфакторной аутентификацией и двухэтапной аутентификацией. Я также расскажу, как современный аутентификатор второго уровня можно запечатать дважды, чтобы повысить его эффективность. Затем опишу свое видение требований и критериев двойных паролей, а также реализации, в которых используются существующие аутентификаторы и технологии. Я надеюсь, что после выполнения упражнений по теории за́мка и изучения

приведенных примеров реализации двойных паролей вы оцените гениальность Кусуноки Масасигэ и сами опробуете его идеи.

Скрытая двухэтапная аутентификация

Протоколам аутентификации и идентификации в кибермире все чаще требуется дополнительный уровень безопасности поверх пароля. Этот подход называется *двухступенчатой аутентификацией*: то есть на втором шаге требуется, чтобы пользователь выполнил дополнительное действие, например ввел секретный код или нажал кнопку на *постороннем устройстве*, не участвующем в остальном процессе аутентификации. Обратите внимание на небольшое отличие от *двухфакторной* аутентификации, которая применяется для предотвращения доступа злоумышленника к учетной записи с украденными учетными данными.

Секретный код (второй шаг аутентификации) может быть рандомизирован с помощью программных приложений, но обычно он всякий раз генерируется с использованием одной и той же процедуры. К сожалению, ее негибкость дает злоумышленникам возможность обойти защиту двухэтапной аутентификации. Например, обычно код для двухэтапной аутентификации отправляется в виде незащищенного текста или сообщения, которое может быть перехвачено путем клонирования SIM-карты телефона. В этом случае пользователь, который получает код 12345 и вводит его в поле, непреднамеренно сообщает его злоумышленнику. Устройство, применяемое для аутентификации (часто это телефон), может быть украдено, взломано с помощью переадресации звонков, клонировано и использовано злоумышленником. И стороннее устройство, применяемое для двухэтапной аутентификации, тоже может быть украдено и использовано для аутентификации и кражи кодов.

Двухэтапный код, дважды запечатанный с помощью техники татисугури исугури, позволяет сгладить недостатки, присущие процедурам аутентификации. У каждого пользователя должен быть заранее заданный идентификатор татисугури исугури, который для этого пользователя уникален и имеет определенное значение. Например, предположим, что пользователю устно или другим безопасным способом было дано указание поменять местами цифры на цифровой клавиатуре относительно цифры 5. Тогда 1 становится 9, 2 становится 8 и т. д.[1], но применять эту технику следует только в случаях, когда код отображается красным шрифтом, а не зеленым.

Смена цвета — это тот самый безмолвный жест из татисугури исугури, срабатывающий, когда система по каким-то своим критериям считает запрос аутентификации подозрительным: это может быть нестандартное время входа, нераспознанное устройство, незнакомый IP-адрес или другие критерии (чтобы скрыть этот протокол

[1] Поклонники сериала HBO «Прослушка» могут помнить это как код «прыгай через пятерку», взломанный в 5-й серии 1-го сезона.

от злоумышленников, которые могут наблюдать за процедурой аутентификации, следует использовать его нечасто). Теперь, когда свой получит красный код 12345, он будет знать, что ввести нужно 98765, а злоумышленник, укравший учетные данные пользователя, об этом скрытом правиле не знает и введет 12345. Процесс аутентификации остановится, учетная запись будет временно отключена, а сеанс получит ошибку двухэтапной аутентификации. Затем двухэтапный аутентификатор отправит подсказку вида «Используйте протокол аутентификатора № 5», а вместе с ней еще один красный код, например 64831, на который пользователь должен ответить, введя 46279. Еще один неправильный ответ может вызвать повторное предупреждение или полную блокировку учетной записи.

Разработка двойных паролей

Аутентификация с двойной печатью, работающая совместно со стандартными средствами управления авторизацией, должна отвечать следующим требованиям.

1. Применяться только в том случае, если личность пользователя под сомнением, например когда он:
   - входит в систему из иного местоположения, с нового устройства, IP-адреса или в нестандартное время;
   - сообщает о том, что его мобильное устройство украдено или скомпрометировано;
   - теряет резервный токен, код или пароль и запрашивает сброс пароля.
2. Применять внеполосный или сторонний канал связи.
3. Использовать секретную информацию, зависящую от некоторого правила. Каждый пользователь должен иметь возможность настраивать протокол и создавать уникальный набор скрытых правил.
4. Задействовать факторы аутентификации, которые легко понять и запомнить, но сложно угадать.
5. Разрешать применение сразу нескольких защитных правил на случай нескольких повторных ошибок или большого промежутка времени между попытками аутентификации.
6. Применять ограничение, заморозку или блокировку учетной записи, если та после нескольких попыток не сумела пройти аутентификацию. Большинство приложений блокируются после нескольких неудачных попыток ввода пароля, но не блокируются после неудачных попыток двухэтапной аутентификации.
7. Не быть описанной в документах службы поддержки или другой документации. Сотрудникам также не следует вслух упоминать о таких средствах безопасности и правилах их использования.

Популяризация двойных паролей требует от разработчиков, инженеров и пользователей изучения новых технических решений и творческого мышления. Для примера рассмотрим различные варианты ввода, которые могут задействоваться в приложениях с двухэтапной аутентификацией на мобильных устройствах, на которых для подтверждения личности пользователя применяются вопросы, требующие ответа «да» или «нет». Приведем примеры ответов, которые может дать пользователь, увидев тайный сигнал татисугури исугури в приложении с двухэтапной аутентификацией.

1. Пользователь переворачивает экран вверх ногами, прежде чем нажать «да», и приложение в фоновом режиме проверяет ориентацию устройства.
2. Пользователь нажимает кнопки регулировки громкости, устанавливая минимальную или максимальную громкость, а затем нажимает «да». Приложение проверит правильность значения громкости.
3. Пользователь не нажимает «да», пока часы мобильного устройства не перейдут к следующей минуте. Приложение проверит метку времени и сравнит ее ЧЧ:ММ:0*X*, где *X* должно быть менее 3 секунд.
4. Пользователь нажимает «да» с усилием, и приложение проверяет событие сильного нажатия.
5. Пользователь выполняет несколько быстрых нажатий кнопки «да», а приложение проверяет их число.
6. Пользователь выполняет определенный жест — смахивание в какую-либо сторону или вращение, нажимая кнопку «да» на мобильном устройстве, а приложение распознаёт его.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Рассмотрим сценарий, в котором вы — правитель средневекового замка, где хранятся ценности. Вам сказали, что ваши опознавательные знаки, эмблемы, секретные сигналы и другие методы идентификации были раскрыты вражеским синоби и теперь он может проникнуть в замок. Вы даже начали менять пароли и знаки три раза в день, но вам говорят, что синоби отслеживают все изменения, хоть и неизвестно, как именно.

Подумайте, как вы можете использовать татисугури исугури, чтобы поймать вражеских синоби. Можно ли создать небинарные татисугури исугури, то есть более сложные скрытые правила, чем сидение или стояние? Как защитить процесс аутентификации татисугури исугури и не дать вражеским синоби раскрыть его? Как совместить разные правила татисугури исугури и проверить, кто из ваших солдат сливает информацию?

Рекомендуемые меры безопасности и предосторожности

Рекомендации следует оценивать с учетом концепции двухэтапной аутентификации (с двойной печатью).

1. Применяйте внеполосную аутентификацию (Out-of-Band Authentication, OOBA) через отдельный канал связи для проверки того, что запросы аутентификации исходят от проверенных пользователей. (IA-2. Идентификация и аутентификация | (13) Внеполосная аутентификация.)
2. Убедитесь, что сотрудники не распространяются о существовании скрытых правил двухэтапной аутентификации. (IA-5. Управление аутентификатором | (6) Защита аутентификаторов.)
3. Задействуйте несколько правил с двойной печатью для придания татисугури исугури динамики. (IA-5. Управление аутентификатором | (7) Неиспользование статических аутентификаторов.)
4. Реализуйте внеполосную передачу и задайте правила с двойной печатью для сохранения конфиденциальности. (SC-37. Внеполосные каналы.)
5. Аккуратно составляйте сообщения об ошибках в случае неудачной аутентификации, чтобы они не раскрывали информацию о пароле и не наводили на мысль о том, как обойти защиту. (SI-11. Обработка ошибок.)

Резюме

В этой главе вы узнали о методе аутентификации, используемом для защиты синоби, который называется *паролем с двойной печатью*, или *татисугури исугури*. Мы рассмотрели различие между факторами и этапами аутентификации. Затем кратко проанализировали критерии хорошего аутентификатора татисугури исугури и привели несколько примеров.

В следующей главе мы обсудим концепцию под названием *часы проникновения*. Вы узнаете, как выбирать время суток, когда наиболее велика вероятность проникновения. Понимание зависящих от времени возможностей может помочь вам выбрать, когда стоит внедрять или запускать аутентификаторы татисугури исугури. К примеру, вы можете запускать их только в определенные часы или в определенные даты, чтобы свести к минимуму использование татисугури исугури и сохранить методику в секрете.

6

Часы проникновения

Подождав до часа Быка, ниндзя понял, что стражник заснул, воцарилась мертвая тишина, а пламя факела погасло, уступив место кромешной тьме.

Для синоби важно знать правильное время для атаки.
Всегда следует выбирать момент, когда противник
устал или утратил бдительность.
«Ёсимори хяку-сю», № 5

При планировании кражи, шпионажа, саботажа, убийства или иного нападения синоби не думает о честной игре по правилам. Даже наоборот, он тщательно продумывает наиболее «выгодный момент и позицию» [7] для нанесения удара. Трактат «Сёнинки» подчеркивает важность выбора момента проникновения, пока цель отвлеклась, невнимательна, склонна к поспешным суждениям, пьяна или просто устала. В «Ёсимори хяку-сю» в стихотворении 63 говорится, что усталость «могла быть причиной серьезной ошибки» [6]. Синоби с особым вниманием отслеживали такие моменты и часто проникали в лагерь в момент, когда враг рубил деревья, занимался обустройством лагеря, был уставшим после боя или менял охрану [7].

Изучая поведение своих врагов, синоби замечали, что в стандартном распорядке дня сами собой возникают окна возможностей для атаки. В трактатах день делится на двухчасовые блоки, и рекомендуется планировать проникновение во время блоков, которые, как правило, совпадают с фазами бодрствования, еды и сна. Наиболее подходящий час зависит от типа атаки. Ночные атаки, например, лучше всего предпринимать в часы Кабана (21:00–23:00), Крысы (23:00–1:00) и Зайца (5:00–7:00) [7].

Кроме того, в «Бансэнсюкай» отмечается, что некоторые генералы верили в счастливые дни [7], которые предсказывали китайские гороскопы. Считалось, что в эти даты боевая операция непременно увенчается успехом. Если синоби удавалось выяснить, что командир склонен к подобным суевериям, он мог использовать эту

информацию, чтобы, например, предугадывать передвижения войск, зная, какой день командир считал удачным или неудачным для начала похода. Когда модель поведения становится предсказуемой, в ней мало что меняется. В этой главе мы обсудим, как злоумышленники могут выбирать более удачное время для нападения в киберпространстве.

Время и возможности

Поскольку люди до сих пор просыпаются, работают, едят, отдыхают и спят приблизительно по тому же графику, что и феодальные японцы, то и часы проникновения, которые предлагается использовать в трактатах, точно совпадают с моментами времени, когда сотрудники отвлекаются, утомляются или теряют концентрацию из-за проблем современного рабочего дня, — именно тогда они наиболее уязвимы для нападения. Рассмотрим временны́е блоки, указанные в трактатах, в контексте использования сети и информационной системы.

- **Час Зайца (5:00–7:00).** Пользователи просыпаются и входят в систему. Автоматические и ручные системы загружаются, появляются скачки в журналах событий и системных журналах.
- **Час Лошади (11:00–13:00).** Многие пользователи прерываются на обед, то есть выходят из системы сами или отключаются автоматически из-за бездействия. Возможно, кто-то занимается личными делами с помощью интернета — читает новости, делает покупки, проверяет почту, выкладывает что-то в социальные сети или делает еще что-то, что может вызвать срабатывание систем обнаружения аномалий.
- **Час Петуха (17:00–19:00).** Пользователи заканчивают работу, сохраняют файлы и, вероятно, спешат уйти домой, что значительно увеличивает риск допустить ошибку в своей работе, а также снижает бдительность в области кибербезопасности. Например, работник может бездумно открыть вложение из срочного письма. Пользователи массово выходят из своих учетных записей, а некоторые не выходят, оставляя систему на произвол судьбы или тайм-аута.
- **Час Кабана (21:00–23:00).** Большинство пользователей не на работе. Когда человек дома, общается с друзьями или готовится ко сну, безопасность рабочей учетной записи, скорее всего, его мало волнует. Организации с достаточным штатом для работы ночью обычно в это время меняют смену, создавая окно для атак злоумышленников, которые могут проникнуть в систему между входами разных пользователей или пока пользователи SOC только заходят в систему. Чем позже, тем больше вероятность того, что люди, даже привыкшие к ночной работе, будут сонными и невнимательными, особенно если ничего интересного не происходит.

- **Час Крысы (23:00–1:00).** Сети и системы выполняют резервное копирование или другое плановое обслуживание, создавая шум в сетевых датчиках и SIEM. Пользователи SOC к этому моменту наверняка уже выполнили свои повседневные задачи по обеспечению безопасности и техническому обслуживанию и могут быть погружены в работу над проектом.
- **Час Тигра (3:00–5:00).** В это время обычно выполняются пакетные задачи, включая обработку журналов, запуск диагностики или сборки программного обеспечения. Большинство пользователей, за исключением сотрудников SOC, спят самым крепким сном и неактивны в своих учетных записях.
- **Удачные дни.** Существуют определенные дни, недели и месяцы, в которые злоумышленники могут атаковать системы и пользователей. Большинство руководителей компаний не руководствуются «удачными днями» в своей работе, но злоумышленники наверняка осведомлены о регулярных плановых обновлениях или обслуживании, когда компании отключают средства защиты, а также о выходных и праздничных днях, когда системы и учетные записи в основном не используются. Если потенциальные угрозы не учесть, нарушения в сетевом трафике и системных журналах могут остаться незамеченными во время таких окон возможностей, позволяя злоумышленникам проводить атаки, осуществлять разведку или управление, распространять вредоносное ПО или извлекать данные.

Разработка мер безопасности и детекторов аномалий с учетом временны́х особенностей

Вы можете использовать информацию о часах проникновения синоби и разработать систему безопасности, учитывающую время и состояние сети в разные моменты времени, отклонения от базового состояния и бизнес-требований. Организация подобных мер безопасности состоит из трех этапов.

1. Определить базовый уровень активности на каждый час.
2. Обучить сотрудников контролировать свою деятельность и ознакомить их с типичной сетевой активностью в их рабочие часы.
3. Оценить бизнес-потребности на каждый час. На основе этой оценки выработать бизнес-логику и аксиомы безопасности для дальнейшей защиты от угроз и обнаружения аномалий.

Во-первых, рассмотрите возможность разделения сетевых и системных журналов на сегменты длиной в один-два часа. Просмотрите историю работы и уровни активности вашей сети и систем, определите базовый уровень и критическую отметку, после которой нужно начинать поиск угроз и выявление проблем. Обратите особое

внимание на время атак и наиболее благоприятные для них моменты, которые определяются особенностями организации, моделированием угроз и опытом.

Когда данные были сегментированы и сопоставлены с базой, обучите аналитиков, системных администраторов и специалистов по безопасности, чтобы они хорошо ориентировались в паттернах активности, характерных для вашей сети. Они также должны знать о том, какие проблемы с безопасностью возникают из-за организационных процедур. Трактаты синоби инструктируют охранников: во время пересменки следует тщательно проверять каждую шероховатость и любые отклонения от нормы. Предполагается, что охранник должен обратить внимание на то, что рыбак прибыл позже обычного или незнакомая птица кричит в необычный час. Сотрудники службы безопасности, нацеленные на обнаружение подобных аномалий, должны более внимательно изучить аномальное событие, что может помочь в обнаружении инцидента с безопасностью. Для получения сотрудниками службы безопасности опыта такой работы можно дать им поручение выполнять мониторинг сектора (например, отдельной системы, которая считается вероятной целью), очень хорошо с ней ознакомиться, а затем просматривать журналы и события из этой системы за каждый двухчасовой период в течение восьмичасовой смены. Эта стратегия резко контрастирует с тактикой «постоянно все контролировать», которой придерживаются большинство SOC и которая вызывает утомление, перегрузку и выгорание. Такой метод позволяет также смягчить проблемы многих автоматизированных систем обнаружения аномалий, в которых человек должен отслеживать каждую аномалию, отзываться на них и расследовать инциденты. Такие системы быстро начинают генерировать огромный объем данных, контролировать который становится невозможно, а сотрудники и без того загружены.

Обратите внимание на то, что журналы, в отличие от шорохов в ночи, вполне осязаемы и доступны для дальнейшего анализа. Вполне вероятно, что хитроумный злоумышленник сможет подделать или удалить журналы безопасности, отфильтровать трафик от сетевых ответвителей и датчиков или иным образом скомпрометировать системы, предназначенные для регистрации деятельности и защиты от вторжений и предупреждений. Однако эти действия должны нарушить нормальное поведение системы, а этого достаточно для того, чтобы проницательный аналитик заметил инцидент.

Затем нужно будет задать себе два вопроса.

- Когда ваши пользователи и системы активны?
- Когда может быть активен злоумышленник?

Понимание того, как и когда пользователи входят в систему и что они там делают, позволяет стратегически ограничивать доступ, затрудняя проникновение извне или изнутри в наиболее опасные моменты. Например, если система не используется

с 20:00 до 8:00, ее можно выключить. Если у пользователей нет бизнес-необходимости в доступе к системе по субботам, отключите доступ для всех пользователей в этот день. Отключение систем в запланированное время также помогает обучить сотрудников SOC обнаруживать аномалии в определенные часы, поскольку в этом случае им придется проверять меньше явлений. Стандарты NIST предлагают внедрять подобные средства контроля доступа, но многие организации предпочитают сценарии, обеспечивающие удобство работы в чрезвычайных ситуациях, какими бы маловероятными они ни были.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Пусть вы — правитель средневекового замка, где есть ценная информация, сокровища и люди. Вы получаете достоверные сведения о том, что синоби планирует проникнуть в ваш замок. Представьте, что ваши охранники прекрасно знают, когда это должно произойти, но подчиняются следующим правилам:

- любые ворота или двери (внутренние и внешние) можно запереть и отпереть в определенное время;
- введен комендантский час, когда любой, кто будет обнаружен на улице, будет задержан.

Подумайте, какого уровня целостности, уверенности и безопасности можно достичь с помощью этих правил. Как бы вы обучили жителей замка действовать в рамках этих ограничений (как им пользоваться уборными ночью, убирать помещения, пока другие спят, принимать ночные роды и т. д.)? На какие компромиссы можно пойти, чтобы введенные вами меры безопасности работали?

Для выполнения этого упражнения полезно будет нарисовать карту воображаемого замка или вашего офисного здания. Как вариант, вместо здания можете использовать абстрактную компоновку вашей сетевой карты или диаграммы потоков данных (DFD), где коммутаторы — это коридоры, маршрутизаторы / межсетевые экраны — двери, системы — комнаты, а VPN / точки выхода — ворота.

Рекомендуемые меры безопасности и предосторожности

В некоторых случаях можно использовать рекомендации и меры безопасности, приведенные в стандарте NIST 800-53. Это следует делать с учетом часов проникновения. (Обратите внимание: здесь нужно, чтобы у журналов и предупреждений были отметки времени, а время во всех системах было синхронизировано. См. AU-8. Отметки времени.)

1. Оцените часы работы и смоделируйте угрозы. Когда вы наиболее уязвимы для атак? Как вы можете обучить и подготовить своих сотрудников? (NIST SP 800-154. Руководство по ориентированному на данные моделированию системных угроз.) [36]
2. Внедрите для учетных записей управление привилегиями на основе времени, зависящее от деловых и операционных потребностей пользователей. Например, можете ограничить для определенных сотрудников возможность отправлять и получать электронную почту после 19:00. (AC-2. Управление учетными записями | (6) Динамическое управление привилегиями.)
3. Ограничьте возможность входа или использования определенных учетных записей в определенные часы. Например, при попытке выполнить несанкционированные действия над неактивной учетной записью между 21:00 и 23:00 следует немедленно попросить пользователя подтвердить свою личность. Если он не отвечает или не сумел пройти аутентификацию, нужно уведомить службу безопасности. (AC-2. Управление учетной записью | (11) Условия использования.)
4. Задействуйте системы эвристического анализа для обнаружения аномального доступа к системе или шаблонов использования, нехарактерных для данного периода времени. Пользователи должны добровольно задокументировать или иным образом описать свой типичный паттерн, чтобы помочь смоделировать свое обычное поведение в течение рабочего дня (AC-2. Управление учетной записью | (12) Мониторинг типичного использования учетной записи.).
5. Требуйте от владельцев и пользователей систем документировать периоды времени, когда системы должны использоваться, а когда их можно отключать. (AC-3. Обеспечение доступа | (5) Информация, важная для безопасности.)
6. Сократите временны́е рамки для деятельности злоумышленников. Определите стратегическую политику предприятия, согласно которой конфиденциальная или служебная информация должна быть доступна только в установленное время, например с 11:00 до 15:00 в будние дни. (AC-17. Удаленный доступ | (9) Отключение доступа.)
7. Сообщайте владельцу учетной записи об удачных или неудачных входах в систему, включая время и дату последнего входа. Отслеживание этой информации помогает пользователю предупредить службу безопасности, если его учетная запись была взломана, и сообщить о несанкционированном доступе. (AC-9. Уведомление о предыдущем входе в систему (доступ) | (4) Дополнительная информация для входа.)
8. После определения рабочих часов настройте пользовательские устройства и системы на автоматическую блокировку и завершение всех сеансов в указанное время. (AC-11. Блокировка сеанса.)

9. Задокументируйте политику, согласно которой назначаются время и даты, когда разрешено изменять инфраструктуру и системы. Это помогает SOC оценивать изменения сети и конфигурации в зависимости от времени. (AU-12. Создание аудита | (1) Общесистемный и временной корреляционный след; CM-5. Ограничения доступа для изменений.)

Резюме

В этой главе вы узнали о традиционном японском разделении суток на часы, названные в честь зодиакальных животных, о влиянии китайской астрологии на поведение и о том, как синоби, вероятно, использовали все это, чтобы проникнуть во вражеский лагерь или перехитрить противника. Вы рассмотрели, как сетевая активность зависит от времени суток и как уменьшить вероятность атаки с помощью управления на основе времени. Вы познакомились со стандартом безопасности синоби. В частности, узнали, что в своей зоне ответственности охранник должен был заметить малейшее несоответствие — все, что могло указывать на присутствие противника. Кроме того, вы ознакомились с руководством по применению некоторых из этих концепций к процедурам поиска угроз, процессам достижения операционной безопасности и системам обнаружения аномалий.

В следующей главе мы рассмотрим применение «временно́й конфиденциальности», то есть хранения информации о времени в секрете от вредоносных программ, что может позволить защитникам использовать определенные варианты их обнаружения и защиты от них.

7

Доступ к данным о времени

Начинать атаку нужно не заранее и не с опозданием, а точно в срок.

Если вы собираетесь поджечь замок или лагерь врага,
вам нужно заранее согласовать время поджога
со своими союзниками.
«Ёсимори хяку-сю», № 83

Во время миссий синоби, особенно ночных, одна из самых важных и сложных задач заключалась в отслеживании времени. И если вы не видите в этом проблемы, то вспомните, что у синоби не было часов. До начала 1600-х годов не было даже песочных часов [5]. Чтобы вовремя получать и отправлять сигналы, координировать атаки и знать, когда противник уязвим, синоби пришлось разработать методы, позволяющие надежно определять время.

Исторически сложилось так, что один из способов измерения времени заключался в зажигании благовоний или свечей, горящих с постоянной скоростью, в ходе чего синоби через определенные промежутки времени звонил в колокольчик, чтобы сообщить, сколько времени прошло. «Бансэнсюкай» рекомендует для определения времени использовать сигналы окружающей среды, такие как движение звезд, или весовые инструменты [5]. В качестве весовых инструментов применялись водяные часы, иногда называемые *клепсидрами*, в которых для определения временны́х интервалов использовались весы и струя воды. В других трактатах описываются более сложные параметры, такие как отслеживание изменений радужной оболочки кошачьего глаза на протяжении дня или неуловимого теплового расширения дома в течение ночи, поскольку оно соответствует определенным часам [7]. Синоби даже учили определять время из информации о том, через какую ноздрю он дышал более активно. В трактатах объясняют, что мы дышим по большей части одной ноздрей, а затем другой, при этом ноздри сменяются через равные промежутки времени, которые можно использовать для измерения. Это может показаться притянутым

за уши, но в 1895 году немецкий ученый Ричард Кайзер выполнял наблюдения и задокументировал, что в течение дня кровь скапливается на разных сторонах носа человека, вызывая заметное уменьшение потока воздуха в одной из ноздрей, а затем то же самое повторяется с другой ноздрей [32]. Мало того что наблюдательные синоби обнаружили это явление более чем за 300 лет до его описания западным ученым, они применяли его на практике. Например, синоби мог прятаться под полом, где нельзя зажечь свечи или благовония, использовать инструменты для отслеживания времени или даже открывать глаза, чтобы их блеск не привлек внимания через щели в полу. В этом случае он лежал неподвижно и следил за своим дыханием, пока не наступало время атаки. Это фантастический пример дисциплины, изобретательности и креативности синоби.

Множество упоминаний работы с временем и описанные в трактатах синоби сложные методы его отслеживания наводят на мысль о том, что они не были бы разработаны, если бы время не было решающим фактором в эффективной работе злоумышленника. Повсеместное распространение дешевых, простых и надежных способов определения времени в современном обществе давно заставило нас воспринимать время и его измерение как должное.

В этой главе мы по-другому взглянем на важность времени в цифровых системах, а также кратко рассмотрим, как оно генерируется, используется и защищается в существующих передовых практиках. Затем зададим вопрос: если для противника так важно точное время, то как мы можем скрыть от него эту информацию или вовсе помешать ему узнать время? А может, даже обмануть его, сообщив неточное время?

Важность времени

Время необходимо для работы практически всех современных компьютерных систем. Синхронизируя последовательную логику и генерируя тактовый сигнал, который определяет время работы функций, компьютеры устанавливают конечные импульсы времени.

Эти импульсы похожи на тиканье часов, по которым работает стабильная и надежная среда ввода/вывода. Обширные, сложные сети и системы, которые управляют работой правительства, экономикой, бизнесом и личной жизнью, работают на этих импульсах, непрерывно запрашивая время. Без часов это все не действовало бы.

Для защиты данных о времени принимаются многочисленные меры безопасности. Проверка подлинности на серверах протокола сетевого времени (NTP) позволяет установить, что злоумышленник не подделывает данные системы о времени. Также используются шифрование и контрольные суммы. Шифрование позволяет защитить обмен данными, а контрольные суммы служат для обнаружения ошибок,

возникших в процессе их передачи. По данным времени NTP-сервера проверяется целостность данных и они защищаются от несанкционированного доступа. Иногда применяется произвольное рандомизированное число, которое прибавляется к времени передачи для предотвращения ошибок повторной передачи. Отметки времени и журнал синхронизации времени позволяют сравнивать системное время с данными, полученными у доверенного источника времени. NTP сохраняет доступность и отказоустойчивость за счет использования нескольких источников времени и альтернативных методов распространения, а если доступ к NTP оказывается закрыт, методы резервного копирования позволят точно оценить время по данным последней синхронизации. Существуют и другие передовые методы безопасности, такие как использование записей аудита с отметками времени, блокировка сеансов в случае бездействия, ограничение доступа к учетным записям в зависимости от времени суток.

Все перечисленные средства управления защищают целостность и доступность данных о времени, однако их секретности часто уделяется недостаточно внимания. Практически любое современное приложение может в любой момент запросить время, и как правило, ему будет разрешен доступ не только к дате и времени, но и к библиотекам и функциям часов. NTP позволяет шифровать временны́е данные, которые передает в систему, но все же контроля над ограничением доступа к текущему системному времени пользователю заметно не хватает. Важно определить эту проблему заранее, потому что время — это критически важная информация, которую злоумышленники применяют для распространения вредоносного ПО. Например, программа Shamoon [44], которая распространялась в Саудовской Аравии, должна была запускаться в начале уикенда, чтобы нанести максимальный урон. Ее целью было стереть все зараженные системы до того, как кто-либо это заметит.

Атаки бывают нацелены также на раскрытие конфиденциальной информации, создание условий гонки, принудительные блокировки, манипулирование состояниями информации и использование временны́х данных для расшифровки криптографических алгоритмов. Более сложные вредоносные программы могут задействовать свой доступ ко времени для:

- временной приостановки деятельности, чтобы избежать обнаружения;
- измерения первых 10 млн цифр числа пи, чтобы подсчитать время вычисления и определить, находится ли зараженная система в песочнице или в среде детонации, предназначенной для обнаружения вредоносных программ;
- связи с командным интерфейсом компьютера с помощью специальных команд, связанных со временем;
- анализа метаданных и другой информации с помощью временны́х атак, определения состояния, положения и возможностей целевой системы.

Если же администратор запрещает программе доступ к данным о времени (локальном, реальном и линейном), работа с целевой информационной системой может стать для злоумышленника более трудной или вовсе невозможной.

Но тут важно отметить, что массовое ограничение доступа приложений ко времени, скорее всего, приведет к каскадным сбоям и ошибкам. При решении этой задачи необходим тонкий подход.

Держите время в тайне

Имейте в виду: поскольку конфиденциальностью временных данных обычно занимаются не так активно, как другими формами временной безопасности, ее применение потребует особых усилий со стороны вашей организации и сообщества в целом.

Определите базовый уровень

Определите имеющиеся в вашей среде программное обеспечение, приложения, системы и административные команды, которым требуется доступ ко времени. Реализуйте перехват функций (перехват вызовов функций) и ведение журнала, чтобы определить, кто и что запрашивает данные о времени. Определив базовый уровень, используйте его для обнаружения лишних запросов данных о времени и определения связанных с ним потребностей, что в дальнейшем позволит применить дополнительные меры безопасности, например Just in Time (JIT).

Оцените технические возможности

Обратитесь к производителям оборудования и поставщикам программного обеспечения, чтобы определить, какие технические средства позволили бы вам ограничить доступ к функциям времени. Если таких средств нет, запросите внедрение новых функций и простимулируйте разработку решений в этой области.

Установите политики

Ограничение доступа к данным о времени относится к нетрадиционным мерам безопасности, но как и в случае с более привычными мерами контроля, принудительное исполнение требует установления стратегической политики, в которой были бы описаны требования к ограничению доступа к данным времени и отслеживанию попыток получить его. По возможности концепцию конфиденциальности времени стоит включать во все решения по управлению изменениями, в закупки нового оборудования и программного обеспечения, а также учитывать при расстановке приоритетов SOC.

Официально задокументируйте новые политики и добейтесь их одобрения директором по информационной безопасности вашей компании.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Вам сообщили достоверную информацию о том, что в замок проник синоби с приказом поджечь его ровно в 3:00. Ночью стражник в башне отмеряет время с помощью свечей и каждые 120 минут бьет в колокол, чтобы другие ночные стражи также были в курсе, но этот звук, как вы полагаете, услышат и синоби.

Как можно проконтролировать доступ ко времени, чтобы снизить опасность этой угрозы? Каким доверенным лицам в вашем замке требуется доступ ко времени, а кому полный доступ можно не давать? Какие действия вы можете предпринять, чтобы предотвратить атаку или обнаружить синоби, используя только информационный контроль над временем?

Рекомендуемые меры безопасности и предосторожности

1. Реализуйте средства защиты, которые блокируют доступ к данным о времени в различных журналах. Организация защиты от утечек данных о времени или временных меток может потребовать физического, экологического, медийного и технического контроля. (AU-9. Защита информация об аудите.)
2. Изучите существующую информационную архитектуру и работу со временем, реализованную в ней, включая философию, требования и тактики, необходимые для реализации контроля доступа и конфиденциальности временны́х данных в вашей среде. Если заинтересованные стороны согласны с вводимыми ограничениями по времени, задокументируйте их в плане безопасности и утвердите выделенные на реализацию бюджет, ресурсы и время. (PL-8. Архитектура информационной безопасности.)
3. Просмотрите журналы и проведите исследования для обнаружения соединений через порт 123 с любыми неофициальными серверами NTP. Ищите NTP-связь с внешними NTP-серверами и рассмотрите возможность блокировки доступа к NTP-серверам, которыми вы не управляете. (SC-7. Граничная защита.)

Резюме

В этой главе мы узнали об инструментах, которые синоби использовали для определения времени, и о том, как им помогало знание времени. Мы обсудили, насколько важным может быть время для кибероперациий и безопасности, и отметили, что современные методы обеспечения безопасности сосредоточены в первую очередь на доступности и целостности данных о времени. Мы привели упражнение на тему того, как избежать атаки синоби с помощью манипуляции временем.

В следующей главе обсудим, как синоби превращают различные вещи в инструменты для выполнения задач. Понимание принципов работы аналогичных цифровых инструментов может помочь вам обезопасить себя от нового оружия, которое можно выковать из таких инструментов, или по крайней мере воспрепятствовать его использованию.

8

Инструменты

Обязательно дождитесь шума ветра, чтобы скрыть любой звук извлечения инструмента ниндзя.

Независимо от того, сколько инструментов вы носите при себе, помните прежде всего, что еда всегда должна быть у вас на поясе.
«Ёсимори хяку-сю», № 21

В голливудских фильмах ниндзя обычно носят с собой сюрикены или катану, но настоящие синоби разработали огромный набор инструментов и оружия и скрупулезно подходили к выбору правильного инструмента для работы [6]. Во всех трех трактатах синоби особое внимание уделяется применению секретных инструментов, многие из которых были для своего времени поистине инновационными. В одном только «Бансэнсюкай» пять объемных томов об инструментах. В нем в числе прочего говорится что лучшие инструменты для различных целей обычно тихие и негромоздкие [5]. «Сёнинки» советует синоби ограничить количество имеющихся при себе инструментов, поскольку неуместные предметы часто вызывают подозрения [7]. Трактат также рекомендует синоби находить и уничтожать инструменты и оружие своих противников. Все это имело решающее значение для успешного выполнения миссии синоби [7].

Разумеется, синоби не приобретали инструменты в супермаркете товаров для синоби. Вместо этого, следуя указаниям трактатов, они превращали в эффективное оружие предметы, которые легко можно было купить, найти или изготовить. У этого подхода несколько преимуществ. Невзрачные бытовые предметы можно носить с собой, не вызывая особых подозрений [5], а иногда они и вовсе могли служить для маскировки синоби. К примеру, несколько правителей, в том числе Тоётоми Хидэёси и Ода Нобунага, вводили «охоту на мечи» — массовую конфискацию всех мечей

и другого оружия у мирных жителей, чтобы снизить риск нападения повстанцев на армию [42]. Все люди, не являвшиеся самураями, могли лишиться оружия. Чтобы обойти запрет, синоби незаметно модифицировали обычные сельскохозяйственные инструменты, чтобы использовать их в качестве оружия, поскольку указов против ношения острого сельскохозяйственного инвентаря в общественных местах не существовало. В руках обученных синоби повседневные сельскохозяйственные орудия становились смертоносными.

«Бансэнсюкай» утверждает, что при использовании инструментов важно не просто владеть ими, но и хорошо понимать их предназначение [5]. Синоби часто размышляли о полезности своих инструментов, постоянно тренировались с ними и переосмысливали их применение в полевых условиях. Благодаря этому синоби постоянно улучшали существующие инструменты, изобретали новые и передавали эти знания другим союзным синоби [5].

В этой главе мы поговорим именно об инструментах. Мы коснемся их двойственной природы и узнаем, как один и тот же инструмент может творить добро или зло в зависимости от того, кто им пользуется. Такая двойственная модель *ин-йо*, или *инь-ян*, полезна для понимания того, как хакер работает с цифровыми инструментами. Например, подумайте, как инструмент, созданный для помощи пользователю, может быть применен для злодеяния.

Помимо возможности «хорошего» и «плохого» применения каждый инструмент можно задействовать для разных целей. Попробуйте придумать, например, с десяток способов использования молотка. Подобные простые упражнения помогут вам лучше понять, что такое молоток, как его можно было бы улучшить или как изобрести новый тип молотка и получить что-то новое. Схожие творческие навыки можно применять для перекодирования цифровых и программных инструментов. У настоящего мастера такое творческое перепрофилирование аналогично работе мастера-кузнеца. Кузнец способен создавать новые инструменты, приспособления и системы, которые могут кардинально изменить его понимание собственного ремесла, тем самым открывая новые возможности и расширяя горизонты разработки нового оружия, средств защиты и инструментов.

Вероятно, состязательное изобретение инструментов невозможно искоренить. Тем не менее в этой главе я опишу лучшие практики безопасности для инструментов, а также некоторые средства управления, которые помогут смягчить последствия атак.

Довольствуемся тем, что есть

В кибербезопасности *инструментами* называются какие-либо средства, которые помогают выполнять задачи вручную или автоматически. Если это определение

звучит слишком широко — что ж, так оно и есть. Существуют физические инструменты, такие как BadUSB, вайфай-снифферы и «отмычки», а также программные инструменты, такие как платформы, эксплойты, код, сценарии и исполняемые файлы. Вся компьютерная система сама по себе является инструментом. Даже применяемый законно инструмент в руках хакера может стать оружием. Представьте, например, клиент SSH, который администратор использует для удаленного обслуживания систем, а злоумышленник — для обратного туннелирования SSH и атаки на системы в обход межсетевых экранов.

Как и синоби, киберпреступникам для достижения целей важны подходящие инструменты, и они постоянно развивают, настраивают, оттачивают и тестируют их на соответствие целям и технологиям на живых примерах. Продвинутые преступники нанимают разработчиков инструментов и возможностей, которые занимаются поддержкой и развитием набора инструментов. В ответ на это предприимчивые специалисты по безопасности изучают методом обратной разработки эти специальные инструменты, создают контрмеры, внедряют полезные политики безопасности и сигнатуры обнаружения, тестируют возможности вредоносных инструментов в песочницах и создают белые списки приложений, которые выявляют и блокируют опасные инструменты. Иногда вновь изобретенные средства защиты настолько хороши, что злоумышленникам не удается загрузить или установить свои инструменты в целевую систему, поскольку система безопасности на хосте немедленно изолирует их, блокирует доступ к ним и предупреждает сотрудников службы безопасности об инциденте.

Поскольку системы безопасности на хостах способны обнаруживать и блокировать специализированные инструменты и вредоносное ПО, многие злоумышленники начали использовать тактику проникновения, называемую «довольствуйся тем, что есть». В рамках этого подхода они сначала собирают информацию о программном обеспечении и инструментах, которые уже применяются в целевой системе. Затем планируют атаку, задействуя только установленные приложения, поскольку защита хост-системы не считает их вредоносными.

В такой атаке может использоваться любой файл на компьютере жертвы, будь то планировщик задач, веб-браузер и система управления Windows, утилиты командной строки, механизмы сценариев, такие как cmd/bat, JavaScript, Lua, Python и VBScript. Хакеры используют имеющиеся в целевой среде инструменты так же, как синоби применяли сельскохозяйственные орудия, которые легко раздобыть и пустить в ход, не вызывая подозрений. Хакеры с помощью имеющегося на целевой машине инструментария способны превратить повседневные пользовательские и административные инструменты, приложения и файлы операционной системы в средство для реализации своих целей.

Одним из самых распространенных инструментов, который часто используют на компьютерах с Windows, является фреймворк Microsoft PowerShell. Даже в Microsoft

признают, что злоумышленники регулярно применяют именно PowerShell, чтобы проникать в системы, выполнять несанкционированные действия и иным образом угрожать работе компании. В ответ на это Microsoft предлагает средства безопасности и смягчения последствий, такие как Privilege Access Management (PAM), для обеспечения Just Enough Administration (JEA) в сочетании с администрированием Just in Time (JIT). Беда в том, что JEA/JIT превращает использование PowerShell в сущий кошмар для системных администраторов. А почему? Если не углубляться в технические детали, просто представьте, что для устранения какой-то проблемы вызвали специалиста, но ему разрешено взять с собой только отвертку и лишь в промежуток с 13:00 до 14:00.

Контроль доступа в виде блокировки инструментов работает правильно только в том случае, если ИТ-отдел согласен серьезно ограничить свою эффективность. Но даже в этом случае опасность не исчезает, если эти инструменты уже установлены в целевой системе. Специалисты по кибербезопасности не раз видели, как злоумышленники с легкостью извлекают нужные инструменты из локальной среды. Важный постулат кибербезопасности заключается в следующем: пока существуют сложные инструменты, существует и возможность злоупотребления ими.

Инструменты для защиты

Парадокс наличия инструментов в том, что без них вы не можете работать, но и хакеру они нужны. Один из подходов к решению этой проблемы — свести к минимуму количество инструментов, их функционал и доступность. Эта стратегия несколько затруднит вам работу, но при наличии адекватных мер безопасности потенциальному противнику станет *еще труднее*. Одним из недостатков этого подхода является то, что вы снижаете отказоустойчивость и надежность средств удаленного управления средой. Таким образом, если злоумышленник скомпрометирует важные инструменты, удалив или испортив их, ваши собственные средства защиты ограничат ваши возможности по управлению системой и восстановлению ее работоспособности. Работу с защитными инструментами можно начать вот с чего.

1. **Определите базовый уровень.** Проведите опрос сотрудников в зависимости от их роли и инвентаризацию программного обеспечения во всех системах вашей организации. Составьте список пользователей, номера версий и расположение каждого инструмента в вашей среде, включая все программное обеспечение/приложения, сценарии, библиотеки, системы

и роли. Сюда относятся даже встроенные в ОС средства, такие как перечисленные далее.

sc.exe	find.exe	sdelete.exe	runasuser.exe
net.exe	curl.exe	psexec.exe	rdpclip.exe
powershell.exe	netstat.exe	wce.exe	vnc.exe
ipconfig.exe	systeminfo.exe	winscanx.exe	teamviewer.exe
netsh.exe	wget.exe	wscript.exe	nc.exe
tasklist.exe	gpresult.exe	cscript.exe	ammyy.exe
rar.exe	whoami.exe	robocopy.exe	csvde.exe
wmic.exe	query.exe	certutil.exe	lazagne.exe

2. **Проанализируйте результаты и оцените свои потребности.** Рассмотрите все инструменты, чтобы определить, какие из них нужны пользователям, а какие нет, а также то, где и когда их применяют. Для каждого инструмента оцените риск и определите вред, который может возникнуть, если злоумышленник получит к нему доступ. Задокументируйте, как можно ограничить возможности инструмента для повышения безопасности, но не в ущерб для бизнес-операций. Компромиссом может быть, например, отключение макросов в Microsoft Word и Excel.
3. **Примените ограничения.** Ограничьте доступность и авторизацию для слишком рискованных инструментов. Задокументируйте любые исключения и запланируйте их пересмотр раз в квартал, чтобы доступ продлевался лишь по запросу пользователей. Можете даже установить временный доступ, чтобы возможность применить инструмент автоматически ограничивалась через определенное время. Создайте белый список одобренных инструментов, чтобы любые нераспознанные или неавторизованные инструменты в систему не попадали. Рассмотрите возможность физической блокировки всех USB, съемных носителей, Thunderbolt, FireWire, консолей и внешних портов на всех системах и открывайте доступ к ним только по одобренному заявлению пользователя.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. В вашем замке производятся редкие запатентованные нитки, необходимые для изготовления и ремонта текстильных изделий. Они очень хорошо и дорого продаются, и на доход с продажи вы обеспечиваете свои владения. Вы получаете достоверную информацию о том, что синоби планирует проникнуть в ваш замок и отравить иглу на веретене, хоть и неясно, кто именно должен стать жертвой.

Смоделируйте сценарии угроз, в которых кто-то может уколоться острием веретена. Затем разработайте меры по снижению вероятности укола и его воздействия. Например, вы можете затупить все острые концы или заставить людей носить прочные перчатки. А может быть, просто переставить прялку так, чтобы работникам было труднее случайно задеть острие? Какие меры контроля доступа вы могли бы установить при транспортировке прялок в пределах замка и какие меры защиты цепочки поставок можно было бы применить для закупки новых игл? Сколько вы можете придумать способов предотвратить использование отравленного острия в преступных целях? Какими другими острыми инструментами рабочие могут заменить иглы, если вы избавитесь от них? Нельзя ли переделать веретено так, чтобы оно работало вообще без иглы?

Рекомендуемые меры безопасности и предосторожности

Эти рекомендации следует оценивать с учетом рассмотренной нами концепции инструментов.

1. Оцените свои технические возможности с учетом принципа минимальной функциональности путем отключения либо удаления ненужных программного обеспечения и системных функций в вашей среде или ограничения доступа к ним. (CM-7. Минимальная функциональность.)
2. Периодически просматривайте функции, инструменты и программное обеспечение, используемые каждым сотрудником в каждой системе, чтобы определить, так ли они необходимы и можно ли их удалить или отключить. Внедрите систему регистрации и отслеживания этих инструментов, а также управления ими. (CM-7. Минимальная функциональность | (1) Периодический обзор | (3) Регистрационное соответствие.)

3. После документирования каждого инструмента, который может потебоваться пользователю или системе, ограничьте их применение лишь теми возможностями, которые нужны для работы компании. (CM-7. Минимальная функциональность | (2) Запрет выполнения программы.)
4. Введите белый или черный список программного обеспечения, приложений и других инструментов. (CM-7. Минимальная функциональность | (4) Несанкционированное ПО / черный список | (5) Разрешенное ПО / белый список.)
5. Наложите физические и сетевые ограничения на аппаратные и программные средства. Например, вы можете поместить все рискованные инструменты на отдельный файловый сервер или портативные заблокированные устройства, доступ к которым возможен только в редких случаях и с применением JEA/JIT. (MA-3. Инструменты для обслуживания | (1) Инспекция инструментов | (3) Предотвращение несанкционированного удаления | (4) Ограниченное использование инструментов; SC-7. Граничная защита | (13) Изоляция инструментов/механизмов/компонентов безопасности.)
6. Проанализируйте все установленное программное обеспечение и определите, какие операции импорта, API, функциональные вызовы и хуки применяются приложениями, которые считаются безопасными. Рассмотрите возможность использования защиты от неправильного кода, чтобы заблокировать любые инструменты, вводящие посторонний или необычный код в систему. Рассмотрите варианты ограничения, отключения и удаления функций, модулей, компонентов и библиотек ОС, которые не задействованы в деятельности компании. (SA-15. Процесс разработки, стандарты и инструменты | (5) Поверхность атаки; SI-3. Защита от вредоносного кода | (10) Анализ вредоносного кода.)

Резюме

В этой главе мы поговорили об инструментах и том, как много с ними можно сделать и почему важно обеспечивать их безопасность. Вы узнали о тактике «довольствуйся тем, что есть» и о сложности создания защищенных, но вместе с тем функциональных систем.

Возможно, вы также начали задумываться о различиях между инструментами и вредоносными программами, а также о том, как отличить одно от другого. В упражнении об отравленном веретене мы подумали, как перехитрить врага, который хочет вторгнуться в контролируемую нами среду.

В следующей главе мы обсудим использование разведчиками синоби обоняния, зрения и слуха и узнаем, чем нам это поможет с точки зрения применения в среде цифровых датчиков.

9

Датчики

И днем, и ночью необходимо отправлять разведчиков для наблюдения.

Даже если синоби не обладает впечатляющими
физическими способностями, важнее всего
всегда его острая наблюдательность.
«Ёсимори хяку-сю», № 11

«Бансэнсюкай» рекомендует помимо охранников у ворот и солдат на сторожевых постах для защиты замка скрытно размещать наблюдателей вдоль дорог, троп и других подходов. Командир обороняющейся стороны должен расставлять разведчиков по периметру замка в шахматном порядке [5]. Это могли быть:

- нюхающие разведчики *(каги)*;
- слушающие разведчики *(моногики)*;
- пешие разведчики *(тогики)*.

Нюхающие и слушающие разведчики использовали обученных собак и располагались на закрытых наблюдательных постах, где ничего не видели, но были незримы для врага. Разведчик искал признаки проникновения, полагаясь на слух и обоняние. Эти методы особенно хорошо работали ночью, поскольку для этого разведчику не требовался свет [5].

Пешие разведчики ловили лазутчиков, проводя зачистку вблизи границ вражеской территории. Они прятались на вражеской территории и следили за любыми передвижениями в сторону своего лагеря. Также могли для обнаружения злоумышленников использовать растяжки, шум или даже физический контакт. В «Бансэнсюкай» сказано, что разведчики *тогики* сами должны быть синоби, поскольку для выполнения своей работы они должны обладать навыками скрытности и наблюдения,

интуитивно угадывать, с какого направления враг будет атаковать, и уметь успешно обнаруживать и перехватывать вражеских ниндзя [5].

В «Бансэнсюкай» говорится о возможности использовать помимо разведчиков-людей (и животных) активные и пассивные методы обнаружения вражеских агентов. В качестве активного метода синоби может применять *саруби* (обезьяний огонь, или огонь на веревке) [5] для освещения темных мест, например рвов, траншей или оснований стен замка. Такой яркости освещения с помощью фонаря достичь было нельзя. В качестве пассивного метода синоби создавали системы обнаружения, например, заполняя широкую, но неглубокую траншею мелким песком, а затем нанося на него сложный узор. Если враг пройдет линию внешней обороны, он оставит следы на песке, предупреждая охранников о вторжении. Следы на песке могут также подсказать наблюдательному синоби, откуда пришел враг и ушел ли он тем же путем, а это ценные данные, позволяющие нейтрализовать непосредственную угрозу и укрепить оборону на будущее [5].

В этой главе мы рассмотрим различные типы датчиков, обычно используемых в сетях, периодически проводя аналогии между современными средствами и тем, как синоби применяли датчики в далеком прошлом. Мы рассмотрим размещение датчиков, а также методы их обхода и, пользуясь мудростью синоби, улучшим нашу защиту от киберопасностей. Также мы рассмотрим датчики, схожие по принципу действия с древними разведчиками.

Идентификация и обнаружение угроз с помощью датчиков

На киберязыке термином *«датчик»* называется множество систем и инструментов обнаружения. Чаще всего он представляет собой расположенное на порте ответвления, тройнике или зеркале устройство мониторинга, которое анализирует всю активность для наблюдения, записи и анализа. Например, датчик может находить и захватывать необработанные пакеты (PCAP), когда они проходят по кабелю, а затем обрабатывать и анализировать их с целью предупредить систему безопасности о подозрительных событиях. Датчики могут быть размещены «на линии», и в этом случае каждый пакет проходит через устройство, которое способно задерживать, блокировать или изменять информацию в пакете, полноценно предотвращая атаки, а не просто сообщая об угрозе. Вторичные датчики, такие как вайфай-датчики, обнаруживают внешние или другие несанкционированные сигналы и соединения, а датчики физической безопасности, такие как камеры, контролируют доступ к конфиденциальным центрам обработки данных, серверным стойкам и электрическим автоматам. В более широком смысле определенные программные агенты на конечных точках тоже работают как датчики, поскольку они анализируют события, действия и активность в хост-системе и отчитываются

перед системой управления и контроля, при необходимости генерируя предупреждения.

Компании часто настраивают датчики на определенные типы трафика, например на шлюз электронной почты для перехвата фишинга или спама, или настраивают системы предотвращения/обнаружения сетевых атак, брандмауэры для перехвата неавторизованных IP-адресов и портов, прокси-серверы для подозрительных веб-сайтов и системы предотвращения потери данных. Устройства с датчиками обычно устанавливаются в основной точке выхода сети в демилитаризованной зоне (DMZ). Поскольку размещать датчики принято в как можно более глубокой части системы, чтобы максимально увеличить объем трафика, который проходит через них, злоумышленник может скрыться от датчика на шлюзе или обойти основной выход, действуя таким образом втайне от датчика.

Несмотря на необходимость обеспечения безопасности, большинство компаний едва ли ринется устанавливать кучу датчиков, поскольку их приобретение, работы по лицензированию, установке, обновлению, обслуживанию и мониторингу нецелесообразны с финансовой точки зрения. К сожалению, во многих организациях предполагают, что если основной датчик выхода не обнаруживает угрозы, то и большее их количество не принесет пользы. Из-за этой ошибки система подвергается риску.

Улучшение работы датчиков

Главная проблема датчиков заключается в том, что им почти всегда требуется человек, который контролирует их работу и распоряжается полученной информацией. Эта проблема усугубляется скудным ассортиментом датчиков безопасности и доступных аналитических платформ. Современные датчики безопасности можно представить следующим образом: по зданию разбросано множество крошечных микрофонов и камер, но все они заключены внутри маленьких соломинок, из-за чего их поле зрения сужается. А теперь представьте, что вы пытаетесь собрать воедино картину проникновения, имея возможность смотреть только через одну соломинку. Более того, каждая соломинка накапливает тысячи часов данных, которые надо хранить, обрабатывать и анализировать. Эту неприятную ситуацию часто можно смягчить с помощью сигнатур, алгоритмов или машинного обучения, которые способны помочь выявить аномалии и вредоносную активность. Однако и такие автоматизированные системы не идеальны. Они часто вызывают ложные срабатывания или создают такой большой поток предупреждений, что лучше было бы без них. Чтобы решить эти проблемы, обратимся к мудрости синоби: мы способны определить пути, по которым может пойти враг, а затем разместить вдоль них разные датчики, чтобы обнаружить атаку заранее. Продумывая возможность улучшения использования датчиков в вашей компании, рассмотрите следующие советы.

1. **Смоделируйте сеть и определите свои слабые стороны.** Создайте карту сети и модель потока данных вашей среды. В ней нужно описать каждую систему и ее назначение, связь систем, точки входа и выхода информации, типы информации, датчики (если они есть), которые проверяют информацию, и точки выхода. Определите места, в которых датчиков нет, и места, которые, по вашему мнению, хорошо контролируются. Попробуйте предугадать, где злоумышленники попытаются проникнуть в вашу сеть. Имейте в виду, что создание достаточно полной карты может занять месяцы и потребует содействия всего предприятия. Созданная карта может быть не идеальной, но даже такая лучше, чем ее отсутствие.
2. **Наймите «красную команду» и выполните тест на проникновение.** «Красная команда» должна попытаться проникнуть в вашу сеть. Рассмотрите подход «фиолетовой команды», при котором защитники вашей сети («синяя команда») наблюдают за «красной командой» в реальном времени, находясь в той же комнате, и могут приостановить задачу, чтобы задать вопросы. Опросите датчики безопасности до, во время и после атаки, чтобы узнать, что они обнаружили и о чем сообщили. Эта информация будет для вас важна. Озадачьте «синюю команду» вопросом о том, как другое размещение датчиков позволило бы быстрее и точнее обнаружить «красную команду». Обсудите архитектурные изменения защиты, настройку датчиков и другие решения, предложенные в ходе тестирования.
3. **Идентифицируйте и заблокируйте зашифрованный трафик.** Блокируйте весь зашифрованный трафик, который не может быть перехвачен и проверен датчиками. Кроме того, лишите ваши машины возможности использовать несанкционированное шифрование. Попросите «красную команду» проверить способность датчиков обнаруживать зашифрованный трафик. Большинство датчиков не может проверять зашифрованный трафик, поэтому многие организации применяют асимметричное шифрование, например эллиптическую кривую Диффи — Хеллмана (elliptic-curve Diffie-Hellman, ECDH), которую нельзя взломать корневыми сертификатами. Разрешив постороннему зашифрованному трафику покидать вашу организацию, не проходя через DLP, вы создаете брешь в безопасности, как если бы охранники замка внимательно осматривали всех прохожих с открытыми лицами и спокойно пропускали тех, кто носит маски.
4. **Разработайте «нюхающие» и «слушающие» датчики.** Изучите возможности создания датчиков, которые могли бы тайно обнаруживать определенные типы угроз. Например, настройте внешний физический датчик, который отслеживает активность ЦП или энергопотребление и может обнаружить несанкционированный доступ или применение постороннего ПО, если производительность не коррелирует с допустимыми командами или активностью пользователя, работающего в системе.

5. **Реализуйте пассивные датчики.** Введите пассивные интерфейсы на коммутаторах и серверах, которые никогда не должны использоваться. Настройте датчики на локальное обнаружение и оповещение при активации интерфейса, что указывало бы на вероятное присутствие в вашей сети злоумышленника. Подобно неглубокой канаве, заполненной песком, такие системы позволяют обнаруживать движение трафика в тех местах сети, где этого быть не должно.
6. **Установите датчики тогики.** Разместите за пределами своей сети обращенные внутрь датчики для обнаружения проникновения. При содействии интернет-провайдера вы можете настроить датчики за пределами сети так, чтобы они мониторили входящий и исходящий трафик, который другие датчики могут не обнаружить. Разместите на Т-образном разъеме возле устройства датчики, работающие вместе с датчиком на хосте, а затем сравните работу устройств, чтобы определить, сообщают ли оба датчика об одной и той же активности. Такой подход помогает идентифицировать скомпрометированные датчики и драйверы сетевого интерфейса.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. За последнюю неделю в нем произошло три поджога, хотя пожарная команда была к этому готова и погасила пламя до того, как оно распространилось. Вы считаете, что поджигатель — это синоби, который извлек урок из реакции вашей команды и проведет новую атаку, на этот раз, возможно, не используя огонь. У вас мало ресурсов, вашей пожарной команде нужны дополнительные сотрудники и оборудование, чтобы лучше работать в случае происшествия, архитектор хочет укрепить и защитить от огня части замка, а начальник службы безопасности требует увеличить число охранников на воротах, чтобы поймать злодея.

Как бы вы разместили в замке датчики для обнаружения поджигателей или других подозрительных лиц? Можно ли улучшить время реакции и возможности пожарной команды, уменьшив при этом ее количество, например используя людей в качестве датчиков, а не активных пожарных? Где и как можно разместить человека, чтобы он мог наиболее эффективно обнаруживать подозрительную активность и предупреждать о ней других ? Как сменять охранников периметра внутри и снаружи замка и как при этом не дать противнику определить, где и когда находится патруль? Какие пассивные датчики могли бы позволить вам поймать поджигателя?

Рекомендуемые меры безопасности и предосторожности

Эти меры следует оценивать с учетом рассмотренной концепции датчиков.

1. Реализуйте сниффер пакетов, полносетевые PCAP и другие автоматизированные датчики для обработки инцидентов, обслуживания и сопровождения информационных потоков. (AC-4. Сопровождение информационных потоков | (14) Фильтры и политики безопасности; IR-4. Обработка инцидентов; MA-3. Инструменты для обслуживания.)
2. Чтобы предотвратить физический доступ и обнаружить попытки взлома, установите датчики на замки коммутационных шкафов, камеры для наблюдения за доступом к центру обработки данных и серверам, датчики воды для обнаружения протечек, которые могут угрожать электрическим устройствам, и датчики прослушивания на линиях связи. (PE-4. Контроль доступа для передачи; PE-6. Мониторинг физического доступа; PE-15. Защита от повреждения водой.)
3. Внедрите программы обучения для персонала, в том числе не связанного с ИТ, чтобы сотрудники выполняли роль живых датчиков и обнаруживали угрозы. Обеспечьте сотрудникам четкий, простой и доступный способ сообщить о подозрительной активности. (PM-16. Программа осведомленности об угрозах.)
4. Перехватывайте зашифрованные данные и разрешите датчикам выполнять глубокую проверку незашифрованных пакетов. (AC-4. Сопровождение информационного потока. | (4) Проверка зашифрованной информации; SC-8. Конфиденциальность и целостность передачи.)
5. Реализуйте датчики, которые будут анализировать пакеты и принимать превентивные меры, такие как блокировка или фильтрация. (SC-5. Защита от отказа в обслуживании; SC-7. Граничная защита | (10) Превентивная фильтрация | (17) Автоматическое применение форматов протоколов.)
6. Запретите беспорядочную активацию датчиков в менее важных системах, чтобы предотвратить разглашение конфиденциальной информации злоумышленникам, получившим доступ. (SC-42. Возможности датчика и данные.)
7. Совместно со своим интернет-провайдером установите датчики надежного подключения к интернету (TIC) за пределами сети. (AC-17. Удаленный доступ | (3) Управляемые точки доступа.)
8. Задокументируйте все внутренние системные соединения, их интерфейсы, информацию, которую они обрабатывают, хранят и передают, и разместите датчики между системами. (CA-9. Внутрисистемные соединения.)

9. Проведите тестирование на проникновение с участием «красной команды» с целью проверить правильность размещения датчика и его возможности. (CA-8. Тестирование на проникновение; RA-6. Обзор средств технического наблюдения и противодействия.)

Резюме

В этой главе мы говорили о «нюхающих», «слушающих» и пеших разведчиках, которых задействовали для обнаружения синоби противника в древней Японии. Мы также рассмотрели активные и пассивные датчики, которые охранники замка использовали для поимки злоумышленников. Затем обсудили различные типы датчиков, которые применяются сегодня и помогают защитникам видеть, что происходит в системе. Мы рассмотрели несколько логистических проблем, связанных с датчиками, например места их размещения, ложные срабатывания и управление датчиками. Наконец, поговорили о том, как применить древние техники синоби для выявления злоумышленников в сетевых системах.

Далее мы обсудим различные типы мостов и лестниц, которые синоби использовали для обхода защитных сооружений замка (эта тема будет связана с датчиками). Например, представьте, что ваш замок защищен рвом и все датчики размещены на подъемном мосту. Вражеский синоби, способный незаметно установить собственный мост и не использовать ваш подъемный, может обойти датчики, что сделает их бесполезными. Мы рассмотрим, как эта проблема возникает в кибербезопасности и сложно ли ее решить.

10

Мосты и лестницы

Не существует такой стены или рва, которые вы не могли бы пройти, какой бы высоты или глубины они ни были, особенно если у вас есть лестница ниндзя.

Ворота замка обычно охраняются лучше всего, но крыша — самое удобное место для крепления крюковой лестницы.
«Бансэнсюкай», ин-нин II [5]

Синоби мог незаметно преодолевать стены и ворота, используя инструменты проникновения, описанные в «Бансэнсюкай» [5] и «Гумпо дзиёсю» [6]. Складные лестницы и переносные мосты, лестницы с шипами, облачные лестницы или транспортировочный канат [5] позволяли синоби пересекать рвы, осторожно и незаметно взбираться по стенам и доставлять грузы другим синоби. Иногда эти лестницы были настоящими и специально изготавливались перед вылазкой, а иногда — временными и создавались в полевых условиях [5]. Это были полезные инструменты, поскольку они обеспечивали доступ в уязвимые места, которые часто оставались без присмотра, так как защитники были уверены в их неприступности.

В трактатах также объясняется, как проникнуть во вражеский лагерь, используя меры безопасности самого противника. В трактате «Сёнинки» говорится, что синоби должен представить, как в замок проникла бы птица или рыба [7], — другими словами, использовать уникальные преимущества, которые можно найти лишь наверху или внизу. Например, забравшись на стену, можно быстро преодолеть другие стены и крыши и проникнуть во внутреннюю часть замка проще, чем через ворота. Проплыв по рву, можно попасть в замок по водяному каналу. «Бансэнсюкай» даже рекомендует попытаться перебраться через стену именно рядом с воротами, где логично было бы разместить большинство охранников, потому что защитники предполагают, что рядом с воротами через стену никто не полезет [5].

В этой главе мы обсудим, чем проникновение через сетевые домены похоже на проникновение через периметр стен замка. Как и стены замка, сети разделяются барьерами и сегментацией, в результате чего трафик должен проходить через контролируемый шлюз. Мосты позволяют угрозам обходить эти шлюзы, минуя меры безопасности, предпринятые в точках выхода шлюзов. Простые меры вроде приказов охранникам пресекать любые попытки перебросить мост через ров замка могут оказаться бесполезными, если ранее архитектор замка решил соединить концентрические кольца рва, чтобы проще было регулировать водные ресурсы. Из-за этого три рва больше не являются тремя отдельными границами, которые противник должен преодолеть. Вместо этого они представляют собой водный мост, по которому можно попасть прямо в сердце замка.

Сетевое граничное соединение

С точки зрения специалистов по кибербезопасности, *мост* — это виртуальное или физическое сетевое устройство, которое работает как на физическом, так и на канальном уровне — на уровнях 1 и 2 модели OSI — и соединяет два сегмента сети, образуя из них единую сеть. Этот термин также относится к любому устройству, инструменту или методу, которые позволяют данным пересекать разрыв, например воздушный зазор в сети или границу сегментации. Мосты обычно обходят меры безопасности и защиты, позволяя красть данные из сети или, наоборот, вносить в нее неавторизованные или вредоносные данные. Такие риски заставили профессионалов в области кибербезопасности развивать методы обнаружения и смягчения последствий для предотвращения наведения мостов, в том числе:

- отключение сетевых мостов на беспроводных картах Ethernet;
- отключение систем с двумя или более активными сетевыми интерфейсами;
- внедрение контроля доступа к сети (network access control, NAC) и мониторинга новых устройств в сети;
- установку датчиков для обнаружения неавторизованных точек доступа вайфай;
- запрет работы определенных сетей с помощью VLAN или другого маршрутизатора;
- использование аутентификации в протоколе обнаружения канального уровня (Link Layer Discovery Protocol, LLDP).

Несмотря на совершенствующиеся меры безопасности, несанкционированные подключения к сети по-прежнему происходят, и некоторые передовые методы проникновения, даже проверенные только в академической или лабораторной среде, способны причинить немалый вред. К самым передовым методам относятся

управление системными светодиодами для передачи битов данных на оптический приемник в другой комнате или здании, использование сигналов FM-частоты для связи с телефонами (как в случае с эксплойтами AirHopper и GSMem), управление вентиляторами и их пульсацией для отправки битов с помощью звука, а также искусственный перегрев и охлаждение процессоров для медленной отправки данных (как с эксплойтом BitWhisper). Злоумышленники могут даже соединять сети через кабели питания системы с помощью технологии Ethernet over power (EOP, не путать с power over Ethernet, POE). Иногда злоумышленники могут удаленно активировать микрофоны и динамики VoIP-телефонов организации, что позволяет передавать звуковые данные или подслушивать разговоры.

Конечно, некоторые виды мостов менее актуальны. Злоумышленник может забраться на крышу офисного здания, подключиться к имеющимся сетевым кабелям и установить небольшую наземную спутниковую станцию, которая обеспечит надежный мостовой доступ к сети. Смартфоны обычно подсоединяют к USB-портам для зарядки, кроме того, заряжаемый телефон подключает компьютер к внешней сотовой сети, которая не проверяется брандмауэрами, системой предотвращения потери данных (data loss prevention, DLP) или другими инструментами безопасности, минуя средства защиты организации и облегчая кражу данных или внедрения кода в хост-сети. При создании моста через *sneakernet* пользователь загружает информацию на портативный носитель и переходит на другой компьютер или в другую сеть, физически обходя меры безопасности. Хакеры также могут задействовать скрытую сеть управления (обычно это сеть 10.0.0.0/8), которая напрямую подключается к консолям маршрутизаторов, межсетевым экранам и другим системам безопасности, задействуя их в качестве точек перехода для соединения различных сетевых VLAN и сегментов, что позволяет использовать саму сеть для обхода ее же средств безопасности. Кроме того, существует риск раздельного туннелирования, поскольку информация может проникать в сети и выходить из них через устройство, подключенное к двум сетям одновременно.

В зрелых организациях исходят из предположения, что злоумышленники постоянно разрабатывают различные мостовые технологии, пытаясь обойти защиту новыми неизвестными способами. И действительно, кажется, что для доступа в сеть можно использовать весь электромагнитный спектр, а также акустические, световые, сейсмические, магнитные, тепловые и радиочастоты.

Борьба с мостами

Предотвратить создание мостов между системами довольно трудно. Идеального решения этой проблемы не существует, но можно ухудшить условия для создания мостов и подумать об изоляции наиболее важных активов. Кроме того, контрмеры, которые сводят на нет вероятность наведения мостов, могут быть многоуровневыми, что тоже повышает эффективность защиты.

1. **Выявите слабые места.** Определите сети и информационные системы, в которых в вашей компании хранятся конфиденциальные, важные или ценные данные. Создайте диаграмму потока данных (DFD), чтобы понять, как информация хранится и перемещается по системе. Затем определите области, где может произойти скрытая атака через внеканальный мост.
2. **Примите меры против создания мостов.** Рассмотрите возможность внедрения элементов управления TEMPEST [45], таких как клетки Фарадея или экранированное стекло, чтобы предотвратить преодоление воздушного зазора с помощью излучения или других сигналов. Чтобы заблокировать мосты, наведенные злоумышленниками, важно определить контактирующие с сетью устройства, прежде чем разрешить им подключаться к вашей сети или другому устройству. Разработайте соответствующие меры безопасности для смягчения потенциальных угроз, определенных в вашей модели угроз.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка с ценной информацией, сокровищами и людьми. Вы получаете достоверные сведения о том, что синоби использовал специальные лестницы с крючьями и переправил людей или какие-то предметы через стены вашего замка, минуя стражу.

Рассмотрите возможные способы изменения конфигурации стен замка, которые позволили бы обнаружить и/или предотвратить наведение лестниц или мостов. Можете ли вы предсказать, в какой точке синоби попытается преодолеть вашу оборону? Как вы можете изменить протоколы работы охранников и обучить их искать временные мосты? Как бы вы отреагировали, узнав, что в замок кто-то проник, и как будете работать дальше, предполагая, что ваше жилище было скомпрометировано и, возможно, не заслуживает доверия?

Рекомендуемые меры безопасности и предосторожности

Рекомендации следует оценивать с учетом концепции мостов.

1. Реализуйте граничную защиту и управление информационными потоками для предотвращения передачи данных или вредоносного кода внешними устройствами, системами и сетями в вашу сеть. (AC-4. Сопровождение информационных потоков | (21) Физическое/логическое разделение информационных потоков; AC-19. Контроль доступа для мобильных устройств; AC-20. Использование внешних информационных систем | (3) Системы/

компоненты/устройства, не принадлежащие организации; SC-7. Граничная защита.)

2. Реализуйте защиту беспроводного доступа для блокировки или обнаружения несанкционированных беспроводных сигналов, которые передаются по вашим сетям на микроволновых, UHF/VHF, Bluetooth, 802.11x и других частотах. (AC-18. Беспроводной доступ; SC-40. Защита беспроводной связи.)
3. Проверяйте доступ к сети и сетевые соединения, чтобы определить внешние сети или системы, например удаленные сетевые принтеры, которые могут служить мостом для передачи данных в вашу сеть. (CA-3. Соединения системы; CA-9. Внутрисистемные соединения.)
4. Введите строгие правила подключения портативных носителей. Требуйте идентификации и аутентификации внешних носителей и устройств, прежде чем разрешать им подключаться к вашей среде. (IA-3. Идентификация и аутентификация устройства; MP-1. Политика и процедуры защиты носителей; MP-2. Доступ к носителям; MP-5. Транспортировка носителей.)
5. Выполните тест на утечки в TEMPEST или наличие других внеканальных сигналов, поступающих из ваших систем. Получив результаты, определите, где требуется реализовать защиту, чтобы воспрепятствовать использованию сигнала в качестве моста. (PE-19. Утечка информации; SC-37. Внедиапазонные каналы.)

Резюме

В этой главе мы поговорили о философии наведения мостов, а также рассмотрели лучшие общепринятые методы использования мостов в сегментированной сети. Разобрали методы создания мостов, которые позволяют преодолевать зазоры такими способами, о которых вы, возможно, раньше и не думали. Упражнение в этой главе должно было заставить вас задуматься о постройке ограждений между лестницами и стенами. Теоретически такие ограждения могут стать основой для модификации современных средств защиты входов/выходов системы.

В следующей главе мы поговорим о замка́х и способах их взлома, применяемых синоби и основанных на принципе, гласящем, что любой замо́к, созданный одним человеком, может быть взломан другим человеком. Мы также получим представление о подходе синоби к безопасности, когда им приходилось полагаться на замо́к, которому они не доверяют. Мы обсудим применение замко́в в кибербезопасности, а также то, чему можем научиться у синоби, чтобы быстрее взламывать замки́.

11

Замки́

Нет замка, который нельзя было бы открыть. Все зависит от вашей квалификации, поэтому вам нужно постоянно практиковаться.

Инструменты для взлома помогут вам с легкостью открыть двери вражеского дома. Таким образом, это один из тех навыков, попрактиковаться в котором можно лишь в стане врага.

«Бансэнсюкай», Нинки III [5]

В древней Японии замки́ были проще, чем сегодня, поскольку технологии того времени не позволяли производить замысловатые штифты, тумблеры и другие элементы, которые входят в современные запоры. Однако эти старые замки́ были элегантно спроектированы с использованием «зубцов, защелок и естественных сил гравитации и напряжения», чтобы защитить ценности от злоумышленников и воров [5].

Синоби во время своих миссий регулярно сталкивались со сложными замка́ми и придумали, как открыть их все. Трактаты говорят, что ни один замо́к, барьер или другой механизм не был препятствием для синоби, обладавшего хорошим инструментом, острым умом, изобретательностью и оптимистично настроенного. Значительная часть всех трех трактатов посвящена тому, как создавать и использовать различные отмычки, щупы и другие инструменты для открытия замко́в, дверей и ворот (рис. 11.1) [5].

Кольцевые защелки, цепочки, запорные планки, крючки и колышки, сложные защелки для ключей — какой бы ни была конструкция замка́, у синоби были методы и инструменты, чтобы открыть его. Фактически синоби могли взломать любую систему безопасности или защиту от проникновения, которыми пользовались в те времена [6]. Зная, что замка́м нельзя полностью доверять, синоби сами разработали методы, позволяющие обеспечить свою безопасность. Некоторые из них были очень простыми: остановившись на ночлег там, где ему могла грозить опасность, синоби иногда привязывал веревку к двери или окну и к пряди волос, что гарантировало пробуждение, если дверная защелка или замо́к откроются, когда он спит [7].

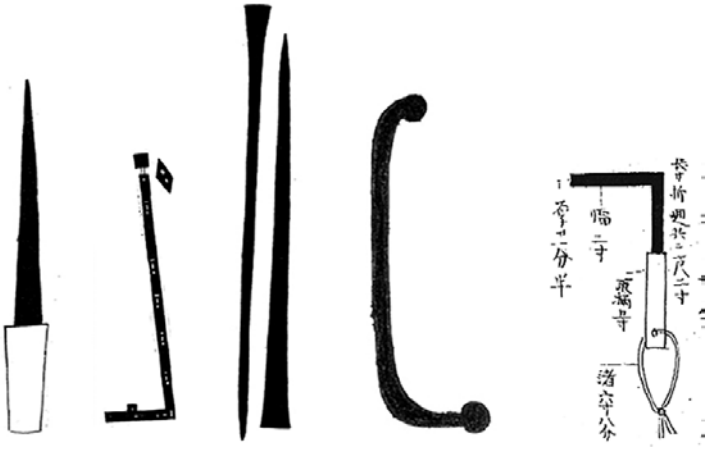

Рис. 11.1. Инструменты для открывания замко́в, дверей и ворот: *слева направо* — щуп, выдвижной ключ, отмычки, отмычка для замков с направляющей и инструмент для открывания дверей («Бансэнсюкай» и «Нимпидэн»)

Сегодня люди все так же используют для защиты своей собственности замки́, а злоумышленники все так же открывают их отмычками. Замо́к, как и всегда, служит нескольким целям: он действует как сдерживающий фактор, дает хозяину уверенность в том, что его имущество в безопасности, и позволяет сузить круг подозреваемых, если замо́к был открыт ключом. Он также служит барьером и сигналом тревоги, так как ворам потребуется время на взлом и в процессе этого они наверняка будут шуметь. В этой главе мы обсудим, как хакеры взламывают замки́ и обходят защиту. Кроме того, поговорим о том, почему для цифровых систем важны физические замки́, и подробно расскажем о необходимых мерах предосторожности.

Мы также рассмотрим некоторые технологические достижения в сфере создания замко́в и отмычек, раскрывающие, чему еще синоби могут научить нас в области безопасности.

Физическая безопасность

Взлом замка́ зачастую является началом ограбления, а взлом цифрового замка́ часто предваряет нарушения кибербезопасности. Поиск слабых мест или удачный доступ к тому, что должно быть безопасным (об успешном взломе свидетельствуют визуальный, тактильный и звуковой сигналы), могут пробудить интерес к сфере безопасности и укрепить уверенность в своих способностях.

В сфере кибербезопасности для ограничения физического доступа в здания, центры обработки данных, к коммутационным шкафам и отдельным помещениям

используются устройства блокировки[1]. Если точнее, то замки́ на стойке ограничивают доступ к серверам, замки́ на корпусе — к физическим компонентам системы, замки́ на портах — несанкционированное применение USB-накопителей или консольных разъемов, жесткое закрепление не позволяет перенести систему в другое место, а блокировка питания не дает включить устройство. Блокирование физического доступа к системам — важнейшая часть стратегии кибербезопасности организации. Если системы уязвимы для физического вмешательства, то после того как злоумышленник получит доступ к ним, меры цифровой безопасности могут оказаться бесполезными. Следует предположить, что если злоумышленник получает физический доступ к машине, он сразу же получает права администратора в системе и все ее данные.

Несмотря на распространение незаконных инструментов и методов взлома, компании, как правило, из года в год используют одни и те же замки́, становясь уязвимыми для атак. Доступ в здания, где располагается большинство информационных систем, закрывают ненадежные штифтовые замки́, такие как цилиндрический замок Yale, запатентованный в 1860-х годах и являющийся сегодня самым распространенным в мире из-за низкой стоимости и простоты массового производства. Также популярны трубчатые, или круглые, замки — самый распространенный тип велосипедных замков. Преступники создают, продают и используют инструменты для взлома, позволяющие легко взламывать стандартные замки́. Например, ключами от банок с газировкой можно открывать некоторые замки́, колпачки для ручек могут имитировать трубчатые ключи, а на 3D-принтере можно легко напечатать пластиковый ключ, имея фотографию оригинала. Автоэлектронные взломщики позволяют даже неквалифицированным преступникам одним нажатием взломать все штифты замка́ за секунды.

Крупномасштабные меры противодействия взлому замко́в принимаются редко, причем иногда скорее для галочки, чем для реальной безопасности. Например, некоторые страховые полисы не покрывают взлом и кражи, если во время преступления были вскрыты некачественные замки́, например, самые распространенные из продаваемых в США. В некоторых странах для производителей замко́в устанавливают стандарты соответствия, а также ограничения, запрещающие продажу некачественных замко́в. В сфере кибербезопасности некоторые правительства защищают свои секретные системы и данные с помощью шифровальных замко́в или других высоконадежных запоров и дополнительных мер безопасности, нивелирующих недостатки самих замко́в.

Тем не менее на многих дверях и во многих системах по-прежнему используется слабая защита из замка́ и ключа, а их может одолеть даже не слишком изощренный

[1] Хотя блокировки информационных систем и данных, безусловно, заслуживают обсуждения, в этой главе таким термином обозначаются именно физические блокировки, используемые для блокирования доступа к информационным системам и средам.

злоумышленник. Замки́ и барьеры информационных систем должны быть способны противостоять распространенным атакам, таким как захват, кража, копирование и принудительное применение.

Улучшение замко́в

Предотвратить абсолютно любой взлом, вероятно, невозможно. Но есть множество превентивных действий, которые вы можете предпринять, чтобы повысить надежность замко́в. Улучшение замко́в напрямую связано с кибербезопасностью, так как защищает от атак физического доступа к вашим системам.

- **Обновите замки́.** Изучите более совершенные системы запирания, такие как европейские замки́ с углублениями, и определите, какие из них подходят вам по требованиям бизнеса и бюджету. Получите одобрение от заинтересованных сторон и отдела безопасности, а затем начните использовать новые, более надежные замки́.
- **Выходите за рамки замка́.** Рассмотрите возможность применения нестандартных решений, например многоэтапных замко́в. Когда механизм первой ступени контролирует доступ к замку́ второй ступени, злоумышленник не сможет легко и быстро открыть оба одновременно.

  Например, чтобы закрыть вход, можно использовать две независимые системы запирания, дополняющие друг друга. Первой ступенью может быть цифровой четырехзначный ПИН-код, который временно разблокирует штифты в замке́ второй ступени. Пока штифты заблокированы, открыть дверь невозможно, но при подготовке к активации замка первой ступени надо вставить ключ. Как только штифты временно разблокируются, можно повернуть ключ и отпереть вход. Но это окно доступа открывается всего на три секунды. После этого цифровой замо́к снова блокирует штифты. Чтобы пройти через дверь, злоумышленник должен сначала узнать ПИН-код, а затем суметь взломать дверной замо́к менее чем за три секунды, что может оказаться невозможным.
- **Усильте защиту.** Рассмотреть возможность укрепления той части, на которой крепится замо́к. Вы можете защитить петли от взлома или установить усиливающие пластины на наличники, дверь, раму, щитки дверных ручек или напольные ограждения.
- **Обратитесь к производителю замко́в.** Подайте производителям замко́в идею включить новые разработки в изделия, используемые для защиты информационных систем. До тех пор пока потребители не начнут требовать обновить устаревшие продукты, производители продолжат продавать старые добрые слабые замки́.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового за́мка, в котором хранятся ценности. Вы знаете, что все они находятся под замко́м в сундуках и хранилищах за дверями и воротами, а еще знаете, что синоби способен обойти все эти препятствия.

Как можно было бы повысить безопасность замко́в? Как узнать, что их вскрывали? Как заблокировать доступ синоби к замка́м? Как расставить ложные замки́, чтобы обмануть синоби и узнать о попытке проникновения?

Рекомендуемые меры безопасности и предосторожности

Рекомендации следует оценивать с учетом концепции замко́в.

1. Храните бумажные файлы, магнитные ленты, жесткие диски, флеш-накопители, диски и другие физические носители в закрытых контейнерах и контролируйте их неприкосновенность. (MP-4. Хранение носителей; MP-5. Транспортировка носителей.)
2. Используйте безопасные ключи или другие блокирующие устройства для обеспечения контроля физического доступа и авторизации в системах и средах. (PE-3. Контроль физического доступа | (1) Доступ к информационной системе | (2) Границы объекта / информационной системы | (4) Запираемые кожухи | (5) Защита от несанкционированного доступа; PE-4. Контроль доступа к среде; PE-5. Контроль доступа устройств вывода.)

Резюме

В этой главе мы поговорили о замка́х и их назначении. Мы отметили, что злоумышленники, независимо от эпохи, всегда будут разрабатывать способы взломать замо́к. Мы рассмотрели распространенные технологии, используемые для защиты доступа к системам, и отметили, почему важно их модернизировать. Особенно важно помнить, что если злоумышленник получает физический доступ к вашей системе, ее можно считать скомпрометированной, и именно поэтому важно ограничивать физический доступ к системам с помощью замко́в.

В следующей главе мы обсудим тактику, которую синоби применяли, когда не удавалось вскрыть замо́к, — обман с целью заставить противника отдать ключ. В некотором смысле защита компании устроена примерно так же, и даже если у вас установлен самый лучший замо́к, но вы отдадите ключ злоумышленнику, замо́к не спасет.

12

Отражение луны в воде

Заключив соглашение со своим господином, вы должны выманить врага с помощью приманки и проникнуть в его оборону.

Используя эту технику, вы должны увлечь противника заманчивой наживкой, например рыбалкой в море или на реке, чтобы заставить врага, который обычно не покидает замка, остаться без защиты.

«Бансэнсюкай», ё-нин II [5]

В этом красочном хайку описывается техника проникновения с открытой маскировкой *суйгецу-но дзюцу* — искусство отражения луны в воде [5]. Эта техника имела множество применений, но синоби использовали ее в первую очередь для атак на сильно укрепленные вражеские лагеря: людям не позволялось выходить из них, входить внутрь и вообще приближаться к ним. Вместо преодоления обороны лагеря силовыми методами синоби обманом заманивали цель в ловушку, заставляя ее выдать протоколы входа, знаки отличия и другие опознавательные знаки, пароли, кодовые слова и парные сигналы. Эта техника также позволяет синоби следовать за целью, когда та возвращается в лагерь, выманивать охранников с постов и беспрепятственно проникать в лагерь или напрямую взаимодействовать с целями и проходить в лагерь с помощью обмана или нападения.

Если цель упорно не желает покидать удобный укрепленный лагерь, трактат советует синоби обратиться за помощью к своим командирам и организовать более сложный обман [5]. Например, командир может выдвинуть отряд на уязвимые позиции, соблазняя врага на атаку и заставляя его отвлечь значительную часть сил от обороны, чтобы синоби сумели проникнуть в лагерь. Как вариант, синоби может атаковать врага, когда тот вернется, измотанный после битвы.

Командир может организовать и нечто более сложное, например полноценную длительную осаду замка. Затем синоби может послать солдата, выдав его за посла союзного генерала, который убедит врага покинуть свой замок, присоединиться

к контрнаступлению и прорвать осаду. Для наглядности командир синоби может даже направить замаскированный отряд, который выглядит как подкрепление союзников, тем самым еще сильнее стимулируя врага покинуть лагерь и дать синоби возможность проникнуть в него. Согласно трактату, после успешного проникновения в лагерь с помощью *суйгецу-но дзюцу* синоби должен:

- сохранять спокойствие, не казаться потерянным;
- копировать поведение находящихся там людей;
- постараться разузнать побольше кодовых слов, паролей, ответов на вопросы и знаков отличия;
- как можно скорее связаться с союзниками [5].

В этой главе мы исследуем способы применения этой древней техники в контексте киберугроз и сравним ее с общепринятыми тактиками социальной инженерии. Рассмотрим способ абстрактно рассматривать сетевые сигналы как входящие и/или выходящие за пределы периметра, несмотря на то что компьютерная система не движется физически. Кроме того, мы поговорим о концепциях противодействия «отражению луны в воде» и методикам социальной инженерии в целом. Наконец, выполним упражнение-загадку, которую приходилось решать древним японским генералам, ставившим целью нейтрализовать «отражение луны в воде».

Социальная инженерия

Тактика «отражение луны в воде», применяемая синоби, поразительно похожа на сегодняшнюю *социальную инженерию*, в которой процессы принятия решений и когнитивные предубеждения цели используются для манипулирования ею, раскрытия конфиденциальной информации или иных злонамеренных действий. В сфере кибербезопасности социальная инженерная в основном применяется шпионами, действующими на территории врага, и основана на доверчивости цели. Рассмотрим примеры типичных атак социальной инженерии.

- **Фишинг.** Злоумышленник отправляет электронное письмо, в котором получателей просят открыть опасный документ или перейти по подложной гиперссылке, что приводит к заражению компьютера вредоносным ПО, запуску программы-вымогателя, краже данных или иным последствиям.
- **Предлог.** Злоумышленник делает звонки или отправляет письма, в которых под вымышленным поводом подталкивает цель к раскрытию конфиденциальной информации или совершению злонамеренных действий.
- **Приманка.** Злоумышленник размещает на видном месте вредоносные портативные носители, например USB-накопители, побуждая цель взять их и подключить к системе, создав тем самым уязвимость для будущей атаки.

Социальная инженерия — это особенно сложная область безопасности, потому что в ней злоумышленник использует саму человеческую природу такими способами, от воздействия которых технические средства контроля не всегда могут обезопасить. Когда стоит задача противодействовать атакам и защищать свои ценные активы, многие организации полагаются на специализированные технические средства контроля, протоколы безопасности и обучение пользователей. Сотрудников учат правильно обращаться с конфиденциальной информацией и системами, а отделы безопасности составляют процедуры проверки личности неизвестных или нежелательных посетителей и требуют, чтобы лиц, не являющихся сотрудниками, сопровождали, когда они находятся на территории компании. «Красные команды» проводят проверки на фишинг и атаки «следование в хвосте», анализируют подготовленность сотрудников к атакам социальной инженерии и противодействию им. Администраторы внедряют технические средства блокировки вредоносных документов и гиперссылок, задействуют программное обеспечение для предотвращения потери данных (DLP), запрещают несанкционированные изменения системы, заносят в черный список незарегистрированные системы и внешние носители, а также используют идентификаторы вызывающей стороны.

Все эти меры хороши и необходимы, но методы работы людей меняются. А вот теория защиты от социальной инженерии еще не эволюционировала настолько, чтобы полностью обезопасить себя от атак «отражение луны в воде», когда цель выманивают за линию защиты.

Современные способы применения собственного устройства (bring your own device, BYOD), повсеместная удаленная работа и многопользовательские облачные ресурсы обеспечивают сотрудникам и организациям бóльшую гибкость. Но в то же время они ослабляют традиционную архитектуру безопасности и подвергают сотрудников новым угрозам социальной инженерии. Например, в большинстве случаев правила брандмауэра с отслеживанием состояния запрещают передачу любых данных из интернета на внутренний хост. Вместо этого брандмауэру требуется внутренняя (интранет) система, которая должна установить связь, после чего он разрешит данным из внешней системы поступать на внутренний хост. Таким образом, хотя внутренний хост физически не покидает защищенный периметр организации, его виртуальное «выманивание наружу» путем посещения вредоносного веб-сайта может позволить злоумышленникам передать что-то в ответ на запросы. Это то же «следование в хвосте», но в цифровом варианте.

Помимо прямых атак на традиционные архитектуры безопасности, злоумышленники могут использовать методики типа «отражение луны в воде», проникая с их помощью в хорошо укрепленные организации. Рассмотрим следующие сценарии.

- Противник активирует пожарную сигнализацию на охраняемом объекте, в результате чего сотрудники массово покидают рабочие места. Пока пожарные проверяют здание, противник смешивается с толпой сотрудников,

крадет бейджи, ключи, жетоны, фотографии, отпечатки пальцев и многое другое. Чтобы облегчить возврат сотрудников на рабочие места, предприятие временно отключает считыватели бейджей, турникеты или другие средства контроля физического доступа, чтобы поток людей не перегрузил систему безопасности, и в этой ситуации проникнуть внутрь становится легко.

- Противник пригоняет фуд-трак, выманивая сотрудников из безопасного места. Затем он словно невзначай применяет к цели приемы социальной инженерии, добиваясь доверия и убеждая человека выполнить действия, добиться которых стандартными средствами социальной инженерии не удалось бы.
- Противник взламывает вайфай-сеть из кафе или с улицы и крадет учетные данные сотрудников целевой организации. Войдя в кафе вместе со своими гаджетами, сотрудники покидают защищенный периметр организации и, не осознавая того, оказываются там, где правит злой гений.
- Противник проводит крупномасштабные деструктивные атаки на целевых сотрудников, системы и данные, побуждая их перейти на менее безопасную платформу для выполнения аварийного восстановления, а туда проникнуть уже легче.

Обратите внимание на то, что даже если злоумышленнику после атаки не удается достичь конечной цели, он может получить иные средства или информацию, которые в сочетании с другими помогут реализовать коварные замыслы.

Защита от социальной инженерии

В большинстве организаций проводят тренинги по социальной инженерии и регулярные фиш-тесты сотрудников. Эта стратегия, разумеется, повышает устойчивость к атакам, но все же многие сотрудники проваливают тесты. К сожалению, в большинстве организаций сотрудники уязвимы к социальной инженерии, поэтому нужно прикладывать больше усилий, чтобы дать им инструменты, необходимые для защиты от такого обмана.

1. **Установите стандарты.** Внедрите стандартный уровень доверия сотрудников, чтобы снизить риск атак социальной инженерии. Определите в вашей среде важные точки, а затем установите протоколы, политики и процедуры безопасности в отношении контроля и работы с конфиденциальной информацией в этих системах (со временем их можно распространить на все системы). Проводите в своей организации тренинги, ознакомительные семинары и упражнения, чтобы повысить уровень осведомленности сотрудников о социальной инженерии, а также используйте итеративное моделирование угроз для проверки и улучшения соответствующих мер безопасности.
2. **Реализуйте «медленное мышление».** Выдайте сотрудникам отдела безопасности книгу Дэниела Канемана «Думай медленно... Решай быстро» [18]

и обсудите ее с ними. В книге описаны две системы мышления: более быстрая и импульсивная и более медленная и логичная. Разработайте решения, которые заставят ваших сотрудников действовать медленнее и думать более системно, что позволяет избежать когнитивных предубеждений и ярлыков, которые чаще всего и используют социальные инженеры. Примеры:

- настройте телефоны в компании так, чтобы они требовали от сотрудника, принимающего вызов, ввести четные цифры телефонного номера вызывающего абонента, прежде чем система выполнит соединение;
- настройте ваш почтовый клиент так, чтобы сотрудники должны были ввести адрес отправителя в обратном порядке, прежде чем можно будет открыть вложение;
- заставьте пользователей, переходящих по URL-адресам, не внесенным в белый список, вводить количество символов доменного имени, после чего браузер сможет выполнить DNS-запрос.

Все эти меры замедлят бизнес-операции, но помогут уменьшить количество атак социальной инженерии.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Ваш замок осажден, и вы не уверены, хватит ли вам провианта, чтобы кормить своих людей. Вы получаете письмо от союзного генерала, в котором говорится, что он пришлет вам еду и другие припасы, если в определенную дату и время вы сможете отвлечь внимание вражеских войск, окружающих ваш замок. В письме содержится просьба отправить своего заместителя в лагерь поблизости, чтобы он помог спланировать контрнаступление против осаждающих.

Как определить, подлинное это письмо или противник хочет вас обмануть? Сможете ли вы самостоятельно проверить подлинность письма? А если письмо подлинное, то как отвлечь атакующую армию? Наконец, какие меры вы бы предприняли, чтобы получить припасы, но не допустить проникновения врага в свой замок во время обмена?

Рекомендуемые меры безопасности и предосторожности

1. Поскольку системы безопасности и средства контроля могут защищать информацию лишь в пределах определенных границ, нужно реализовать меры безопасности, которые не позволяют информации и системам выходить за

эти границы и попадать в руки социальных инженеров. (AC-3. Обеспечение доступа | (9) Контролируемый выпуск; PE-3. Контроль физического доступа | (2) Границы объекта / информационной системы; SC-7. Граничная защита.)

2. Контролируйте свой информационный поток так, чтобы даже вышедшие за защитный периметр данные не могли свободно перемещаться между неавторизованными информационными системами. (AC-4. Сопровождение информационного потока; PL-8. Информационная безопасность; SC-8. Конфиденциальность и целостность передачи.)
3. Для всех нелокальных (то есть сетевых) систем установите протоколы утверждения, требуйте использования строгих аутентификаторов и задокументированных политик, а также проводите мониторинг. (MA-4. Нелокальное обслуживание.)
4. Реализуйте защиту данных за пределами контролируемых зон и ограничьте обработку данных узким кругом уполномоченных лиц. (MP-5. Транспортировка носителей | (1) Защита за пределами контролируемых территорий.)

Резюме

В этой главе мы описали продвинутую технику синоби под названием «отражение луны в воде». Рассмотрели различные сценарии, в которых можно было бы модернизировать технику «отражение луны в воде» для атаки на компании. Изучили проблемы, с которыми сталкивается социальная инженерия, и различные формы ее реализации. Рассмотрели существующие методы обеспечения безопасности, предназначенные для работы с социальной инженерией, и изучили новые концепции защиты. Выполнили упражнение из трактатов синоби, которое помогло понять, насколько хрупка наша модель доверия и как трудно защитить ее от атак методами социальной инженерии.

В следующей главе мы обсудим внутренние угрозы — одну из самых интересных тем в сфере безопасности. Трактаты синоби подробно описывают, как определить людей, которых с помощью социальной инженерии можно было бы нанять в качестве инсайдеров. Рассмотрим метод защиты от внутренних угроз, противоречащий передовой современной практике.

13

Внутренний враг

Сделайте из врага миномуси, или агента-червя (внутреннего врага).

Миномуси — это некто, кто служит врагу, но работает
на вас. Такой агент подобен червю в животе врага,
который поедает его изнутри.
«Бансэнсюкай», ё-нин I [5]

Богатый яркими образами и аналогиями трактат «Бансэнсюкай» описывает технику проникновения с открытой маскировкой, называемую «искусство червя в животе» (или агент-червь), которая требует от синоби вербовать вражеских инсайдеров для выполнения поручений. Чтобы выбрать подходящего агента, синоби должен быть очень умным. Он должен был определить подходящую цель, разработать возможности подобраться к ней, незаметно проанализировать, что объект думает о работодателе, каковы его проблемы, желания и амбиции [5].

Трактат гласит, что выбор кандидата — это чрезвычайно ответственная задача, потому что попытка завербовать в качестве агента-червя не того человека может серьезно навредить всей миссии синоби. Чтобы до максимума увеличить вероятность успешной вербовки, синоби разработали восемь архетипов вероятных агентов-червей [5].

- Люди, которые были несправедливо или слишком строго наказаны своим работодателем за какие-либо нарушения и затаили глубокую обиду.
- Люди, которые, несмотря на хорошее стартовое положение или впечатляющие способности, не оценены по заслугам, не получают продвижения по службе и считают, что их потенциал не раскрывается.
- Сверхуспешные работники, которые раз за разом добиваются хороших результатов, но награждаются за это лишь символическими титулами, не-

большими бонусами или недостаточным повышением зарплаты (или вообще не награждаются). Такие работники считают, что у них могла бы сложиться более успешная карьера, будь у них другой работодатель. Они также считают, что компания принимает неверные решения и руководство ценит лишь подхалимов и лизоблюдов, а не лояльных сотрудников с реальными достижениями.

- Умные и талантливые работники, которые не ладят с руководством. Такие люди, как правило, часто раздражают других, работодатели дают им низкие должности, пытаются найти повод для увольнения и, как правило, заставляют их чувствовать себя нежеланными.
- Эксперты в своей области, чьи работодатели пользуются обстоятельствами, например личной преданностью или семейными обязательствами сотрудников, чтобы не повышать их в должности.
- Лица, чьи должностные обязанности прямо противоречат их мироощущению, семейным потребностям или чьи убеждения заставляют сожалеть о том, чем они занимаются.
- Жадные и коварные люди со сбитым моральным компасом.
- «Паршивые овцы», имеющие плохую репутацию из-за прошлых проступков и недовольные таким положением.

Когда синоби выбрал потенциального *миномуси*, ему нужно спланировать, как познакомиться и завязать отношения с кандидатом. «Бансэнсюкай» инструктирует синоби: притвориться богатым господином и завоевать доверие цели с помощью денег; используя дружеские шутки, понять, каковы вкусы жертвы, ее убеждения и чувство юмора; с помощью все тех же шуток понять, о чем думает жертва. Если личность цели соответствует архетипу агента-червя, то синоби пробует завербовать его в качестве *миномуси*, обещая богатство, признание и помощь в реализации тайных амбиций (как правило, алкоголь и секс) в обмен на предательство своего работодателя [5].

Перед началом работы с новообращенным *миномуси* синоби рекомендовалось брать с него клятву преданности или что-то в залог, чтобы обеспечить лояльность агента-червя, а также договориться о тайных сигналах и гарантиях безопасности (operational security, OPSEC) [5].

В этой главе мы рассмотрим внутренние угрозы. Сравним недовольного работника с завербованным инсайдером. Мы также коснемся методов обнаружения и сдерживания, которыми компании могут пользоваться для борьбы с внутренними угрозами, и рассмотрим новый вдохновленный трактатами синоби подход, позволяющий предупреждать превращение сотрудников в инсайдерские угрозы. Наконец, при выполнении упражнения вам будет предложено представить, какие бывшие и/или нынешние сотрудники могут стать внутренними угрозами, и выяснить, как с ними взаимодействовать.

Внутренние угрозы

Внутренняя угроза — это сотрудник, пользователь или другой внутренний ресурс, действия которого могут намеренно или случайно нанести вред организации.

Незадачливый сотрудник, у которого нет цели выполнять злонамеренные действия, но который открывает фишинговое письмо и заражает свою рабочую станцию вредоносным ПО, является внутренней угрозой, хоть и не знает этого. А недовольный работник, целенаправленно распространяющий в организации вирус как по своей инициативе, так и от имени злоумышленника, представляет собой преднамеренную внутреннюю угрозу. Поскольку внутренние угрозы — это легальные авторизованные пользователи с аутентификацией, привилегиями и доступом к информационным системам и данным, они представляют собой очень сложную проблему кибербезопасности, которую требуется сгладить.

Многие организации задействуют средства технического контроля и обнаружения, чтобы как можно раньше определить внутренние угрозы. Технические методы обнаружения — это, например, поведенческая эвристика, которая позволяет выявлять потенциальные внутренние угрозы. ИБ-специалисты могут более внимательно присматриваться к пользователям, совершающим нехарактерные или не подходящие к ситуации действия, например загрузку всех файлов на внешний носитель, поиск конфиденциальных данных, не связанных с их непосредственными обязанностями, вход в систему для выполнения неприоритетной работы в выходные или праздничные дни, запрос файлов с ограниченным доступом, загрузку и использование хакерских инструментов для выполнения действий, выходящих за рамки их служебных обязанностей.

Но технические меры контроля — это лишь часть надежной стратегии защиты даже в сформировавшихся организациях. Работодатель может проверять информацию о работнике и его биографию, криминальную и финансовую историю, выполнять обследование на употребление наркотиков. Это помогает убедиться, что на сотрудника трудно повлиять. Отдел кадров играет ключевую роль в выявлении потенциальных внутренних угроз. Некоторые отделы кадров проводят ежегодные опросы сотрудников с целью определения потенциальных проблем, а иногда и вовсе заблаговременно увольняют ненадежных сотрудников или рекомендуют аннулировать их права доступа в случае каких-либо сомнений. К сожалению, организации обычно принимают минимум мер предосторожности. Многие попросту доверяют своим сотрудникам, другие игнорируют проблемы, а третьи готовы пойти на риск внутренних угроз, чтобы не нарушать бесперебойную работу бизнеса.

Организации, которые активнее других борются с инсайдерскими угрозами, например компании, работающие в оборонной промышленности, и разведывательные организации, внедряют передовые меры обнаружения внутренних

врагов — полиграфы, стандартные проверки допуска, программы контрразведки, раздельные помещения для сотрудников, суровые наказания за нарушения, и все это наряду с передовыми техническими мерами. Но даже такие способы контроля не могут гарантировать предотвращения всех возможных атак и внутренних угроз, особенно если противник умен. К тому же у подобных средств есть недостатки, связанные с их внедрением и эксплуатацией.

Новый подход к внутренним угрозам

Компании, которые регулярно проверяют сотрудников и пытаются поймать их на месте преступления, уже опоздали. Упреждающий события подход заключается в создании такой рабочей среды, условия в которой не способствуют появлению внутренних угроз. Далее приведены некоторые предложения, позволяющие нивелировать некоторые типы угроз.

1. **Разработайте методы обнаружения угроз и смягчения последствий их реализации.** Изучите продукты и технические средства контроля, которые ваша организация использует для выявления и устранения внутренних угроз. Проводите для сотрудников тренинги и ознакомительные занятия, просматривайте отчеты об инцидентах и выполняйте с «красной командой», например, фишинговые тесты для выявления непреднамеренных внутренних угроз. Затем ослабьте воздействие таких лиц, внедрив дополнительные меры безопасности в отношении их учетных записей, систем, привилегий и доступа. Ваша служба безопасности может ограничить для сотрудников возможность совершать подрывные действия за счет строгих политик и мер контроля. Приведем примеры.

   - Запрет включать или выполнять макросы в системах.
   - Настройка электронной почты так, чтобы письма приходили в виде неформатированного текста без гиперссылок.
   - Помещение в карантин всех внешних вложений электронной почты.
   - Отключение просмотра веб-страниц или его включение только через изолированную интернет-систему, не подключенную к внутренней сети вашей организации.
   - Отключение USB-портов и внешних носителей на определенных системах.

   Мониторинг преднамеренных внутренних угроз требует как передовых методов обнаружения, так и технологий, поддерживающих секретность и обман. Нужный вариант следует выбирать в зависимости от результатов моделирования угроз в организации и оценки рисков.

2. **Внедрите защитные кадровые политики.** Когда перечисленные технические средства контроля и методы обнаружения будут внедрены, следует уделить внимание работе с персоналом. Убедитесь, что отдел кадров ведет учет действующих сотрудников, уволившихся и кандидатов, включая в их данные показатели *миномуси*. Задавайте во время собеседования точные вопросы, а также анализируйте результаты работы и разговоров перед увольнением, чтобы зафиксировать результаты.
3. **Исключите обстоятельства, которые порождают миномуси.** Отделу кадров следует внедрить общеорганизационные политики, соответствующие архетипам *миномуси*.
   - Изучайте дисциплинарные протоколы сотрудников, чтобы предотвратить несправедливые или чрезмерные наказания. Требуйте, чтобы сотрудники и кандидаты сообщали, работают ли в вашей организации какие-либо их родственники. Дайте отделу кадров указание выяснить, считают ли сотрудники примененные к ним дисциплинарные меры несправедливыми или чрезмерными, а затем совместными усилиями выработайте решения, позволяющие уменьшить враждебность сотрудников.
   - Регулярно проводите опросы работающих в компании для оценки их морального духа и выявляйте сотрудников низкого ранга, чьи способности используются не в полной мере. Проводите прозрачные интервью с персоналом и руководством, чтобы определить, готов ли сотрудник к продвижению по службе, оценены ли по достоинству его недавние достижения, нуждается ли он в обучении в определенной сфере. Возможно, кто-то считает, что достоин повышения зарплаты или должности. Кто-то может считать, что работает лучше коллег. Совместно с руководством подумайте, как снизить озлобленность сотрудников и как в целом улучшить их взаимоотношения с компанией.
   - В рамках оценки эффективности с помощью коллег определите менеджеров, которых сотрудники низкого ранга считают наиболее ценными, а также тех, кто считает, что не получает должного признания. Устраните эти обиды вознаграждением и/или учитывайте их при принятии организационных решений.
   - Пересмотрите политики и перестаньте использовать те, которые не дают талантам продвигаться наверх. Это могут быть соглашения об отказе от конкуренции, несправедливое присвоение интеллектуальной собственности сотрудников, недостаточные бонусы по результатам работы или иные стимулы. Эти средства нацелены на защиту компании, но их реальный эффект может оказаться противоположным.

- Открыто выясняйте у сотрудников и соискателей, не расходится ли их мироощущение с миссией вашей организации. Если имеется конфликт, назначьте этих сотрудников на должности, на которых их личностные приоритеты будут лучше соответствовать выполняемой работе.
- Разработайте методы выявления тех сотрудников, которых смогут переманить конкуренты. Рассмотрите возможность сузить их доступ к системе и понизить уровень привилегий, тем самым уменьшив полезность для злоумышленников.

Тесно взаимодействуйте с сотрудниками, которые с высокой вероятностью могут стать *миномуси*. Выделите им дополнительные ресурсы, время и мотивацию, чтобы сгладить возможные обиды, обеспечьте им возможности для личностного роста и простимулируйте их чувство собственного достоинства. Сведите к минимуму или исключите действия, которые порождают плохие воспоминания, и перестаньте припоминать сотруднику прошлые проступки.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, где есть ценная информация, сокровища и люди. Вы получаете достоверные сведения о том, что синоби планирует завербовать кого-то в вашем замке и использовать против вас то, что этому человеку доверяют и он обладает широкими возможностями. Вам дали список из восьми различных типов людей, которых синоби может завербовать. Неясно лишь, кто конкретно является целью или чего добивается синоби.

Кого вы заподозрили бы в первую очередь? Почему этот человек уязвим для вербовки и как вы могли бы исправить ситуацию? Как бы вы обнаружили вербовку одного из ваших подданных или поймали вербовщика? Как разместить охрану, чтобы предотвратить внутреннюю угрозу? Как научить людей сообщать о внутренних угрозах, не породив при этом междоусобицу? Как долго нужно поддерживать программу борьбы с внутренними угрозами?

Чтобы избежать этических ловушек, связанных с применением подобных тактик на вашем нынешнем рабочем месте, подумайте о создании и использовании списка бывших сотрудников. Если вы сможете выполнять это упражнение с небольшой группой заинтересованных лиц, можно перейти к рассмотрению действующих сотрудников.

Рекомендуемые меры безопасности и предосторожности

В некоторых случаях можно использовать рекомендации и принять меры безопасности, приведенные в стандарте NIST 800-53. Их следует оценивать с учетом концепции внутренних угроз. (Для получения дополнительной информации см. PM-12. Программа борьбы с внутренними угрозами.)

1. Дайте SOC задание работать совместно с отделом кадров, чтобы сопоставить информацию о потенциальных внутренних угрозах, подходящих под архетип *миномуси*. SOC должны более внимательно отслеживать и проверять лиц с высоким уровнем риска, а также ограничивать их возможности. Также совместно с отделом кадров можно разработать ловушки для инсайдерских угроз, например файлы в общих сетевых ресурсах с надписью «ЗАПРЕЩЕНО, НЕ ОТКРЫВАТЬ», с помощью которых можно определить сотрудников, склонных к вербовке. (AC-2. Управление учетными записями | (13) Отключение учетных записей для лиц с высоким уровнем риска; AU-6. Аудиторский обзор, анализ и отчетность | (9) Корреляция с информацией из нетехнических источников; SC-26. Приманки.)
2. Используйте свою учетную запись для выполнения действий внутреннего злоумышленника (без использования «красной команды») над файлами и системами, которые, как вы знаете, не причинят вреда компании. Это может быть изменение или удаление данных, вставка ложных сведений или кража данных. Запишите, к каким системам и данным ваша учетная запись может получить доступ, а затем примените привилегированную учетную запись администратора или root-пользователя для выполнения привилегированных вредоносных действий. Например, вы можете создать нового администратора с несуществующим именем. Узнайте, может ли SOC обнаружить, какие данные вы украли, удалили или изменили в течение определенного времени, и проверьте качество их аудита выполненных вами действий. (AC-6. Наименьшие привилегии | (9) Аудит использования привилегированных функций; CA-2. Оценка безопасности | (2) Специализированные оценки.)
3. Обучите своих сотрудников опознавать *миномуси* и в целом вредительское поведение. Дайте сотрудникам возможность быстро и анонимно сообщать о возможных внутренних угрозах и сотрудниках-*миномуси*, как и о фишинговых атаках. Проведите обучение по информированию о внутренних угрозах в рамках обычного обучения по вопросам безопасности. (AT-2. Осведомленность о безопасности | (2) Внутренние угрозы.)

Резюме

В этой главе мы рассмотрели технику синоби по вербовке уязвимых людей в целевой организации для совершения злонамеренных действий. Подробно описали восемь архетипов кандидатов на должность внутренней угрозы и обсудили различные типы программ обнаружения и защиты от внутренних угроз, которые в настоящее время используются организациями. Мы описали новый вдохновленный трактатами синоби подход, согласно которому нужно посочувствовать недовольному сотруднику. В упражнении в этой главе было предложено оценить не только потенциальных внутренних врагов, но и собственные действия по отношению к коллегам, что в конечном итоге позволяет организовать работу по предотвращению угроз совместными усилиями.

В следующей главе мы обсудим инсайдеров на перспективу — сотрудников, нанятых противником до того, как они переступили порог вашей компании. Поскольку эти люди намеренно скрывают любое недовольство компанией, их обнаружение становится еще более проблематичным.

14

Призрак на Луне

Согласно японской легенде, если вы сумеете найти призрака, который ухаживает за деревьями на Луне, он пригласит вас на Луну и угостит листьями с дерева, сделав вас невидимым.

В мирное время, прежде чем возникнет необходимость, вы должны завербовать тайного агента, который станет предателем, которого вы внедрите в стан врага, словно призрака, который в легенде Кацура-отоко находится на Луне.

«Бансэнсюкай», ё-нин I [5]

В числе прочих наиболее изощренных методов проникновения «Бансэнсюкай» описывает долгосрочную тактику открытой маскировки под названием «призрак на Луне». Эта тактика была разработана для получения конфиденциальной информации и доступа через специально размещенного секретного агента. Сначала синоби вербует человека, который заслуживает доверия, умен, мудр, отважен и верен. Если же рекрут не отличается верностью, в трактате предлагается взять в заложники кого-то из его семьи, чтобы он был посговорчивее. Затем синоби отправляет агента в чужую провинцию или замок. Тот проводит там долгие годы, усердно работает над своей миссией, создает себе репутацию, приобретает связи, знания и получает доступ во многие места. В идеале он должен работать в тесном контакте с вражеским руководством.

Для связи с синоби агент должен использовать правдоподобные, надежные и заметные средства. Если вражеский замок когда-либо станет целью для атаки, синоби может вызвать секретного агента для получения от него разведданных или помощи, совершения саботажа и иных атакующих действий, включая убийства [5]. Пусть даже вклад в такого агента может окупиться лишь через долгие годы, для терпеливого и последовательного синоби достижение цели будет стоить потраченного времени.

В этой главе мы рассмотрим тактику «призрака на Луне» как разновидность внутренней угрозы. В этом контексте представим аппаратные имплантаты как попытку найти призрака на Луне с помощью телескопа. По этой причине мы затронем тему имплантатов, безопасности цепочки поставок и скрытых аппаратных бэкдоров. Мы сравним характеристики растения, которое выращивает призрак на Луне, с идеальными аппаратными имплантатами. Поговорим об управлении рисками в цепочке поставок и стратегиях поиска угроз, отметив, что существуют проблемы, из-за которых избавиться от угрозы полностью будет просто невозможно.

Имплантаты

Корпоративный шпионаж и государственный шпионаж исторически основывался на агентах, которые выполняли долгосрочные миссии. Сегодняшние технологии порождают новые и более дешевые способы получения результатов, которые раньше можно было получить только с помощью людей. Предположим, что ваша организация много лет назад купила и установила в своей сети маршрутизатор иностранного производства и он отлично работает. Но в какой-то момент злоумышленник активирует установленный еще на заводе скрытый имплантат, обеспечивающий прямой доступ к важным системам и данным в обход всех фильтров и системы безопасности.

Индустрия кибербезопасности классифицирует этот вид атаки как *атаку на цепочку поставок*. Здесь под *цепочкой поставок* понимаются продукты и услуги, связанные с коммерческой деятельностью или системами организации. Это может быть оборудование, программное обеспечение и облачные хостинги. В рассмотренном примере маршрутизатор выполняет требуемую от него в сфере электронной торговли бизнес-задачу по перемещению информации по сети.

Эвристика или методы поиска угроз способны обнаружить аномальное поведение маршрутизатора, но надежного способа защиты от скрытых имплантатов не существует. Некоторые компании привлекают специалистов по обеспечению качества для мониторинга производства, но и они не могут гарантировать, что все системы построены правильно. Однако существуют передовые методы кибербезопасности, способные сгладить последствия атак цепочки поставок через маршрутизатор. Например, компания могла бы сделать следующее.

1. Проанализировать на наличие угроз маршрутизаторы всех производителей и, основываясь на результатах анализа, приобрести маршрутизатор, который с меньшей вероятностью будет содержать скомпрометированное оборудование или программное обеспечение.

2. Использовать надежную и безопасную службу доставки для предотвращения злонамеренного перехвата во время приобретения маршрутизатора.
3. Провести экспертизу маршрутизатора после его получения и подтвердить, что он не был скомпрометирован и соответствует ожидаемым спецификациям.
4. Защитить маршрутизатор с помощью средств защиты от несанкционированного доступа и технологий обнаружения, чтобы выявить и предотвратить несанкционированные изменения.

Обратите внимание на то, что подобные меры могут касаться не только маршрутизаторов. Компании могут принимать подобные меры предосторожности в отношении всех служб, устройств, систем, компонентов и программных приложений в своей цепочке поставок.

Скрытые имплантаты так же ценны для современных государств, как и для синоби, потому что необходимость находить их и защищаться от них создает сложные и долгосрочные организационные проблемы. Специалисты по кибербезопасности постоянно тестируют новые способы решения этих проблем. Например, организация может меньше доверять системам, которые ранее были скомпрометированы, и ограничить к ним доступ. Но значительное влияние подобных ограничений на бизнес-операции делает их применение практически невозможным.

Защита от имплантатов

Компании, которые будут пытаться оценить или проанализировать каждую систему в поисках следов преступления, скорее всего, запутаются в процессе управления цепочкой поставок. Более того, продвинутые злоумышленники, способные скомпрометировать цепочку поставок, скорее всего, научатся внедрять вредоносные функции в стандартную структуру системы, не добавляя ничего лишнего. Таким образом, только злоумышленник будет знать об имплантате, который будет добавлен в каждую систему. Возможно, в ходе инспекции компания даже обнаружит угрозу, но не сможет распознать ее. В этом и заключается масштаб проблемы — это все равно что пытаться найти призрак на Луне. Тем не менее для защиты организации от подобных имплантатов можно принять следующие меры.

1. **Определить условия атаки на цепочку поставок.** Составьте список компонентов вашей цепочки поставок, которые могут стать призраками. Перечислите элементы, которые:
   - считаются доверенными;
   - могут осуществлять связь;

- могут предоставлять косвенный или прямой доступ к конфиденциальной информации или системам;
- трудны в инспектировании;
- редко заменяются или обновляются.

В частности, обратите внимание на программное и аппаратное обеспечение, которое взаимодействует с внешними системами или управляет другими системами, осуществляющими связь (например, встроенное ПО на маршрутизаторах, сетевых интерфейсных картах (network interface card, NIC) и концентраторах VPN). Имплантат может иметь форму аппаратного устройства, например тонкого металлического блока в разъеме PCI, который играет роль посредника сетевой карты и влияет на поток данных, целостность, конфиденциальность и доступность сетевых коммуникаций для этого интерфейса.

Представьте, что ваш антивирус, гипервизор, сканер уязвимостей или анализатор не может выполнять тестирование в вашей среде. «Призраки» в цепочке поставок должны уметь выживать в окружающей среде цели, поэтому должны состоять из компонентов, которые долго не ломаются и не изнашиваются, которые нелегко модернизировать или заменить более дешевыми аналогами, которые слишком важны, чтобы их можно было выключить или утилизировать, которые сложно изменить и обновить (например, микропрограммное обеспечение, BIOS, UEFI и MINIX). Требования к автономности и скрытности для этого класса имплантатов цепочки поставок таковы, что имплантат должен избегать проверок, сканирования и других типов тестирования целостности, имея при этом доступ к командам процессора.

2. **Защитить цепочку поставок.** Внедрите меры безопасности и защиты в цепочке поставок там, где это необходимо. Атака «призрак на Луне» в цепочке поставок — одна из самых сложных для обнаружения, предотвращения или смягчения последствий. Поэтому многие компании просто принимают или игнорируют этот риск. Вы можете начать с разработки основных принципов — фундаментальных понятий о безопасности и целях вашего бизнеса, а затем использовать их в качестве критерия оценки угрозы, с которой сталкивается организация. Ознакомьтесь с публикацией Зальцера и Шредера *A Contemporary Look at Design Principles* (1975 год) [31] и другими важными работами по вопросам безопасности, которые помогут вам определить меры по устранению угрозы. Также бывает полезно обобщить проблемы до концепций более высокого уровня, на котором они станут знакомыми и понятными, а затем решить их. Рассмотрим упражнение.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Вы получаете достоверную информацию о том, что один из ваших писцов — вражеский «призрак на Луне». Он последние 10 лет учился копировать ваш почерк, манеру разговора и методы запечатывания писем, запомнил имена и адреса всех ваших важных контактов. Он в состоянии подменить ваши приказы, например направить вашу армию далеко от ключевых оборонительных позиций. Неясно, кто из писцов является агентом и активирован ли он вражеским синоби. Писцы — дефицитный ресурс в вашем государстве, их нахождение и обучение требует больших затрат и времени, а их работа критически важна.

Как определить, кто из писцов — вражеский агент, причем как до, так и после активации? Подумайте, какие меры предосторожности могут помешать писцу отправлять поддельные приказы от вашего имени. Какие протоколы аутентификации позволили бы предотвратить подделку сообщений? Какие меры по обеспечению целостности сообщений позволили бы предотвратить их подделку? Какие меры позволили бы не поверить ложным сообщениям, отправленным от вашего имени? Как гарантировать, что будущие писцы не окажутся скомпрометированы врагом? Наконец, рассмотрите все эти вопросы в сценарии, в котором сразу несколько писцов завербованы врагом.

Рекомендуемые меры безопасности и предосторожности

1. Рассмотрите возможность внесения неоднородности в цепочку поставок путем выделения, сегментации и разделения разных ее компонентов. Разнообразие цепочки поставок значительно снижает потенциальное влияние скомпрометированных компонентов. (SC-29. Неоднородность.)
2. Проанализируйте процесс закупок вашей организации и определите области, в которых вы можете снизить риск атаки на цепочку поставок. Используйте слепые закупки, надежные службы доставки, ограничение покупок в определенных компаниях или странах, другой язык в контрактах на закупку, а также рандомизацию или уменьшение до минимума времени закупки. (SA-12. Защита цепочки поставок | (1) Стратегии/инструменты/методы закупок.)
3. Постарайтесь как можно дольше откладывать обновления, не связанные с безопасностью, равно как и закупку нового, непроверенного программного обеспечения, оборудования и услуг. Внедрите передовые контрмеры

и ограничьте для изощренных злоумышленников возможность атаковать вашу организацию. (SA-12. Защита цепочки поставок | (5) Ограничение вреда.)

4. Приобретите или оцените несколько экземпляров одного и того же оборудования, программного обеспечения, компонента или услуги у разных поставщиков и попробуйте выявить изменения или неоригинальные элементы. (SA-12. Защита цепочки поставок | (10) Проверка подлинности и оригинальности; SA-19. Подлинность компонентов; SI-7. Программное обеспечение, микропрограммное обеспечение и целостность информации | (12) Проверка целостности.)
5. Внедрите независимые механизмы внеполосного мониторинга и тесты работоспособности, чтобы убедиться, что компоненты с высоким уровнем доверия, подозреваемые в атаке на цепочку поставок, не создают скрытых соединений и не изменяют потоки данных. (SI-4. Мониторинг информационной системы | (11) Анализ аномалий в трафике | (17) Интегрированная ситуационная осведомленность | (18) Анализ трафика/скрытая эксфильтрация.)

Резюме

В этой главе мы рассмотрели технику синоби, в рамках которой они вербовали надежных людей, которые должны были внедриться в организацию и приносить пользу синоби. Мы сравнили эту тактику с аппаратными имплантатами и обсудили, какие устройства и системы подходят для аппаратных имплантатов. Мы поговорили об атаках на цепочки поставок, а также о способах их обнаружения. В упражнении вам было предложено выявить скомпрометированного писца, имеющего привилегированный доступ к переписке. Писец — это аналог маршрутизатора, VPN или другого устройства третьего уровня, которое должно быть прозрачным для коммуникаторов, что лишь усложняет поиск неполадок в таком устройстве.

В следующей главе мы обсудим резервный план синоби на случай, если внедренный агент будет пойман. Часто синоби заранее, задолго до своей тайной миссии, подбрасывают ложные доказательства, чтобы снять с себя вину в случае провала. В случае успеха эта тактика заставляет жертву поверить в предательство союзника, что само по себе полезно.

15

Способ светлячка

Способ светлячка должен применяться лишь после того, как вы узнаете о противнике все в мельчайших подробностях, чтобы обман был спланирован в соответствии с мышлением жертвы.

Перед тем как начать наблюдение или другую
операцию синоби, оставьте записку на будущее.
«Ёсимори хяку-сю», № 54

В «Бансэнсюкай» описывается техника проникновения с открытой маскировкой для синоби, называемая способом светлячка (хотаруби-но дзюцу) [5]. Я думаю, она была названа в честь вспышки светлячка, которая на мгновение остается у вас перед глазами, заставляя вас ловить руками воздух, когда насекомое уже улетело. «Сёнинки» описывает эту же технику как искусство маскировки [7]. Используя ее, синоби размещает в нужном месте улику, которая заставляет врага предпринимать какие-то действия, в том числе неверно определять, на кого работает синоби, делать ложные предположения о его мотивах и опрометчиво реагировать на попытки атаки, становясь еще уязвимее.

Поддельные письма с дезинформацией или ложными данными о противнике применялись часто и в разных вариантах. В трактатах описывается, как синоби зашивали такое письмо в воротник, чтобы его можно было быстро найти в случае поимки или обыска [5]. Также синоби мог нанять инициативного, но неумелого человека на роль «ниндзя», дать ему письмо с ложными сведениями и отправить на задание в стан противника, зная, что этот «ниндзя» обречен на провал и будет пойман. Важно отметить, что сами рекруты об этой части плана не знали. При обыске новобранца охранники находили фальшивое письмо, в котором говорилось, что один из высокопоставленных командиров является, к примеру, заговорщиком. «Ниндзя», скорее всего, не выдерживал пыток и подтверждал подлинность сообщения, лишь ухудшая ситуацию для объекта провокации [5]. Все это позволяло обмануть врага и заставить его напасть на собственных союзников.

В еще более сложном варианте синоби тщательно готовил доказательства, подтверждающие информацию, содержащуюся в поддельном письме, и помещал последнее в доступное место, например в апартаменты доверенного советника вражеского командира. Подделанное письмо становилось своего рода спасательным кругом. Если бы синоби поймали, он бы терпел пытки ровно столько, сколько требовалось, чтобы выведать планы врага, а затем рассказывал о письме. Враг находил фальшивое письмо и связанные с ним доказательства. Заслужив доверие, синоби обещал стать двойным агентом или раскрыть секреты своего господина в обмен на жизнь [5]. Это позволяло сбить противника с толку, чтобы он начал сомневаться в том, кто друг, а кто враг.

В этой главе мы рассмотрим проблемы, связанные с определением источника угрозы. Рассмотрим, как определить его с точки зрения аналитики угроз, видимых доказательств и поведенческих оценок. Мы также поговорим о более серьезных противниках, которые знакомы с методами определения источника угрозы и умеют противостоять последним. Чем больше внимания защитник уделяет определению такого источника, тем более сложной будет работа киберпреступника, поэтому мы также обсудим способы устранения повышенного риска.

Определение источника угрозы (атрибуция)

Атрибуция в кибербезопасности — это анализ наблюдаемых доказательств для идентификации субъектов в киберпространстве. Доказательства могут принимать разные формы. Поведение злоумышленника, инструменты, методы, тактики, процедуры, возможности, мотивы, намерения и другая информация — все это позволяет сформировать полезный контекст и стимулирует реагирование на инциденты в области безопасности.

Предположим, у вас дома сработала сигнализация, что означает разбитое окно. Ваша реакция будет различной в зависимости от атрибуции: пожарный, который ворвался в дом, чтобы потушить огонь, — это не то же самое, что грабитель, пробравшийся с целью украсть ваши вещи, или шальной мяч для гольфа, попавший именно в ваше окно. Разумеется, правильная атрибуция — это не всегда просто. Вор может несколько усложнить опознание, надев перчатки и маску. Также он может переодеться в пожарного, чтобы скрыть свою личность и обманом заставить хозяев впустить его. Вор может подбросить, уничтожить или замести за собой следы преступления во время или после его совершения, усложняя дальнейшую работу следователей. По-настоящему хитрый преступник может даже подставить другого человека, используя поддельные отпечатки пальцев, украденные образцы волос, крови или предметы одежды, реалистичную маску, напечатанную на 3D-принтере, или оружие, приобретенное у ничего не подозревающего простофили. Если у обвиняемого нет алиби или есть мотив для совершения этого преступления, у властей будут все основания для ареста бедолаги.

С этими и другими проблемами атрибуции сталкиваются специалисты по кибербезопасности. Она осложняется из-за присущей киберсреде анонимности. Даже после выполнения непростой задачи по отслеживанию атаки вплоть до физического адреса компьютера специалисту по кибербезопасности может быть чрезвычайно сложно определить личность злоумышленника. Чтобы отследить на скомпрометированной машине, откуда он, приходится блуждать по туннелям, VPN, шифрованию и арендованным машинам, где нет внятных журналов или доказательств. Особо хитрые злоумышленники могут даже взламывать чужие машины, удаленно подключаться к ним и использовать их в качестве плацдарма для атаки на другие системы. После обнаружения злоумышленника стоит не блокировать его сразу же, а некоторое время последить за ним, чтобы определить его личность и цели[1].

Иногда хакеры специально оставляют после себя инструменты или другие доказательства, чтобы «помочь» в составлении атрибуции. Известно, что Соединенные Штаты, Россия и Северная Корея изменяли или копировали сегменты кода, инфраструктуру и артефакты своих киберинструментов, чтобы следствие пошло по ложному следу [13]. Когда специалисты по кибербезопасности обнаруживают и исследуют функционал особо скрытных вредоносных программ, иногда им удается обнаружить в коде уникальные строки. Возможно, их просто упустили из виду — и тогда это ошибка разработчика. Но они могут быть и ложными доказательствами, предназначенными для обнаружения и неверной атрибуции.

Обратите внимание на то, что для обмана и для идентификации личности используются одни и те же инструменты. Дампы памяти, образы дисков, реестры, кэши, сетевые записи, журналы, сетевые потоки, анализ файлов, код, метаданные и многое другое позволяют выявить субъекта киберугрозы. Различные разведывательные дисциплины, такие как сигнальная разведка (signal intelligence, SIGINT), киберразведка (cyber intelligence, CYBINT) и разведка по открытым источникам (open source intelligence, OSINT), также вносят свой вклад в атрибуцию, а разведка по человеческим источникам (human intelligence, HUMINT) позволяет собирать данные из определенных источников, которые после обработки и анализа помогают определить источник кибератаки. Эти возможности обычно держатся в секрете, так как если злоумышленники узнают об их существовании, они смогут научиться обходить их и усложнить процесс атрибуции.

Подходы к атрибуции

Организациям, разумеется, хочется знать, кто атакует их системы и сети и откуда это делается. Понятно, что иногда даже хочется предпринять ответные меры вплоть до

[1] Более подробно это описано в книге: *Stoll C.* The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York: Pocket Books, 2005.

взлома, чтобы узнать личность злоумышленника. Вот только они, как и синоби, всегда найдут способы скрыть свое имя посредством отрицания и обмана, внося в атрибуцию немалую неопределенность. Кроме того, история учит нас, что необходимость в определении личности синоби исчезла лишь после того, как Япония объединилась и в ней воцарился мир, а синоби канули в Лету. В обозримом будущем мир вряд ли объединится, поэтому кибератаки между государствами, скорее всего, никуда не денутся. Ну а пока мир во всем мире не наступил, приведенные далее подходы к атрибуции способны помочь вам определить, что вы можете сделать с киберконфликтами.

1. **Избавьтесь от когнитивных искажений.** Оцените свои когнитивные искажения и логические ошибки. Слабые места в рассуждениях есть у всех, но мы можем помнить о них и работать над их исправлением. Исследуйте тему. Пересмотрите прошлые суждения, которые оказались неверными, определите, в чем была ваша ошибка, и подумайте, как улучшить свои аналитические способности. Эту задачу можно выполнять постепенно, маленькими (логические головоломки, кроссворды и головоломки — отличный способ улучшить когнитивные функции) или большими шагами. Вы можете читать статьи и книги по психологии, из которых можно много узнать о когнитивных искажениях и логических ошибках. Затем, вооружившись новыми знаниями, вы можете избавиться от собственных ошибок[1].
2. **Обеспечьте возможности выполнения атрибуции…** Определите, какие источники данных, системы, знания и элементы управления вы можете использовать, чтобы организовать атрибуцию в вашей компании. Применяется ли в компании открытый незащищенный вайфай, который позволяет незарегистрированным и неопознанным лицам анонимно подключаться к вашей сети и инициировать атаки? Разрешают ли ваши маршрутизаторы использование поддельных IP-адресов, задействуются ли технологии защиты обратной пересылки (reverse-path forwarding, RFP) для предотвращения анонимных атак изнутри вашей сети? Правильно ли вы публикуете политику отправителя, предотвращая подделку адресов электронной почты злоумышленниками и действия под видом сотрудника организации?

   Многие из перечисленных изменений конфигурации не влекут за собой прямых затрат ресурсов, но на внедрение таких широкомасштабных изменений потребуются труд, время и иные затраты, что может затормозить развитие бизнеса. Но тут стоит задуматься о том, поможет ли установить преступника принятое ранее решение купить хорошие камеры и обеспечить хорошее освещение у кладовщика. Введение методов ведения журналов, документации и сбора доказательств расширяет возможности атрибуции, улучшает

[1] Для получения дополнительной информации см.: *Heuer R. J., Randolph Jr., Pherson H.* Structured Analytic Techniques for Intelligence Analysis. Los Angeles: CQ Press, 2015.

технологическую подотчетность и позволяет конечным пользователям лучше видеть сетевые угрозы.

3. **…или вообще забудьте об атрибуции.** Совместно с заинтересованными лицами в вашей компании определите, сколько в целом сил и времени нужно уделять атрибуции. Для организаций, способных перехватывать субъекты угрозы или предпринимать контрнаступление, атрибуция обязательна. Однако многие компании не могут и не пытаются ловить или атаковать злоумышленников, выяснять их личность или возможности. И действительно, определение конкретного субъекта угрозы требуется не всегда. Для анализа угрозы и защиты от нее может быть достаточно знать о ней.

   Например, предположим, что два злоумышленника посягают на интеллектуальную собственность вашей организации. Один хочет продать ее на черном рынке и заработать, а другой — использовать для создания систем вооружения для своей страны. Но на самом деле разницы между ними нет. Независимо от цели злоумышленников и способности организации их отследить, защитники должны думать о том, как не допустить самого проникновения. Не обязательно оценивать мотивацию злоумышленника, чтобы защититься от угрозы.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Ваши охранники поймали незнакомца, который роет туннель под одной из стен замка. В ходе допроса с пристрастием выяснилось, что ему заплатили за то, чтобы он вырыл туннель до амбара, а бандиты позже могли украсть припасы. Охранники обыскивают заключенного и обнаруживают у него записку с инструкциями о том, как связаться с одним из ваших доверенных советников. В записке говорится, что советник планирует поднять восстание против вашего правления, лишив жителей еды. Сообщение выглядит подлинным. Ваши охранники не могут идентифицировать ни злоумышленника, ни его нанимателя.

Подумайте, как можно выполнить атрибуцию и определить, кто злоумышленник, откуда он, какова его мотивация и на кого он может работать. Как проверить утверждение незнакомца о том, что его конечная цель — именно украсть еду, а не уничтожить ее или не проложить путь для другого злоумышленника, который собирается напасть на жителей замка или даже начать восстание? Как проверить, причастен ли советник к замыслам врага? Что бы вы предприняли, если бы нашли дополнительные доказательства атрибуции злоумышленника? А если нет?

Рекомендуемые меры безопасности и предосторожности

Рекомендации следует оценивать с учетом концепции атрибуции.

1. Привязывайте учетные записи к личности пользователей. Подтвердите личность человека, связанного с учетной записью, с помощью биометрических данных, идентификации, логических или физических доказательств или средств контроля доступа. (SA-12. Защита цепочки поставок | (14) Идентичность и прослеживаемость.)
2. Разработайте для организации план оценки атрибуции агентов угроз. (IR-8. Реагирование на инциденты.)
3. Разработайте программы осведомленности об угрозах, в рамках которых можно собирать и распространять информацию о характеристиках субъектов угроз, способах их идентификации в вашей среде, доказательствах атрибуции и другие данные. Используйте для сбора данных атрибуции специальные методы, например приманки. (PM-16. Программа осведомленности об угрозах; SC-26. Приманки.)
4. Применяйте меры безопасности и собирайте сведения. Смоделируйте угрозы для выявления их источников. (SA-8. Разработка принципов безопасности и конфиденциальности.)

Резюме

В этой главе мы рассмотрели способ светлячков — методики ложной атрибуции, используемые синоби. Хакеры постоянно совершенствуются в своем ремесле, поэтому, вероятно, будут использовать этот метод в своей работе, а может, уже делают это. Мы отметили, что в некоторых типах угроз уже сейчас применяются методы неправильной атрибуции, и обсудили подходы к работе с атрибуцией, а также поговорили о ее мрачном будущем.

В следующей главе мы обсудим тактику синоби по правдоподобному отрицанию вины во время допроса. Будут рассмотрены также передовые методы допроса синоби и инструменты, используемые при поимке вражеских синоби.

16

Взять живым!

Важно правильно определить, действительно ли цель невнимательна или она лишь притворяется, пытаясь заманить ниндзя в ловушку

Если во время ночного патрулирования вы обнаружили подозрительного человека, нужно во что бы то ни стало взять его живым.

«Ёсимори хяку-сю», № 74

Частью повседневной работы синоби всегда были убийства, но «Бансэнсюкай» рекомендует брать врагов, особенно чужих ниндзя, живьем, а не убивать. Допрос захваченного ниндзя позволяет синоби узнать, что злоумышленник уже совершил или еще планирует совершить, определить его нанимателя, выведать ценные секреты и навыки. Все это может помочь защититься от атак в будущем и правильно оценить стратегические угрозы. Кроме того, захваченный враг мог оказаться замаскированным союзником, а это не всегда можно выяснить без глубокого допроса [5]. Трактат «Нимпидэн» гласит, что подозреваемый ниндзя должен быть связан по рукам и ногам и посажен на поводок. Также он рекомендует использовать приспособления вроде кляпа с шипами, чтобы пленник не мог говорить, поскольку опытный ниндзя может подать сигнал союзникам, убедить охрану освободить его или даже откусить себе язык, чтобы совершить самоубийство[1].

В трактатах говорится, что захватить вражеского ниндзя живым нелегко. В «Бансэнсюкай» упоминается метод, в котором мушкет заряжался кусочком ваты, обсыпанным порошком чили. Получался древний аналог перцового баллончика. При выстреле с близкого расстояния этот снаряд создавал невыносимое раздражение в глазах и носу цели, делая ее уязвимой для захвата. Трактаты описывают и более сложные приемы, такие как засады и ловушки *фуши-камари*. Например, ловушка

[1] Стихотворения 6–10.

для тигра (*могари* или *кораку*), описанная в «Бансэнсюкай», создавалась для поимки тигров, как следует из названия, но позже была модернизирована для захвата ниндзя. В ней используются преграды, которые ведут злоумышленника через лабиринт скрытых ловушек. Союзники всегда знают правильный путь, а ниндзя, проникающий в одиночку ночью, маршрута не знает, что повышает вероятность попадания в ловушку. Еще один тип ловушки называется *цуиритей*, или поддельная стена. Ловушка представляет собой облицовку, которая выглядит как настоящая стена, но состоит из клиньев и ложных столбов. Когда ниндзя пытается забраться на такую стену, она рушится, ниндзя падает, получает увечья и попадает в руки защитников.

«Бансэнсюкай» описывает способы защиты от захвата, а также обнаружения и обхода ловушек *фуши-камари*. Синоби советуют изучать леса, поля, долины, овраги и другие места на предмет неестественного поведения птиц и животных, наличия помятой травы, так как все это может быть признаком ловушки. Необычные запахи тоже могут быть признаком засады [5]. На территории врага синоби могут использовать ряд тактик уклонения, в том числе:

- **перепелиное гнездо (узура-гакуре).** Синоби сворачивается в клубок на земле и старается быть невидимым для врага и не подавать признаков жизни. Даже когда охранник толкал ниндзя копьем или мечом, тот не должен был реагировать;
- **отступление енотовидной собаки (тануки-ноки).** Убегая пешком, синоби рисковал быть пойманным более быстрым преследователем. Когда дистанция между ними сокращалась, синоби внезапно падал на землю и направлял свой меч на преследователя, пронзая его прежде, чем тот успевал среагировать;
- **отступление 100 петард (Hyakurai-Ju).** Синоби размещал рядом с целью петарды, зажигая их самостоятельно с некоторой задержкой либо договариваясь об этом с союзниками. Звук отвлекал преследователей противника;
- **лисьи прятки (кицунэ-гакуре).** Синоби сбегал от преследования, двигаясь по вертикали. Вместо того, чтобы пытаться бежать с вражеской территории, двигаясь из точки А в точку Б, синоби забирался на высокое дерево или прятался в канаве. Эта тактика часто ставила в тупик врага, который не всегда додумывался посмотреть в поисках цели вверх или вниз.

Были и другие методы побега: например, синоби имитировал звуки, издаваемые собакой или другим животным, чтобы обмануть преследователей, или лгал врагу, чтобы ввести его в заблуждение и бежать [5]. Синоби, знавший, что за ними следят, мог притвориться, что не слышит преследователей, и говорил что-то воображаемому союзнику так, чтобы его услышали. Если синоби говорит: «Давай тихонько пойдем в спальню хозяина и убьем его во сне», охранники, скорее всего, отправятся туда, позволяя синоби сбежать в другом направлении.

Конечно, лучший для синоби способ избежать захвата — это не оставлять за собой следов того, что атака вообще произошла. Трактаты подчеркивают: важно выполнить задачу, не оставляя следов, чтобы у цели не было причин подозревать, что здесь действовал синоби. Руководство по тайным операциям весьма обширно и красочно описывает все это. «Ёсимори хяку-сю» № 53 гласит: «Если вам нужно что-то украсть, когда идет снег, ваш злейший враг — это ваши же шаги» [6].

Захват противника живьем, увы, для многих организаций не является приоритетом. Обнаруживая угрозу в системе, компании часто делают противоположное тому, что рекомендуется в трактатах синоби: немедленно отключают машину, стирают все данные, переформатируют диск и устанавливают новую версию операционной системы. Реакция вида «стер и забыл» устраняет угрозу, но также исключает любую возможность поймать того, кто угрожает, не говоря уже о расследовании или анализе злоумышленника целей, как уже достигнутых, так и потенциальных.

В этой главе мы обсудим важность перехвата киберугроз и взаимодействия с ними, пока они «живы». Рассмотрим существующие методы анализа или захвата, а также способы, которыми злоумышленники могут попытаться избежать последнего. Мы рассмотрим способы перехвата киберугроз «живьем» с помощью тигровых ловушек и приманок — методов, на разработку которых вдохновили древние синоби. Кроме того, мы рассмотрим современные реализации тактик уклонения синоби (например, прятки в стиле перепелов и лисиц), которые используются в долговременных угрозах. Наконец, рассмотрим большую часть рекомендаций по захвату и допросу из трактатов синоби и узнаем, как правильно контролировать угрозу, чтобы она не могла предупредить своих союзников или самоликвидироваться.

Живой анализ

В кибербезопасности экспертиза компьютера может обеспечить необходимый анализ угроз. Образы для экспертизы обычно создаются после инцидента безопасности (например, заражения вредоносным ПО) или нарушения правил использования (например, загрузки на устройство детской порнографии), причем создание образа выполняется таким образом, чтобы сохранить доказательства, не нарушив целостность данных на устройстве. Данные экспертизы могут помочь специалистам по безопасности узнать, в чем заключалась угроза и как она использовала уязвимости системы. Затем экспертиза может предоставить информацию, необходимую для разработки сигнатур, мер защиты и упреждающей блокировки. Например, понимание того, что злоумышленник хотел раздобыть определенную интеллектуальную собственность в определенной системе, говорит защитникам о необходимости защиты последней. Если экспертиза определит, что атака прошла успешно и конфиденциальные данные были скомпрометированы, организация может с помощью этих знаний разработать план дальнейших действий. Если атака не удалась, организация может подготовиться

к возможным последующим атакам. Полученные в ходе экспертизы индикаторы могут позволить понять, кто является источником угроз, а затем разработать ответные меры. Стратегия организации должна учитывать серьезности угрозы — был ли злоумышленник иностранным правительством, недовольным сотрудником или просто ребенком, занятым безобидным взломом.

Сбор данных устройства для анализа включает *живой захват* (он же *живой анализ*), а также *визуализацию* (также *экспертная визуализация,* или *зеркальное отображение*). Организации используют приманки и целые виртуальные среды для оперативного захвата и даже взаимодействия со злоумышленниками. Такие системы часто делаются такими, чтобы они привлекали хакеров или были легко доступны для вредоносных программ, поэтому когда угроза проникает в систему, скрытые средства ведения журналов и мониторинга фиксируют, что именно угроза делает, как делает и с какими данными взаимодействует. К сожалению, многие злоумышленники знают об этих приманках и проверяют, не находятся ли они в ненастоящей среде, предназначенной для сбора информации. Если подозрения подтвердятся, злоумышленник прекращает работу, сводя на нет все усилия службы безопасности. Устройства контроля доступа к сети (NAC) тоже могут перехватывать угрозы путем динамического переключения системы в зараженную среду VLAN, где угроза продолжает «жить» и ждет реакции защитников.

Экспертный анализ на живом захвате обычно не выполняется. Аналитик чаще изучает статические, инертные или мертвые данные, в которых определенная информация или уникальные детали угрозы могут быть утеряны. Обычно это наблюдается в бесфайловых вредоносных программах, которые хранятся в памяти, или во вредоносных конфигурациях или артефактах, например в кэше таблиц маршрутизации. Живой анализ не проводится по ряду причин, в числе которых:

- особые технологические требования;
- необходимость обходить организационные политики, требующие отключения-включения, карантина или блокировки скомпрометированных систем;
- отсутствие квалифицированных экспертных ресурсов, способных здесь и сейчас выполнить живой анализ;
- отсутствие у сотрудников доступа к жизненно важным системам во время расследования.

Важно отметить, что при неправильном выполнении анализа в реальном времени угроза может узнать о наличии в системе экспертного ПО и спрятаться, удалить себя, принять контрмеры или атаковать систему.

Чтобы ускользнуть от методов захвата, угрозы развертываются в несколько этапов. На начальном этапе угроза старается понять, не используются ли технологии

захвата, и загружает вредоносные программы и инструменты только после того, как будет ясно, что в зараженной среде можно безопасно работать. Такие меры предосторожности злоумышленнику необходимы, так как если его ПО будет перехвачено и проанализировано, информация об инструментах и методах, используемых угрозой, попадет к другим организациям и защитникам, что позволит им извлечь уроки из атаки, исправить проблему или разработать контрмеры. Правоохранительные органы могут задействовать тактику экспертизы для отслеживания злоумышленников или предоставления доказательств их противозаконной деятельности.

В последнее время наиболее хитрые хакеры переместились в те области работы с компьютерами и сетями, которые стандартные инструменты криминалистической экспертизы, захвата и анализа охватить не могут. К числу нововведений можно отнести, например, установку на жесткий диск прошивки, которая создает скрытую закодированную файловую систему, встраивание вредоносного ПО в хранилище BIOS, использование локального хранилища на микрочипе для работы за пределами обычной рабочей памяти, а также модификацию низкоуровневых модулей и кода сетевого оборудования, например маршрутизаторов, коммутаторов, принтеров и других устройств, которые обычно не участвуют в экспертизе. Некоторые угрозы имитируют базовую ОС или доверенные компоненты безопасности, проникая в них на уровне производителя, который тоже считается доверенным лицом и не рассматривается в рамках криминалистического анализа. Некоторые хакеры стирают следы своей работы, перемещаясь в память или в систему, которая редко перезагружается (например, контроллер домена), и ожидая там, пока утихнет шум и можно будет вернуться к первоначальной задаче.

Защита от угроз в реальном времени

Организации часто сталкиваются с инцидентами безопасности именно в тот момент, когда единственный человек, способный работать с инструментами криминалистической визуализации, отсутствует на рабочем месте. Иногда до момента передачи атакованной машины ему на проверку проходит несколько дней, а к тому времени атака уже закончилась. Неспособность действовать с той же или большей скоростью, что и угроза, заставляет защитников брать на себя функции эксперта, который собирает доказательства и устраняет последствия уже после того, как злоумышленник сделал все что хотел.

Заблаговременное создание ловушек, засад и возможностей для противостояния угрозе позволяет захватить ее живьем и тщательно допросить.

1. **Создайте возможности для проведения экспертизы.** Организуйте работу специальной группы, у которой есть оборудование, опыт, сертификаты

и полномочия для выполнения компьютерных криминалистических экспертиз. Создайте соответствующие инструменты с блокировщиками записи, защищенными жесткими дисками и другими специализированными программами и устройствами. Убедитесь, что в каждую систему, используемую для захвата и анализа, назначен криминалистический агент, чтобы группа могла немедленно идентифицировать, локализовать, изолировать угрозу и начать сбор данных. Убедитесь, что все сотрудники понимают, чем и как могут помочь группе криминалистов в идентификации и локализации ущерба, а также сборе доказательств. Если с момента экспертизы прошло больше месяца, проведите с группой экспертов курсы повышения квалификации или обучение. Самое главное, когда будет подготовлен отчет об экспертизе, прочтите его, чтобы выявить основные причины инцидентов безопасности, и примите меры для устранения уязвимостей.

2. **Разложите приманки.** При необходимости дайте вашей команде возможность устраивать засады на злоумышленников, а не просто следовать за ними по пятам. Для активного отлавливания угроз и охоты на них требуется тесное взаимодействие с облачными хостами, интернет-провайдерами, регистраторами, поставщиками услуг VPN, Центром жалоб на интернет-преступления (Internet Crime Complaint Center, IC3), финансовыми службами, правоохранительными организациями, частными охранными и коммерческими компаниями. Организуйте создание в сети области, враждебной для злоумышленников, в которой вы и ваши партнеры объединенными усилиями сможете устраивать засады на злоумышленников, собирать доказательства, а также выявлять используемые ими вредоносные программы, инструменты и эксплойты.

3. **Расставьте ловушки для тигров.** Рассмотрите возможность установки ловушек для тигров в вероятных целях в вашей сети, например в контроллере домена. Возможно, на рынке появится продукт, который выполнял бы функции производственной системы с возможностями настройки ловушек, срабатывающих в случае выполнения неправильного действия. Поскольку злоумышленники, пытающиеся обойти меры безопасности, обычно переключаются с одной системы на другую или перемещаются по системам и сетям, у вас может получиться установить ложные или заминированные переходы, которые на первый взгляд ведут в другую сеть, но на самом деле — прямиком в ловушку. Установите эти ловушки таким образом, чтобы неправильные действия заставляли систему приостановить работу, блокировать или изолировать атаку, что позволит защищающимся заблокировать угрозу или исследовать ее в режиме реального времени. Это можно сделать, заморозив тактовый сигнал процессора, заставив жесткий диск работать только в буферном режиме или используя гипервизор для перехвата и регистрации активности. Обучите системных администраторов и других ИТ-специалистов работать в системе, не попадая в ловушку.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Ваши охранники недавно поймали злоумышленника, которого сочли за ниндзя, быстро убили его и сожгли тело. Воины утверждают, что эти меры были приняты с целью устранить любой остаточный риск, который мог возникнуть из-за ниндзя. Когда вы спросили охранников, почему они вообще решили, что злоумышленник был ниндзя, что у него было при себе, что этот человек делал в замке и как он сумел в него проникнуть, охранники не смогли ответить. Вероятно, они даже ожидают похвалы за быстрое устранение угрозы с минимальным ущербом.

Какие более эффективные протоколы, процедуры и инструменты можно было бы разработать для ваших охранников, чтобы безопасно задерживать подозреваемых? Как бы вы допросили злоумышленника, если бы он действительно был ниндзя и пережил встречу с охранниками? Что бы вы искали в вещах ниндзя, если бы они не были сожжены? Как, по-вашему, ниндзя проник в ваш замок и как это доказать? Как бы вы обыскали свой замок, чтобы определить, совершил ли ниндзя саботаж, расставил ли ловушки и подал ли сигнал союзникам? Что бы вы спросили у охранника, который обнаружил ниндзя, и как его ответы могут помочь вам обучить других охранников? Что вы ожидаете узнать из этого расследования и какие действия можете предпринять на основе сделанных выводов?

Рекомендуемые меры безопасности и предосторожности

1. Ограничьте применение внешних систем и компонентов в организации, если у вас нет разрешения или возможностей проводить по ним экспертизу. (AC-20. Использование внешних систем | (3) Системы и компоненты, не принадлежащие организации.)
2. Используйте внешние датчики и SIEM, к которым трудно получить доступ, внедрите автоматизированные механизмы сбора данных в реальном времени, PCAP, системный журнал и другие средства, необходимые для криминалистического анализа. (AU-2. События аудита; AU-5. Действия в случае сбоев аудита | (2) Оповещения в реальном времени; IR-4. Обработка инцидентов | (1) Автоматизированные процессы обработки инцидентов; SA-9. Внешние системные службы | (5) Места обработки, хранения и обслуживания; SC-7. Граничная защита | (13) Изоляция инструментов, механизмов и вспомогательных компонентов.)

3. Если в качестве меры противодействия угрозам вы решите избавиться от постоянных компонентов, например, путем регулярного переоснащения или сброса всех ваших систем для уничтожения любого несанкционированного доступа, то рассмотрите возможность выполнения экспертизы перед повторным созданием образа и сохраните полученные доказательства существования угроз. (AU-11. Сохранение записей аудита | Долгосрочное восстановление; MP-6. Чистка носителей | (8) Удаленная очистка или стирание информации; SI-14. Непостоянство; SI-18. Удаление информации.)
4. Реализуйте, документируйте и применяйте в своей организации базовые конфигурации систем, чтобы аналитики легко смогли определить, какая информация могла быть изменена угрозой. (CM-2. Базовая конфигурация | (7) Настройка систем и компонентов в зонах высокого риска; SC-34. Неизменяемые исполняемые программы.)
5. Организуйте обучение и имитационные упражнения для ваших экспертов, чтобы повысить эффективность реагирования в случае нарушений безопасности в будущем. (IR-2. Обучение по реагированию на инциденты | (1) Моделируемые события.)
6. Организуйте группу экспертов-криминалистов, способную и уполномоченную выполнять сбор данных и расследования в режиме реального времени. (IR-10. Группа комплексного анализа информационной безопасности.)
7. Используйте меры предосторожности, чтобы убедиться, что в охраняемые системы и программное и аппаратное обеспечение никто не вмешивался. (SA-12. Управление рисками цепочки поставок | (10) Проверка подлинности и отсутствия изменений | (14) Идентичность и прослеживаемость.)

Резюме

В этой главе мы рассмотрели техники захвата и допроса синоби противника, а также тактики, позволяющие избежать захвата. Мы коснулись того, как сбор большего количества доказательств дает злоумышленнику больше возможностей для подлога данных, и поговорили о том, почему лучше взаимодействовать с живыми угрозами. Мы обсудили передовой опыт в области криминалистики в задачах отслеживания угроз, а также передовые методы противодействия угрозам, такие как засады и ловушки.

В следующей главе мы обсудим наиболее разрушительный способ атак в арсенале синоби — поджог.

17

Поджог

Во-первых, устроить пожар довольно легко, во-вторых, противнику трудно потушить огонь, и в-третьих, если ваши союзники в этот же момент будут атаковать замок, противник потеряет преимущество, так как часть сил будет перетянута в другое место.

Если вы собираетесь поджечь замок или лагерь врага,
вам нужно заранее согласовать время поджога
со своими союзниками.
«Ёсимори хяку-сю», № 83

Одна из самых впечатляющих вещей, которые может совершать проникший в замок или крепость синоби, — это устроить пожар, причем желательно на пороховых складах, складах дров, продовольствия, на мостах или около них. Правильно разведенный огонь быстро распространяется, оставаясь невидимым, сложно сдержать его распространение или потушить, и он становился серьезной угрозой для самого укрепления, запасов и жителей замка. Защитники замка вынуждены выбирать между тушением огня и борьбой с вражеской армией, напавшей прямо в момент пожара. Попытка выиграть обе эти битвы одновременно лишала цель возможности преуспеть в обеих. Тех, кто боролся с огнем, настигали атакующие солдаты, а те, кто не обращал внимания на огонь, в конечном итоге проигрывали битву независимо от того, насколько хорошо сражались [5].

В трактатах подробно рассказывается о совершении поджогов и приводятся описания различных инструментов, тактик и навыков, используемых для этого. Перед атакой синоби изучали жителей замка, чтобы определить, кто и когда спит и в какой момент ключевые позиции остаются без охраны. Затем они совместно с другими захватчиками определяли время. Синоби готовил множество специальных

инструментов для проведения атаки, таких как огненные стрелы, мины, бомбы и метательные факелы. Одним из самых страшных были «горящие лошади» — лошади с прикрепленными к седлам факелами, которые бешено носились внутри укреплений, хаотично поджигая все вокруг, отвлекая охранников и жителей и отказываясь успокаиваться [6]. Пользуясь суматохой, синоби связывался с силами, собравшимися за пределами замка, чтобы дать сигнал к атаке, когда огонь распространится достаточно сильно.

Средневековые армии умели проводить огневые атаки издалека, например, с помощью лучников, стреляющих огненными стрелами. «Бансэнсюкай» рекомендует вместо этого задействовать синоби. По сравнению с внешними атаками пожары, устроенные синоби, обнаруживают позднее и потушить их труднее. Кроме того, синоби мог целенаправленно поджечь место хранения горючих или стратегически ценных вещей и помочь пожару набрать достаточно силы [5].

Успех огневых атак сделал их популярными в феодальной Японии, поэтому во многих замках начали применять контрмеры. Это были противопожарные укрепления с *дозо-дзукури* (огнеупорная штукатурка), огнеупорный лак [27], здания из огнеупорных материалов, таких как как глина или камень, использование огнеупорной черепицы, организация групп пожарной охраны и создание противопожарных заграждений в виде поддельных зданий, то есть зданий, которыми можно пожертвовать, чтобы предотвратить распространение огня на критически важные объекты инфраструктуры [6]. Охранников предупреждали о том, что пожары могут быть лишь средством отвлечения внимания для выполнения кражи, нападения или других действий [5] (этот совет позже появился в руководстве «Гумпо дзиёсю» [6]).

Важно помнить, что у синоби не было зажигалок, а защитники постоянно следили за поджигателями (как и современные компании, в системах у которых постоянно работают антивирусы). Синоби разработали хитроумные методы, позволяющие скрытно развести огонь, использовать его в качестве оружия и поджечь горючие цели. Организация кибератак во многом перекликается с изобретательностью синоби, которую они проявляли при поджогах.

В этой главе мы увидим, насколько огненные атаки синоби похожи на современные тактики кибервойны. Огонь очень похож на кибератаки вирусами-червями, поскольку они распространяются на все, к чему могут прикоснуться. Мы рассмотрим примеры разрушительных кибератак, а также то, как современные злоумышленники их выполняют. Поговорим о различных средствах защиты, которые используются для предотвращения, смягчения, сдерживания кибератак и восстановления после них. Выводы из этой главы могут быть применены к брандмауэрам, а также к новым, более продвинутым стратегиям защиты сети.

Деструктивные кибератаки

Как только компьютеры научились соединяться и общаться друг с другом, тут же появились самораспространяющиеся вирусы и черви. Деструктивные атаки со временем начали происходить все чаще. Атака на сеть одной организации может распространяться быстро, словно пожар, уничтожая системы и данные в интернете. Учитывая растущее число связей между системами в киберпространстве, а также пробелы в их безопасности, любая сеть или машина, подключенная к интернету и не имеющая надлежащих средств защиты, фактически просто стоит и ждет, когда ее подожгут.

В начале 2000-х годов произошли первые атаки программ-вымогателей. В этих атаках вредоносное ПО шифровало данные системы или сети, удаляя резервные копии, и не расшифровывало их до тех пор, пока цель не заплатит выкуп. Такие вирусы быстро распространяются из систем в сетевые и облачные хранилища, захватывают данные и вовсе уничтожают их с помощью шифрования, если жертва отказывалась заплатить. Подобно поджогам, программы-вымогатели часто используются для отвлечения внимания от более серьезных вещей. Например, однажды злоумышленники (предположительно из Северной Кореи) организовали атаку программы-вымогателя FEIB Hermes, чтобы отвлечь внимание киберзащитников от проводимой одновременно финансовой атаки на SWIFT, и заработали на этом миллионы долларов [30].

Затем начались атаки с удалением, когда злоумышленник внедряет в несколько систем «бомбу замедленного действия», которая в какой-то момент удаляет системные данные и резервные копии. В качестве примера можно привести вирус Shamoon, который, как полагают, был применен иранскими злоумышленниками против Саудовской Аравии и запущен в начале выходных с целью уничтожить данные и вывести из строя промышленные нефтяные системы [43].

В последнее время злоумышленники начали применять вредоносные программы саботажа против промышленных систем управления, научившись считывать показания датчиков или управлять техникой, переключателями, клапанами и приводами, которые управляют доменными печами [25], электрическими сетями [4], системами противовоздушной обороны [34] и ядерными центрифугами [26]. Такая атака способна вывести критически важные системы из строя или вызвать сбои в их работе, привести к взрывам или другим разрушениям.

Защитники с целью предотвращения распространения атак могут стараться уменьшить плоскость атаки за счет усиления защиты систем, чтобы настроенные меры безопасности могли свести потенциальный ущерб к нулю. Также полезно реализовывать отказоустойчивость, создавая несколько резервных копий систем и данных в других местах, чтобы компании было куда отступить, если кибератака уничтожит

основные системы (иногда такие резервные копии реализуются аналоговыми или ручными системами).

Есть и другие технические решения, такие как размещение по периметру сети брандмауэров. Если же злоумышленник обходит их, проникает в сеть и начинает самораспространяющуюся атаку, брандмауэр не помешает ей выйти за пределы сети. Дело в том, что брандмауэры обычно используются для блокирования входящих, а не исходящих атак. Кроме того, обнаружить и остановить деструктивную атаку могут антивирусное программное обеспечение, системы предотвращения вторжений (intrusion prevention systems, IPS), системы обнаружения вторжений на хост (host intrusion detection systems, HIDS) и объекты групповой политики (Group Policy Object, GPO). Такие технические средства защиты могут немедленно идентифицировать разрушительную атаку, отреагировать на нее и нейтрализовать ее, но они, как правило, работают по сигнатурам, поэтому не всегда эффективны.

Существует и более новый подход — киберстрахование, которое представляет собой соглашение, защищающее организацию от юридических и финансовых последствий атаки. Страховой полис позволяет смягчить ущерб организации в случае кибератаки, но от самой атаки не защищает, так же как страхование от пожара не защищает от огня.

Возможно, лучшим вариантом защиты от разрушительных атак было бы строгое разделение и изоляция сети (воздушный зазор), что позволяет ограничить доступ к ресурсам и остановить распространение вируса. Это весьма эффективный способ защиты от кибератак, но он не всегда возможен, так как способен существенно повлиять на работу бизнеса. Кроме того, его можно обойти с помощью инсайдера.

Защита от киберпожаров

Для компаний обычным делом является страхование от пожаров и одновременная реализация стратегий их предотвращения и локализации. Однако по какой-то причине некоторые компании покупают киберстраховку, но не принимают мер защиты от кибератак. Возможно, они не видят в кибератаках такой опасности, как от настоящего пожара, при котором на карту поставлено имущество и даже человеческие жизни. Но с развитием технологий интернета вещей (IoT) тесное сближение физического мира с киберпространством будет способствовать росту рисков. Принятие описанных далее защитных мер может быть чрезвычайно полезно для вашей компании.

1. **Проведите киберпожарные учения.** Сымитируйте разрушительные атаки для проверки системы резервного копирования, отработки отказа, скорости реагирования, восстановления и способности своевременно «эвакуировать»

данные. Подобное упражнение отличается от тестов аварийного восстановления или резервного копирования тем, что вместо воображаемой угрозы с сетью взаимодействует реальная модельная угроза (нужно также принять такие меры, как шифрование данных с помощью известного ключа, чтобы во время упражнений случайно не уничтожить важные данные).

Netflix использует упражнение под названием Chaos Monkey: специальная программа случайным образом отключает серверы, портит конфигурации и отключает службы. Таким образом организация постоянно проверяет возможность плавной и немедленной балансировки нагрузки или переключения на резервные копии. В случае реальной проблемы команда безопасности будет иметь на руках протестированные и работоспособные решения. Netflix предоставляет программу Chaos Monkey бесплатно, поэтому любая компания может использовать ее и с ее помощью научиться обнаруживать атаки, противодействовать им, реагировать на опасность и восстанавливаться после сбоев[1].

2. **Внедрите системы киберпожаротушения.** Выделите ресурсы на изучение того, как распространяется та или иная атака, что именно она разрушает и что делает ваши системы уязвимыми для нее. Внедрите адаптеры жестких дисков, разрешающие только чтение и выполняющие операции в буфере жесткого диска. Такие жесткие диски держат данные заблокированными и не позволяют уничтожить их, так как никакое ПО не может с ними взаимодействовать. Удалите «горючее» программное обеспечение: приложения, библиотеки, функции и другие компоненты, которые могут распространять атаки. На рынке может появиться специализированное программное обеспечение, оборудование и устройства, обеспечивающие киберогнеупорность. Эти приложения могут иметь большое влияние на рынок: они делают серверы или данные устойчивыми к разрушительным атакам или по крайней мере замедляют или останавливают их распространение.
3. **Установите киберпожарные ловушки.** Существуют богатые возможности для создания автоматизированных киберловушек, которые заманивают злоумышленников или вредоносные программы в бесконечные циклы или запускают механизмы, которые заставляют атаку изолироваться и погасить саму себя. Один из таких способов защиты — создание папок в общих сетевых ресурсах с бесконечными рекурсивными каталогами. Когда вредоносная программа пытается перебирать такие папки, она застревает в бесконечном цикле [3]. Для обнаружения такого поведения можно использовать специальные датчики, способные предупредить отдел безопасности или самостоятельно убить процесс, который инициировал бесконечный каталог.

[1] Для получения дополнительной информации см.: Chaos Monkey, GitHub, Inc., Lorin Hochstein, last modified July 31, 2017 // https://bit.ly/3noAJhL.

4. **Создавайте динамические кибербарьеры.** Распространение кибератак упрощается из-за того, что системы обычно бывают включены и соединены друг с другом. Хотя атака не может напрямую скомпрометировать данную систему, она может распространиться на связанные с ней системы. Это неоднократно демонстрировалось сотнями тысяч, если не миллионами ботнетов, червей и других самораспространяющихся вредоносных программ.

   В большинстве случаев разделение и изоляция реализуются за счет статически разработанной архитектуры. Но ИТ-организации могут внедрять также дополнительные ручные и программные барьеры. Известно, что у некоторых компаний в здании есть главный рубильник, с помощью которого вручную отключают организацию от внешней сети. Связь внутри сети продолжает работать, но все внешние сетевые соединения немедленно разрываются, создавая физический воздушный зазор. Польза этой возможности может показаться сомнительной, но в случае глобального киберпожара у компании есть возможность быстро и легко изолироваться от угрозы без необходимости рубить кабели топором.

   В более совершенной версии этой реализации каждая система, комната, этаж и здание будут иметь собственный переключатель, что позволит сотрудникам службы безопасности принимать быстрые решения и предотвращать разрушительные атаки. Узнав об атаке, сотрудники могут быстро скопировать себе любые критически важные рабочие документы, а затем отключить свой компьютер от сети и предотвратить распространение атаки.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Вы тратите значительные средства на его противопожарную защиту. Замок построен из камня, укреплен с помощью новейших технологий защиты от огня, а охранники обучены реагировать на пожар.

Подумайте, как еще может произойти пожар? Например, можно ли защитить или переместить свои пороховые склады? Можно ли изолировать их, не лишив военных советников свободного доступа к пороху? Как бы вы защитили продовольственные склады от огня, не испортив продукты? Как отсматривать или сортировать товары, движущиеся через ваш замок, чтобы предотвратить перемещение горючих материалов? Где в лагерях, казармах или других районах замка можно установить огневые барьеры? Какие пожарные ловушки могут помочь вам сдержать или погасить распространяющийся огонь либо поймать поджигателя? Можете ли вы для обучения своих солдат разработать упражнение по пожарной подготовке с использованием настоящего огня, но без риска для замка?

Рекомендуемые меры безопасности и предосторожности

Рекомендации следует оценивать с учетом концепции пожарных атак.

1. Мониторьте индикаторы деструктивных действий в своей организации. Предотвратите взлом журналов системного мониторинга, событий аудита и данных с датчиков путем пересылки данных в сегментированные сборщики событий. (AU-6. Аудиторский обзор, анализ и отчетность | (7) Разрешенные действия; AU-9. Защита аудиторской информации; SI-4. Системный мониторинг.)
2. Реализуйте разделение и изоляцию сетей и систем, чтобы уменьшить скорость распространения атак. (CA-3. Системные соединения; SC-3. Изоляция функций безопасности; SC-7. Граничная защита | (21) Изоляция компонентов системы; SC-11. Надежный путь | (1) Логическая изоляция; SC-39. Изоляция процесса.)
3. Выполняйте тесты резервного копирования и упражнения на отказоустойчивость, чтобы определить, работают ли механизмы восстановления так, как задумано. (CP-9. Резервное копирование системы | (1) Тестирование на надежность и целостность | (2) Восстановление по семплам; CP-10. Восстановление системы | (1) Тестирование плана действий в чрезвычайных обстоятельствах.)
4. Требуйте от уполномоченных лиц двойной авторизации, прежде чем разрешать им выполнять команды удаления данных. (CP-9. Резервное копирование системы | (7) Двойная авторизация.)
5. Реализуйте меры по поддержанию безопасности вашей организации в случае атаки, нацеленной на системы безопасности. Например, настройте брандмауэры, которые переходят в автономный режим и блокируют все системы, или настройте систему на переход в безопасный режим в случае атаки. (CP-12. Безопасный режим; SC-24. Отказ в известном состоянии.)
6. Внедрите механизмы передачи носителей с учетом защиты от атак. Проверьте, что диски с конфиденциальными данными отключены от сети, хранятся в безопасном месте и защищены от физических атак вроде пожара. (MP-5. Транспортировка носителей; PE-18. Расположение компонентов системы; SC-28. Защита неиспользуемой информации.)
7. Перед подключением портативных носителей или устройств к системам или сетям вашей организации тестируйте и сканируйте их на предмет наличия вредоносного ПО. (MP-6. Обработка носителей; SC-41. Доступ к портам и устройствам ввода/вывода.)
8. Оцените риски и определите, какие данные и системы в случае компрометации нанесут наибольший вред вашей организации. Примите меры

предосторожности и установите специальные меры безопасности для таких систем и данных. (RA-3. Оценка риска; SA-20. Особая разработка критических компонентов.)

9. Создайте средства защиты, например защиту от вредоносного кода, чтобы снизить потенциал атак. (SC-44. Детонационные камеры; SI-3. Защита от вредоносного кода.)

Резюме

В этой главе мы поговорили о пожарах, устраиваемых синоби, и о том, как они применяли огонь в качестве оружия. Упомянули несколько громких кибератак и способов защиты от них. А также узнали, чем киберугрозы похожи на пожары.

В следующей главе мы подробно обсудим, как синоби взаимодействуют и координируют свои действия перед выполнением поджога. Синоби реализовывали тайную связь множеством хитрых способов, похожих на методы, используемые вредоносными программами.

18

Тайная связь

Если синоби, проникнув в стан врага, хочет связаться с генералом, он должен сообщить своим союзникам, где находится. Для этого необходимо выбрать время и место.

Чтобы добиться успеха в ночной атаке, отправьте синоби заранее,
чтобы тот побольше разузнал о позиции врага,
и лишь после этого отдавайте приказы.
«Ёсимори хяку-сю», № 12

Поскольку синоби были в первую очередь экспертами по шпионажу, они должны были безопасно передавать секретные сообщения с разведданными, планами атак и другой важной информацией, чтобы помочь своему правителю и союзникам принимать более удачные тактические и стратегические решения. Правители, генералы и другие синоби, в свою очередь, должны были тайно передавать внедрившимся агентам информацию о том, когда следует выполнить поджог или иное действие. Такие сообщения должны быть удобны для расшифровки самим синоби-получателем, но недоступны для всех остальных.

В «Бансэнсюкай», «Нимпидэн» и «Гумпо дзиёсю» описываются секретные методы, которые синоби использовали для общения с другими синоби, силами союзников или нанимателем после проникновения на вражескую территорию. Некоторые из них очень просты. «Бансэнсюкай» описывает методики сокрытия сообщения в животе рыбы или даже внутри человека (додумайте сами как), который может свободно приходить на территорию или покидать ее, не вызывая подозрений. Обычно для этого задействовали монахов и нищих. В этом же трактате описаны методы запутывания, например разрезание сообщения на несколько частей и их

отправка с разными посыльными, а также изготовление чернил из мандаринового сока, ржавой воды, саке или касторового масла, которые после высыхания на бумаге становятся невидимыми, но проявляются огнем. Синоби даже придумали *синоби ироха* (нестандартный алфавит, который способны расшифровать только они сами), а также использование разбитых на части слов или символов для создания контекстной двусмысленности, понять которую может только синоби-получатель [5].

Еще один простой и популярный метод отправки секретных сообщений назывался *ябуми*: на бамбуковое древко стрелы наматывали секретный свиток, а на ее оперение ставили специальные отметки, позволяющие идентифицировать получателя. Из-за логистических сложностей феодальной Японии синоби не всегда удавалось выпустить ябуми в заранее оговоренное время и место, поэтому они разработали стрелковое «рукопожатие», которое для постороннего глаза казалось просто перестрелкой. Если одна сторона видела определенное количество быстро выпущенных в одно и то же место стрел, она открывала ответный огонь, также выпуская определенное количество стрел в ответ. Этот сигнал и ответный сигнал позволял понять, что союзник на связи. Тогда синоби мог выпустить *ябуми*, которую получатель должен был подобрать [5]. Этот метод связи стал настолько распространен, что в «Гумпо дзиёсю» предупреждали: враг может посылать со стрелами фальшивые письма. Таким образом, получатель должен внимательно изучать *ябуми* с помощью специальных лингвистических приемов [6].

Для передачи сигналов на дальние расстояния или других случаев, когда свиток передать не удавалось, синоби разработали систему передачи сигналов с помощью флагов, огня, дыма и фонарей (*хикьякуби*). Когда и это было невозможно, они использовали секретные барабаны, гонги и раковины. Громкий и хорошо различимый уникальный звук сигнального устройства говорил синоби в тылу врага, что следует подготовиться к получению сообщения. Точный образец сигнала согласовывался за пару дней до проникновения, чтобы избежать путаницы. После предупреждающего *хикьякуби* с помощью сигналов барабана, гонга или раковины [5] отправлялось само сообщение.

В этой главе мы рассмотрим, чем методы тайного общения синоби очень похожи на современное вредоносное ПО для перехвата управления. Обсудим, зачем нужны средства связи для управления и какова их роль в совершении атак. Мы коснемся различных методов, которые современные злоумышленники используют для тайной связи. А также обсудим различные способы защиты от этой техники и проблемы ее применения. Наконец, мы рассмотрим множество передовых методов обеспечения безопасности для защиты от управляющей связи. Поскольку

в трактатах синоби нет никаких указаний о том, как прекратить тайное общение, предполагается, что сделать это не так-то просто.

Управляющая связь

Обычно вредоносные программы не могут быть полностью независимыми и автономными. Если бы это было так, вредоносное ПО было бы тяжеловесным, сложным, подозрительным и видимым для защитников. Большинству вредоносных программ во время работы требуется возможность получать указания, поэтому злоумышленники используют метод, называемый *«командование и управление»* (command and control, сокращенно C2, CnC или C&C), с помощью которого связываются с вредоносными программами, бэкдорами, имплантатами и скомпрометированными системами в атакованной сети. Операторы применяют связь C2 для передачи команд скомпрометированной системе, указывая ей загрузить данные, обновить конфигурацию или даже самоудалиться. Также имплантат C2 может инициировать обмен данными, отсылать статистику или ценные файлы, запрашивать новые команды или отправлять сигнал о том, что система находится в сети, а также ее местоположение и текущий статус. Субъекты киберугроз часто подготавливают инфраструктуру C2, включая доменные имена, IP-адреса и веб-сайты, за пару недель до проникновения.

Функциональность C2 широко известна, и многие брандмауэры, IDS/IPS и другие устройства безопасности и средства управления не дают злоумышленникам напрямую связываться с целевыми системами и получать информацию от них. Чтобы обойти эти меры защиты, злоумышленники постоянно разрабатывают более совершенные методы, тактики и процедуры C2. Например, данные C2 можно встраивать в полезную нагрузку команды `ping` или в команды, скрытые в изображениях, размещенных на общедоступных сайтах. Злоумышленники использовали C2 в лентах Twitter и комментариях на сайтах. Также C2 применяли для установки прокси-серверов и ретрансляторов электронной почты в скомпрометированных системах. После установки выполняется обмен данными через известные протоколы и безопасные сайты, которые не блокируются средствами безопасности и устройствами. Телефоны, подключенные к скомпрометированным системам, могут заражаться вредоносным ПО, которое при USB-соединении вызывает C2 через вышки сотовой связи, минуя брандмауэры и другие средства защиты сети и способствуя общению между злоумышленником и C2 во время зарядки аккумулятора телефона. В некоторых методах связи C2 задействуются мигающие светодиоды (словно сигнальный огонь), варьируется температура процессора (дымовой сигнал), используются звуки жестких дисков или динамиков ПК (звуковые барабаны) и волны электромагнитного спектра для преодоления воздушного зазора.

Злоумышленники реализуют C2 с помощью шифрования и других методов обеспечения конфиденциальности, чтобы поддерживать связь со скомпрометированной системой, не раскрывая своего присутствия. Они могут избежать обнаружения следующими способами.

- Ограничением ежедневно передаваемого объема данных, чтобы изменения трафика оставались незамеченными (например, не более 100 Мбайт в день, чтобы замаскировать загрузку 1,5 Тбайт в течение двух недель).
- Отправкой или получением маяков только во время работы активного пользователя, чтобы замаскировать трафик (поэтому лучше не отправлять маяки в нерабочее время).
- Переключением на новые, случайные или динамически изменяемые точки C2, чтобы избежать статистических аномалий.
- Регулярным созданием «нормального» трафика, чтобы избежать проверок и анализа поведения.
- Отключением или удалением журналов активности, чтобы скрыть свое присутствие от экспертов.

Более сложные тактики C2 могут быть особенно ужасными, практически необнаруживаемыми и неблокируемыми. Пусть у нас есть ИТ-администратор, работающий на Windows, который внедрил строгие средства управления брандмауэром, разрешая системе заходить только на сайт technet.microsoft.com — официальный веб-портал Microsoft для ИТ-специалистов. Разрешен только протокол HTTPS, антивирус обновлен и работает, а операционная система полностью пропатчена. Никакие внешние программы, такие как электронная почта, Skype или iTunes, не работают, за исключением сайта Microsoft TechNet, который необходим администратору для выполнения своей работы.

Ситуация кажется безопасной, но теперь представим, что китайский пользователь APT17 закодировал в комментариях на Microsoft TechNet скрытые IP-адреса, которые взаимодействовали с трояном удаленного доступа BLACKCOFFEE в скомпрометированной системе [10]. Если бы вы проверили прокси-трафик, анализ поведения, эвристику аномалий, сигнатуры IDS, антивирус или предупреждения брандмауэра, никаких признаков злонамеренной связи не нашли бы.

В рамках усиления защиты для противодействия сложным C2 обычно создаются воздушные зазоры между системами, но в последние годы появились новые методы связи C2. Одним из примеров является использование USB-накопителя с руткитами или скомпрометированной прошивкой и вредоносными программами, которые после подключения к системе инициируют обмен данными с имплантатом

в скомпрометированной системе, собирают упакованные данные и незаметно загружают их для фильтрации на внешний компьютер.

Управление командами

Организации часто подписываются на рассылку нескольких индикаторов угроз. По этим рассылкам компания регулярно получает вредоносные URL-адреса, IP-адреса и домены, замеченные в работе в качестве C2. Получив информацию, организация начнет предупреждать и/или блокировать эти угрозы в своих брандмауэрах и устройствах безопасности. Это хорошая отправная точка для создания защиты от C2, но в мире появляется бесконечное количество новых URL-адресов, IP-адресов и доменов, позволяющих злоумышленникам использовать новые идентификаторы и обходить защиту. Для решения проблем C2 необходим как старый, так и новый подход, некоторые из них предлагаются далее.

1. **Реализуйте лучшие практики.** Предотвратить все коммуникации C2 может быть непрактично или даже невозможно, но вы можете заблокировать базовые или умеренно продвинутые C2, внедрив передовые методы кибербезопасности: хорошее знание своей сети, установленные границы, контроль за потоком данных, белые списки, разрешение на превентивную блокировку связи C2 службой безопасности. Не пренебрегайте передовым опытом, а займитесь серьезной работой по обеспечению безопасности. Документируйте, тестируйте и проверяйте свои лучшие практики, а также консультируйтесь с независимыми сторонними экспертами по поводу внедрения дополнительных мер проверок. Инвестируйте в повышение безопасности, поддерживая и улучшая существующую передовую инфраструктуру.
2. **Реализуйте сегментацию с помощью элементов «удаленного просмотра».** Под сегментацией и изоляцией сети понимается создание нескольких сетей и машин, таких как машина интрасети и неклассифицированная машина интернета, отделенные друг от друга. Сегментация должна препятствовать передаче связи C2 через эти разделительные границы. К сожалению, пользователи часто «на пару минут» подключают интранет-машину к интернету, чтобы загрузить документы или библиотеки, нарушая тем самым протоколы безопасности. Один из подходов к решению таких проблем — настроить компьютер интрасети так, чтобы он удаленно просматривал другой изолированный компьютер, подключенный к интернету. Изолированный интернет-бокс физически недоступен пользователям, они могут лишь отдавать команды и смотреть на экран, но фактическую информацию с этого компьютера не видят и не получают. Блок удаленного

просмотра — это фактически ТВ-монитор, на котором отображается другой компьютер в другой комнате. Таким образом, связь C2, вредоносные программы и эксплойты не могут дойти до вас через видеосигнал и причинить вред.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Каждую неделю ваши писцы создают новые свитки, в которые записывают государственные секреты, новые исследования и открытия, финансовые данные и другую конфиденциальную информацию. Эти документы ни в коем случае не должны попасть в руки врага. Однако ходят слухи, что кто-то делает копии важных свитков, хранящихся в вашей библиотеке, и недавние действия врагов, похоже, подтверждают эти подозрения. При этом писцы и архивариусы вне подозрений и об инсайдерской угрозе речи не идет.

Какие ограничения доступа или физическую защиту можно было бы установить, чтобы предотвратить кражу или воспроизведение свитков? Как можно отследить их кражу или уничтожение, не останавливая свободный проход товаров и людей в ваш замок и из него? Нельзя ли хранить свитки таким образом, чтобы противник не знал, какие из них важные, а какие нет? Какими еще способами злоумышленник может получить доступ к свиткам или украсть информацию и как от этого защититься?

Рекомендуемые меры безопасности и предосторожности

1. Внедрите на уровне систем, границ сети и точек выхода из нее меры безопасности, позволяющие находить признаки кражи данных. Это может быть блокировка зашифрованных туннелей, которые ваши датчики не могут перехватить, а также поиск доказательств применения несанкционированных протоколов, форматов данных, водяных знаков, меток данных и больших файлов или потоков, покидающих сеть. (AC-4. Сопровождение информационного потока | (4) Проверка содержимого зашифрованной информации; SC-7. Граничная защита | (10) Предотвращение эксфильтрации; СИ-4. Системный мониторинг | (10) Видимость зашифрованных сообщений.)
2. Создайте несколько сетей с изоляцией и сегментацией интернет-ресурсов и ресурсов интрасети. Не подключайте критически важные внутренние системы к интернету. (AC-4. Сопровождение информационных

потоков | (21) Физическое и логическое разделение информационных потоков; CA-3. Системные соединения | (1) Несекретные соединения системы национальной безопасности | (2) Секретные соединения системы национальной безопасности | (5) Ограничения на внешние системные подключения; SC-7. Граничная защита | (1) Физически разделенные подсети | (11) Ограничение входящего коммуникационного трафика | (22) Отдельные подсети для подключения к разным доменам безопасности.)

3. Ограничьте удаленный доступ к любым системам, хранящим важную информацию. (AC-17. Удаленный доступ.)
4. Реализуйте ограничения и средства управления конфигурацией для обнаружения и предотвращения несанкционированной беспроводной связи. (AC-18. Беспроводной доступ | (2) Мониторинг несанкционированных подключений; PE-19. Утечка информации; SC-31. Анализ скрытых каналов; SC-40. Защита беспроводной связи; SI-4. Системный мониторинг | (15) Сочетание проводной и беспроводной связи.)
5. Обучите свою команду безопасности и сотрудников распознавать коммуникации C2. (AT-3. Обучение на основе ролей | (4) Подозрительные сообщения и аномальное поведение системы; SI-4. Системный мониторинг | (11) Анализ аномалий коммуникационного трафика | (13) Анализ шаблонов трафика и событий | (18) Анализ трафика и скрытая эксфильтрация.)
6. Запрещайте применять любое неавторизованное программное обеспечение, которое может быть средством C2 или имплантатом. (CM-7. Наименьшая функциональность | (5) Разрешенное программное обеспечение — белый список.)
7. Защитите прямые физические подключения к системам, которые обходят меры безопасности и границы. Это могут быть шкафы с переключателями, настенные розетки Ethernet и компьютерные интерфейсы. (PE-6. Мониторинг физического доступа; SC-7. Граничная защита | (14) Защита от несанкционированных физических подключений | (19) Блокировка связи с посторонними хостами.)
8. Требуйте проверять и сканировать съемные носители, которые попадают в вашу организацию или покидают ее, чтобы персонал не мог вручную переносить данные для коммуникации с C2 через внешние носители. (PE-16. Доставка и удаление.)
9. Реализуйте белый список для запрета связи с любым ресурсом или адресом, не находящимся в этом списке. Многие C2-сайты — это недавно созданные домены без истории использования вашей организацией. (SC-7. Граничная защита | (5) Запрет по умолчанию, разрешение по исключению.)

Резюме

В этой главе мы рассмотрели различные методы связи синоби, используемые для получения команд от союзников и отправки их обратно. Описали различные современные методы C2, а также сравнили их с методами синоби.

В этой главе мы лишь прошлись по верхам, так как весьма вероятно, что о самых сложных методах C2 нам еще предстоит узнать. Как лучшие методы скрытого общения синоби нигде не описываются, так и мы, возможно, никогда не узнаем о гениальности самых передовых методов C2. Мы обсудили несколько передовых практик, в том числе использование белого списка и проверку шифрования, которые позволяют смягчить последствия атак C2, однако идеальное решение проблемы еще предстоит найти.

В следующей главе мы поговорим о специальных знаках или позывных синоби. У них были свои методы общения с союзниками на вражеской территории, основанные на уникальных метках или сообщениях. Такие позывные никогда не выходят за границы окружающей среды, поэтому традиционные методы блокировки или обнаружения связи C2 против них обычно не работают.

19

Позывные

Проникнув внутрь, вы должны первым делом пометить маршрут и показать союзникам, где можно войти и выйти.

Успешно проникнув в стан врага, главное не начать
по ошибке сражаться друг с другом, а не с врагом.
«Ёсимори хяку-сю», № 26

В культурной среде синоби часто изображаются как воины-одиночки, но на самом деле многие из них работали в командах. Члены этих команд были особенно искусны в тайной передаче информации друг другу в полевых условиях. «Гумпо дзиёсю» описывает три знака, или физических маркера, с помощью которых синоби могли общаться друг с другом, не вызывая подозрений. В зависимости от того, какой именно маркер использовался и где он был размещен, он мог помочь синоби идентифицировать цель, выбрать нужную развилку на дороге, найти лагерь врага или начать атаку. Позывные были хорошо известны в кругах синоби, поэтому те всегда согласовывали перед миссией точный и уникальный набор знаков, чтобы гарантировать, что цели или даже вражеские синоби не смогут распознать их. Трактаты предполагают использование переносных одноразовых маркеров, которые можно быстро разместить на земле или убрать. Маркеры должны быть визуально уникальны и различимы, но непримечательны для непосвященных.

Например, синоби мог указать на свое местонахождение, оставив в заранее определенном безобидном месте окрашенные зерна риса. Один синоби оставлял красный рис, другой зеленый и т. д. Другой синоби, увидев несколько цветных зерен, мог понять, кто из союзников тут уже был. Прелесть системы заключалась в том, что синоби могли быстро найти нужные предметы, а вот обычные прохожие не заметили бы несколько странно окрашенных зерен риса. Аналогичным образом синоби могли незаметно положить на землю кусок сломанного бамбука, чтобы направить союзника к нужной тропинке, или бросить на землю небольшой листок бумаги, чтобы

указать на дом, которой будет сожжен, чтобы члены команды не стали жертвами или подозреваемыми в поджоге [6].

В этой главе мы рассмотрим способы применения позывных в сетевых средах и расскажем, для чего киберпреступники могут их использовать. Подумаем о том, где в сети могут быть размещены сигналы и как они могут выглядеть. Кроме того, мы обсудим, как можно охотиться за ними в целевой сети. Рассмотрим задачу обнаружения сложных позывных и в целом задачу контроля и мониторинга вашей среды на предмет действий злоумышленника. Мысленно вы сможете построить ментальные модели и выработать решения для борьбы с позывными врага. В конце рассмотрим меры безопасности, которые могут помешать злоумышленникам использовать позывные в вашей среде, а также ограничить их возможности.

Работа оператора

Во время взлома Национального комитета Демократической партии (Democratic National Committee) в 2016 году российские ГРУ (также известное как APT28, или FANCYBEAR) и ФСБ (APT29, или COZYBEAR) работали в одной сети и системах, не используя позывные для общения друг с другом. Из-за этого деятельность потребовала вдвое больших усилий и привела к возникновению наблюдаемых аномалий и других признаков взлома в атакуемой сети, что, вероятно, способствовало провалу обеих операций [21]. Отсутствие коммуникации, которое, видимо, было вызвано недружественными отношениями этих организаций, дает повод для размышлений о том, какой опыт стоило бы перенять у синоби.

Сообщество кибербезопасности еще не встречало случаев, когда несколько нападавших обменивались скрытыми маркерами, но взлом DNC демонстрирует необходимость существования такого протокола. Разумно предположить, что ГРУ и ФСБ подготовили отчет о последствиях своих попыток взлома DNC и, возможно, уже решили внедрить протокол позывных для будущих операций, чтобы не повторить допущенных ошибок. Если организации, занимающиеся кибершпионажем, начнут регулярно работать в изолированных, но пересекающихся группах, им потребуется способ передачи различной информации о своем присутствии в системе и о своих целях, особенно если использование обычных каналов связи невозможно.

Если бы подобные позывные действительно существовали, как бы они выглядели? Эффективные киберпозывные, скорее всего:

- регулярно менялись бы, как маркеры синоби;
- реализовались бы в инструментах и вредоносных программах, которые невозможно перехватить и реконструировать. Для их идентификации были бы необходимы люди, использующие клавиатуру;

- располагались бы там, где вторая шпионская группа их точно найдет, например на первичном контроллере домена (domain controller, DC). Из-за наличия мониторов безопасности файлов и особенностей работы, из-за которых контроллеры домена перезагружаются не очень часто, группа атакующих может поместить маркер в память контроллера домена, чтобы максимально увеличить его надежность и обнаруживаемость.

Пока неясно, какие именно строки или уникальные байты могут выполнять роль маркеров, в каком кэше, вре́менной таблице или ячейке памяти они могут находиться и как дать другому оператору возможность их легко обнаружить. Но обратите внимание на то, что индустрия кибербезопасности исследовала несколько семейств вредоносных программ, которые оставляют определенные файлы или ключи реестра в качестве сигнала о том, что заражение успешно распространилось на данную машину и, таким образом, не нужно пытаться заразить ее снова [14]. Защитники могут создавать файлы и ключи реестра, которые ложно сигнализируют о заражении, что побуждает вредоносное ПО уйти восвояси. Хотя против злоумышленника-человека это вряд ли поможет.

Определение наличия позывных

Многим организациям бывает сложно даже определить, кто из пользователей удалил файл с общего сетевого диска, не говоря уже об обнаружении скрытых позывных, спрятанных внутри удаленных частей системы. Но это не отменяет того, что защитникам придется столкнуться с угрозами, которые сообщаются друг с другом прямо внутри атакованной среды. Чтобы поймать злоумышленников, защитникам потребуется освоить новые навыки, необходимо будет также внедрить инструменты обнаружения и обеспечить видимость хоста.

1. **Реализуйте расширенный мониторинг памяти.** Определите в своей сети важные системы, которые, по вашему мнению, злоумышленник выберет в качестве основной или промежуточной цели. Затем изучите возможности организации по отслеживанию и ограничению изменений памяти в этих системах. Рассмотрите имеющиеся на рынке продукты и услуги. Оцените усилия и время, которые потребуются для исследования источника изменений памяти. Наконец, определите, можете ли вы с уверенностью определить, что те или иные изменения являются признаком атаки.
2. **Обучите сотрудников.** Научите службу безопасности, охотников на угрозы и ИТ-отдел не игнорировать непонятные ситуации, а рассматривать необычные объекты в памяти как потенциальные индикаторы атаки, особенно на важных объектах вашей инфраструктуры.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Вы получили достоверную информацию о том, что вас собираются атаковать несколько команд синоби, которые для связи друг с другом используют определенные позывные. Сигналы представляют собой разложенные на земле незаметные маркеры, в том числе окрашенный рис, муку и кусочки бамбука.

Как бы вы научили своих охранников определять эти и другие подобные, но еще неизвестные техники? Как помочь им не делать стойку на каждый ложный сигнал, который может возникнуть, если кто-то случайно уронит на землю рисовое зерно или ветер принесет клочок бумаги? Какие архитектурные изменения вы можете внести в свой замок и территорию, чтобы обнаруживать секретные маркеры стало легче? Какие контрмеры могут разрушить, нарушить или ухудшить способность этих маркеров передавать информацию и как можно ввести в заблуждение синоби, отправляющих и принимающих сигналы?

Рекомендуемые меры безопасности и предосторожности

Рекомендации следует оценивать с учетом концепции позывных сигналов.

1. Убедитесь, что пользователям, которые в данный момент работают с некоторой системой или ресурсом, недоступна информация о предыдущем пользователе. (SC-4. Информация в общих ресурсах.)
2. Определите системные коммуникации, которые могут задействоваться для несанкционированной передачи информации. Хороший пример потенциального скрытого канала — это элемент управления «PE-8. Записи доступа посетителей». Бумажные журналы регистрации или цифровые устройства, которые посетители используют для входа на объекты, могут применяться для размещения информационных маркеров, сигнализирующих другим участникам шпионажа о том, что это место уже посещали другие. (SC-31. Анализ скрытых каналов.)
3. Ищите индикаторы потенциальных атак и несанкционированного использования системы и развертывайте устройства мониторинга для отслеживания необычных перемещений информации. (SI-4. Системный мониторинг.)
4. Защитите системную память от несанкционированных изменений. (SI-16. Защита памяти.)

Резюме

В этой главе мы рассмотрели физические маркеры, которые использовались командами синоби для связи на вражеской территории. Мы рассказали, чем они были полезны, и дали описание рекомендованных в трактатах позывных. Затем рассмотрели операцию, в которой отсутствие позывных и связанная с ним несогласованность действий способствовали обнаружению атакующих. Обсудили, как современные хакеры, вероятно, будут продолжать совершенствовать свое искусство, в том числе за счет применения позывных. Мы изучили, как могут выглядеть современные цифровые позывные и как их можно заметить.

В следующей главе обсудим противоположность позывных — меры предосторожности, принимаемые синоби, чтобы стереть следы своей активности на вражеской территории. Для этой цели даже использовались ложные сигналы, предназначенные для обмана защитников.

20

Тушите за собой свет и выключайте воду

Традиции древних синоби говорят, что сперва нужно запереть дверь и лишь затем включать фонарь.

Когда нужно совершить кражу во время снегопада,
ваш злейший враг — это ваши же следы.
«Ёсимори хяку-сю», № 53

Уход от нежелательного внимания являлся основой ремесла синоби, и они усердно тренировались, чтобы научиться действовать скрытно. Если фонарь синоби испускал свет, который тревожил животных, эхо шагов будило спящую цель, а кожура от фруктов указывала на чье-то присутствие, то синоби сам же ставил свою миссию (а может, и жизнь) под угрозу. В трактатах приведено обширное руководство по перемещению и тактическим действиям, в котором делается акцент на обращение со светом, звуками и мусором.

Световая дисциплина диктует несколько общих принципов. Например, в трактатах рекомендуется, чтобы, проникнув в дом, синоби запирал дверь изнутри, перед тем как зажигать фонарь, чтобы свет не был виден снаружи (и никто не зашел) [5]. Рассматриваются в них и специфические техники. «Бансэнсюкай» подробно описывает ряд умных инструментов для управления освещением, таких как огненное яйцо *ториноко*. Это пучок специального горючего материала с тлеющим углем в центре, по форме и размеру напоминающий яйцо. Оно лежит в ладони синоби таким образом, чтобы, разжимая или сжимая пальцы, контролировать количество кислорода, которое делает свет тлеющего угля ярче или тусклее, и направлять свет в нужную сторону. Синоби мог быстро разжать руку, чтобы увидеть, кто спит в комнате, а затем мгновенно погасить свет, сжав кулак [5]. По сути, огненное яйцо можно было включать и выключать так же, как современный фонарь.

Тишина для синоби была невероятно важна, и трактаты описывают множество техник, позволяющих при проникновении сохранять тишину. В «Нимпидэн» предлагалось прикусить полоску бумаги, чтобы заглушить звук дыхания. Некоторые синоби передвигались на небольшие расстояния, держась за подошвы ног ладонями рук и наступая на них, чтобы заглушить звук шагов. Эта техника наверняка требовала значительной практики и подготовки. Часто синоби носили с собой масло или другие вязкие вещества для смазывания скрипучих петель ворот или деревянных раздвижных дверей — всего, что может скрипеть и выдать присутствие чужого. Трактаты также предупреждают, что нельзя наносить эти жидкости слишком обильно, так как они могут привлечь внимание и указать на проникновение [6].

Не все методы шумовой дисциплины связаны с тишиной. Трактаты учат и специально создавать шум. «Сёнинки» описывает методику, называемую *куцукаэ*, или «смена обуви», которая на самом деле подразумевает изменение поступи, а не обуви. Проникающий синоби мог подделывать походку, хромать, топать, делать прерывистые шаги или издавать слышимые, но особые звуки шагов, чтобы обмануть слушающего. Затем, когда синоби возвращался к своей естественной походке, тот предполагал, что слышит другого человека, или думал, что человек внезапно остановился [7]. «Нимпидэн» советует стучать палкой, звать на помощь или имитировать тревогу, проверяя реакцию охранников на шум [6]. «Бансэнсюкай» описывает более тонкий шумовой тест, в котором синоби, находясь рядом с целью или охранником, начинал все более громко шептать, чтобы определить слуховой порог цели. Шумовые тесты помогают синоби понимать реакции цели:

- как быстро цель реагирует;
- возникают ли между охранниками споры по поводу шума;
- появляются ли охранники быстро и с оружием в руках;
- застал ли шум цель врасплох;
- отреагировала ли цель вообще.

Эти наблюдения не только говорят синоби о том, насколько внимательна цель и остер ее слух, но и позволяют понять уровень навыков и подготовленность цели к реагированию на события. Эту информацию синоби может использовать для будущего проникновения [5].

Что касается вещественных доказательств, синоби придерживались принципа «не мусорить» задолго до того, как это стало мейнстримом. Приспособление под названием *нагабукуро* («длинный мешок») использовалось как вещмешок. Когда синоби взбирался на высокую стену и ему нужно было проделать дыру, чтобы пролезть, он брал с собой большую толстую кожаную сумку с мехом или войлоком внутри, чтобы собирать камни и глушить звук их падения. Затем синоби мог тихо опустить

мешок в незаметное место на земле внизу. Это было гораздо лучше, чем позволить камням упасть на землю или в ров [5].

В этой главе мы вместо света, шума и мусора будем использовать их эквиваленты в сфере киберугроз. Рассмотрим некоторые инструменты и методы, с помощью которых хакеры старались скрыть свои следы, а также кое-какие хитрости. Мы обсудим тему обнаружения «низких и медленных» угроз, а также изменения вашей среды таким образом, чтобы она работала на вас. В упражнении будет рассмотрен метод, используемый синоби для маскировки шагов, который может быть применен и к современным цифровым системам. В конце главы мы рассмотрим дисциплину обнаружения как способ противодействия особо хитрому противнику, который помнит, какие следы он оставляет в сети, а какие нет.

Киберсвет, шум и мусор

Цифровой мир не всегда работает так же, как физический. Иногда бывает сложно распознавать и постоянно искать киберэквиваленты света, шума и мусора. Поскольку у защитников не хватает времени, ресурсов и возможностей для постоянного мониторинга и охоты в отслеживаемых системах, оставляемые противником свет, шум и/или следы часто не документируются. В результате злоумышленникам может быть легче осуществить киберпроникновение, чем физическое проникновение.

Многие инструменты и фреймворки для сканирования и эксплуатации, такие как Nmap [28], поддерживают «медленные» режимы, отслеживающие размеры пакетов или полезной нагрузки, частоту отправки пакетов и использование полосы пропускания в целевой сети. Злоумышленники разработали очень маленькие вредоносные файлы (например, China Chopper весит менее 4 Кбайт [35]), размер которых заставляет ошибочно думать, что маленький файл не причинит вреда. Вредоносное ПО может быть настроено так, чтобы минимизировать количество генерируемого шума, пореже отправлять сообщения управления и контроля (C2), сводить к минимуму шум в журналах процессов или памяти, целенаправленно переходить в спящий режим или подолгу бездействовать. Чтобы не оставлять цифрового мусора, который может выявить присутствие чужого, некоторые вредоносные программы не сбрасывают файлы на диск. Злоумышленники и вредоносные программы в соседней сетевой инфраструктуре могут использовать пассивный сбор информации, что сделает работу в целевой среде медленной, но плодотворной. Примечательно, что многие из этих угроз тоже иногда оставляют после себя свет, шум или мусор и осознанно идут на этот риск.

Разумно предположить, что у продвинутых хакеров есть процедуры для контроля оставляемого света, шума и мусора, такие как:

- использование не более 100 Мбайт трафика в день;
- маскировка вредоносных артефактов, файлов и строк, чтобы они не указывали на присутствие хакера или вредоносного ПО;
- отключение звука журналов, предупреждений, «растяжек» и других датчиков для обеспечения безопасности и секретности.

Можно подумать, что большинство современных устройств и систем безопасности должны срабатывать в ответ на точную сигнатуру известной угрозы, например конкретный IP-адрес, журнал событий или байтовый паттерн. Даже специализированному программному обеспечению вроде Wireshark [49], которое показывает аналитики активности угроз в режиме реального времени, требуются значительные усилия для сбора, обработки и изучения подобной информации. Этот процесс похож на то, как мы прислушиваемся к шагам. Поскольку люди не могут воспринимать цифровую сферу так же чутко, как физическую среду, меры безопасности в основном сводятся к тому, что мы усиливаем органы чувств программ и ждем, пока они что-то ощутят.

Дисциплина обнаружения

К сожалению, не существует идеального способа поймать кого-то, кто умеет не попадаться. У некоторых злоумышленников есть преимущество перед защитниками, так как они могут получить несанкционированный доступ к инструменту регистрации инцидентов группы безопасности и таким образом видеть, не исследует ли кто-то их злонамеренные деяния. Тем не менее защитникам есть что улучшить, чему научиться, какие меры внедрить и какие уловки применить, чтобы поймать того, кто им угрожает, на ошибке.

1. **Развивайте бдительность.** В рамках подготовки к охоте на угрозы, реагированию на инциденты и анализу системы безопасности научите отдел безопасности искать признаки света, шума или мусора, оставленного противником.
2. **Установите скрипучие ворота.** Подумайте о внедрении обманных индикаторов обнаружения и предупреждения атак (AS&W), например событий безопасности, которые срабатывают каждую минуту на контроллерах домена или других значимых системах или сетевых устройствах. Например, вы можете реализовать предупреждение, которое гласит: «[Предупреждение журнала событий безопасности]: Windows не удалось активировать Защитник Windows/Проверить версию Windows». Это может заставить атакующего думать, что вы не обращаете внимания на предупреждения от операционной системы, отключить их или увести свои журналы подальше от ваших датчиков. Внезапное отсутствие ложного предупреждения проинформирует

защитников вашей системы о присутствии злоумышленника (а в случае иного сбоя — о необходимости перезагрузить систему или попросить ИТ-отдел расследовать сбой).

3. **Сделайте деревянные трещотки.** Продвинутый злоумышленник тоже может целенаправленно запускать предупреждения или вызывать заметный сетевой шум из защищенного или скрытого места в вашей среде (то есть атаковать известные приманки), наблюдая за тем, способна ли ваша группа безопасности обнаруживать проникновения и реагировать на них. Это киберэквивалент ниндзя, который идет ночью по дому и гремит трещоткой, слушая вашу реакцию. Разумно предположить, что хакер может прощупывать вашу безопасность таким образом, чтобы определить, какое время и какие методы лучше всего подойдут для проникновения.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Поскольку невозможно повсюду иметь глаза, вы разместили своих охранников так, чтобы они могли прислушиваться к странным звукам на ключевых путях входа. Вы также научили охранников подмечать аномальные звуки. Вам сообщили, что у синоби есть специальные сандалии с мягкой тканевой подошвой, позволяющие ходить по плитке или камню, не создавая шума.

Как можно использовать эту информацию, чтобы обнаружить ниндзя в замке? Какие доказательства могут оставить после себя эти особые сандалии? Какие контрмеры вы могли бы применить, чтобы уменьшить угрозу от этих сандалий? Как ваши охранники должны реагировать, видя человека, подозрительно тихо идущего по замку?

Рекомендуемые меры безопасности и предосторожности

Эти рекомендации следует оценивать с точки зрения света, шума и мусора, которыми может сопровождаться нападение.

1. Определите возможности своей организации по обнаружению, смоделировав как шумное и быстрое проникновение, так и медленное и тихое. Задокументируйте, какие журналы с какой наблюдаемой деятельностью связаны и где у вас могут быть сенсорные мертвые зоны. (AU-2. События аудита; CA-8. Тестирование на проникновение; SC-42. Возможности сенсора и данные.)

2. Сопоставляйте журналы инцидентов, предупреждения и наблюдаемые данные с задокументированными действиями при угрозах, чтобы лучше информировать своих сотрудников и проверить, понимают ли они, как угрозы будут «звучать» в сети. (IR-4. Обработка инцидентов | (4) Корреляция информации.)
3. Настройте свои песочницы и детонационные камеры, чтобы искать признаки злоумышленника. (SC-44. Детонационные камеры.)
4. Используйте сигнатурные методы обнаружения скрытых действий, избегающих идентификации по сигнатурам. (SI-3. Защита от вредоносного кода | (7) Обнаружение без сигнатур.)
5. Разверните мониторинг информационной системы для обнаружения скрытой активности. Избегайте размещения сверхчувствительных датчиков в местах с высокой активностью. (SI-4. Мониторинг информационной системы.)

Резюме

В этой главе мы рассмотрели меры предосторожности, которые принимали синоби, и инструменты, используемые ими, чтобы скрыть свидетельства своей активности. Например, они измеряли, какой шум не услышат охранники, и следили, как они станут реагировать, если синоби все же будет обнаружен. Мы обсудили несколько киберинструментов, применяемых злоумышленниками, и их эквиваленты света и шума, которые могут обнаружить защитники. Наконец, рассмотрели возможные контрмеры, которые могут принять защитники.

В следующей главе мы обсудим обстоятельства, которые помогают синоби в проникновении, сглаживая проблемы со светом, шумом и мусором. Например, сильный ливень может скрыть шум и видимость, а также свидетельства присутствия. Киберзащитник может учитывать аналогичные обстоятельства для защиты своих систем.

21

Обстоятельства проникновения

Проникать можно в тот момент, когда противник движется, а если он не движется — нельзя.

Когда идет дождь, вы должны использовать его
для работы синоби и ночных атак.
«Ёсимори хяку-сю», № 1

В «Нимпидэн» и «Бансэнсюкай» написано, что при движении к цели синоби должен использовать укрытие, чтобы его не обнаружили. Он может дождаться момента, когда укрытие появится само, или при необходимости создать его. В трактатах описан широкий спектр обстоятельств, которые могут способствовать проникновению, от природных явлений (сильный ветер и дождь) и общественных мероприятий (торжества, свадьбы и религиозные службы) до действий, инициированных самим синоби (он может отвязать лошадей, спровоцировать драку или поджечь здание) [5].

Хитрый синоби должен уметь извлекать выгоду из отвлекающих факторов, волнения, замешательства и других условий, рассеивающих внимание цели, независимо от их происхождения [5]. Синоби умели превратить плохую погоду в благоприятные условия для проникновения. Например, сильные ливни обычно означали пустые улицы, плохую видимость и шум, заглушающий звуки шагов. Конечно, плохая погода для всех плохая, и второе стихотворение из «Ёсимори хяку-сю» гласит, что слишком сильный шторм может помешать синоби, затрудняя его действия: «В середине ночи, когда бушует ветер и дождь, на улицах так темно, что даже синоби не может провести атаку» [6].

Синоби может воспользоваться личными обстоятельствами, например трагической смертью в семье жертвы. Трактаты говорят, что пока цель в трауре, она в течение двух или трех ночей плохо спит, а это означает, что синоби могут приблизиться незамеченным во время похорон, раствориться в толпе скорбящих или проникнуть в дом на третью или четвертую ночь, когда цель наконец крепко уснет [5].

Конечно, судьба не всегда благоволила миссии синоби. В некоторых случаях они сами вносили в атакуемый объект какую-нибудь инфекцию. Больные были неэффективными защитниками, а ухаживающие за ними люди беспокоились и отказывали себе во сне, рискуя тоже заболеть. Когда пострадавшие начинали выздоравливать и их опекуны спокойно засыпали, возникал момент для проникновения синоби. Есть и другой вариант: синоби могли разрушить критически важный объект инфраструктуры, например мост, а затем дождаться, пока цель под жарким летним солнцем начнет большой ремонт, и проникнуть в замок измученного противника [5].

Военные действия тоже могут быть отвлекающими факторами. «Бансэнсюкай» описывает технику, называемую *кионин* («создание удачного момента с помощью неожиданности»), в которой используется помощь вооруженных сил или других синоби. Задействованные союзники заставляют цель думать, что атака уже началась: начинают обстрел, стучат в боевые барабаны или кричат. В образовавшейся суматохе синоби может проскользнуть внутрь. Когда синоби нужно безопасно уйти, фокус можно повторить [5].

В этой главе мы рассмотрим, как в цифровую эпоху воспользоваться описанными в трактатах синоби ситуациями, способствующими проникновению.

Способ использования удобной ситуации зависит от защитников, систем безопасности и организаций, которым не хватает рук, чтобы делать все и сразу. Из-за перегрузки, путаницы и акцентирования внимания не на тех вещах могут сложиться обстоятельства, которыми способен воспользоваться злоумышленник. Мы определим различные возможности, которые возникают в современных сетевых средах, и объясним, как они соотносятся с тем, что написано в трактатах синоби. Наконец, рассмотрим, как организации могут использовать меры безопасности и отказоустойчивость, чтобы подготовиться к возникновению ситуаций, которые потенциально могут ослабить защиту.

Состязательная возможность

Хакеры могут отвлекать свои цели и специально создавать угрозы, которые можно легко и быстро обнаружить, как когда-то делали синоби. Например, когда киберзащитники обнаруживают внезапную распределенную DDoS-атаку, стандартные рабочие процедуры требуют оценки силы и продолжительности DDoS и создания тикета (записи в системе управления безопасностью) с инцидентом безопасности для регистрации активности. Защитники не всегда распознают, что DDoS-атака представляет собой лишь прикрытие для атаки злоумышленника на сеть. Таким образом, когда атака подавляет датчики безопасности цели, системы захвата пакетов (packet capture, pcap) и системы обнаружения или предотвращения вторжений (IDS/IPS), эти системы начинают отказывать из-за неспособности обработать слишком много данных и пропускают пакеты с вредоносным содержимым. Когда DDoS-атака

прекратится, защитники увидят, что значительного простоя не возникло, и возвращают работу в нормальное состояние, не понимая, что хотя атака длилась всего 10 минут, поток пакетов дал противнику достаточно времени, чтобы обойти защиту системы и закрепиться в сети. (Во втором стихе «Ёсимори хяку-сю» говорилось, что сильный шторм может помешать как цели, так и атакующему, поэтому атака, скорее всего, окажется не слишком интенсивной. Очень интенсивная атака может привести к тому, что сетевое оборудование будет отклонять пакеты и терять данные связи, включая данные самой атаки. Вместо этого злоумышленник, скорее всего, замедлит (trottle) целевые системы, чтобы нарушить безопасность, не нарушая связи.)

У злоумышленников есть много других способов создать на объекте проникновения благоприятные обстоятельства, разнообразие которых ограничено лишь их изобретательностью. Выгодно проводить атаки на качество и надежность сервисов и инфраструктуры, например, нарушая работу интернет-провайдеров или межсетевых соединений. Терпеливые злоумышленники могут дождаться, когда коммерческие поставщики выпустят неисправные обновления или исправления, после чего служба безопасности или ИТ-персонал целевого объекта временно снимет часть ограничений или ослабит меры безопасности для устранения проблемы. Злоумышленники могут отслеживать процесс приобретения компанией чего-либо, чтобы определить, когда новые системы и серверы будут перемещаться в производство или в облако и, следовательно, когда они могут быть временно не защищены или неправильно настроены. Атакующие могут также отслеживать слияние компаний и пытаться атаковать разрывы, образовавшиеся при объединении сетей разных компаний. Также злоумышленники могут использовать специальные мероприятия, проводимые в здании цели, такие как большие конференции, выставки поставщиков и иные встречи, чтобы смешаться с толпой незнакомцев и проникнуть в здание. Возможно, им даже удастся что-то утащить.

Состязательные трудности

Невозможно гарантировать 100%-ную безотказную работу цифровых систем, и еще сложнее гарантировать их 100%-ную безопасность. Более того, почти наверняка невозможно предотвратить бедствия, опасности, аварии, сбои и непредвиденные изменения, которые могут создать удобные обстоятельства для атакующих. Стремление максимально застраховаться от любых подобных обстоятельств может помешать бизнесу реализовывать смелые стратегии и добиваться поставленных целей. Одним из возможных решений может быть дублирование многоуровневых систем для уменьшения вероятности проникновения. Команды безопасности могут ввести в действие эквивалент безопасности высокой доступности, а именно многоуровневое резервирование более слабых систем. Это и есть *осведомленность и готовность к действию*. В рамках протоколов службы безопасности по управлению изменениями, событиями, инцидентами, кризисами, стихийными бедствиями и другими отвлекающими

обстоятельствами можно обучить службу безопасности находить признаки того, что событие было создано искусственно или используется злоумышленниками для проникновения в организацию. Задокументируйте роли сотрудников в организационных политиках и процедурах. Задействуйте моделирование угроз, тренировки и управление рисками для выявления потенциальных отвлекающих факторов, а затем подумайте о мерах безопасности, контрмерах и способах устранения таких факторов.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Вы заметили, что во время особенно сильных и холодных штормов охранники у ворот прячутся в будки, закрывают лица, что мешает им смотреть, и согреваются у небольших костров, которые делают их силуэты видимыми.

Как синоби может воспользоваться погодными условиями, такими как метель или ледяной шторм, чтобы проникнуть в замок? Как ему следует одеться? С какой стороны зайти? Насколько свободно синоби может действовать с учетом работы охраны? Какие ограничения физического доступа и протоколы безопасности могут применять ваши охранники во время метели? Нельзя ли улучшить сторожевые посты, чтобы ваши солдаты могли эффективно наблюдать за действиями в таких условиях? Какие еще отвлекающие обстоятельства помимо погодных явлений вы можете придумать и как им противостоять?

Рекомендуемые меры безопасности и предосторожности

Рекомендации следует оценивать с учетом концепции обстоятельств проникновения.

1. Определите и задокументируйте, как различные меры безопасности и протоколы, например аутентификация, могут во время чрезвычайных ситуаций помочь предотвратить проникновение злоумышленника. (AC-14. Разрешенные действия без идентификации или аутентификации.)
2. Установите меры контроля и политики для условий использования внешних информационных систем, особенно в моменты ослабления запретов. (AC-20. Использование внешних информационных систем.)
3. Проведите обучение по тестированию на проникновение во время тренировок по отработке смоделированных чрезвычайных ситуаций, например пожарных учений, чтобы проверить возможности защиты и обнаружения. (CA-8.

Тестирование на проникновение; CP-3. Обучение на случай непредвиденных обстоятельств; IR-2. Обучение реагированию на инциденты.)

4. Принудительно ограничьте физический доступ посетителям, особенно в ситуациях, когда невозможно сопровождать большой неконтролируемый поток людей, например сотрудников пожарной команды. В любом случае необходимо предотвратить несанкционированный вход в систему и выход из нее. (PE-3. Контроль физического доступа.)
5. Научитесь отключать информационные системы и сети в случае чрезвычайной ситуации, если есть подозрение, что вашу защиту скомпрометировал злоумышленник. (PE-10. Аварийное отключение.)
6. Подумайте, как ваша организация может включить отслеживание возможных атак в планирование действий в чрезвычайных ситуациях. (CP-2. План на случай чрезвычайных ситуаций.)
7. Оцените, создаст ли внезапный перенос бизнес-операций на резервную платформу или их возобновление благоприятные обстоятельства для проникновения злоумышленника. После этого подумайте о защитных мерах предосторожности и смягчения последствий этих действий. (CP-7. Смена платформы.)

Резюме

В этой главе мы рассмотрели тактику создания и/или ожидания обстоятельств, обеспечивающих прикрытие для проникновения в целевой объект. Привели несколько примеров того, как синоби могут создавать себе возможности, если цель хорошо защищена, и исследовали, как эта тактика может применяться в современных сетевых средах. Мы поговорили о различных методах управления безопасностью в моменты ослабления защиты и в ходе решения мысленного упражнения рассмотрели подготовку к обстоятельствам, в которых риска нельзя избежать.

В следующей главе мы обсудим нулевой день — настолько новое и секретное средство проникновения, что от него пока не придумано защиты. У синоби были подвиги и техники, похожие на нулевые дни, но они были настолько секретными, что их было запрещено записывать, а трактаты ссылались на них лишь косвенно. У нас остались только загадочные подсказки, предназначенные для того, чтобы напомнить синоби о секретной технике, но не для обучения ей. Тем не менее трактаты дают представление о том, как создавать новые нулевые дни, о процедурах защиты от них и о хитростях при их реализации. Кроме того, трактаты описывают несколько использовавшихся ранее техник нулевого дня, которые утратили новизну из-за их раскрытия, что дает нам представление о современных эксплойтах нулевого дня и возможном развитии этой тактики в будущем.

22

Нулевые дни

Секрет работает, лишь пока хранится в секрете.
Стоит разболтать его — и ты проиграл.

Важно знать, что не стоит использовать какие-либо
древние известные людям способы, чтобы
не потерять эффект неожиданности.
«Сёнинки», Takaki wo Koe Hikuki ni Hairu no Narai [7]

Одним из ключевых тактических преимуществ синоби была скрытность. Трактаты неоднократно предупреждали синоби, что нельзя давать посторонним понять, на что он способен, так как если информация о технике синоби станет достоянием общественности, последствия могут быть катастрофическими. Мало того что при жизни целых поколений эти техники станет невозможно использовать, так еще и сами синоби, применяющие уже не секретные техники, будут смертельно рисковать. «Сёнинки» и «Нимпидэн» описывают опасности раскрытия секретного ремесла ниндзя посторонним, а иногда даже советуют убивать цели, которые слишком много знают, или посторонних, которым удалось увидеть синоби в действии [5].

«Сёнинки» и «Нимпидэн» приводят в пример древние техники, уничтоженные публичным разоблачением. Например, когда древние ниндзя (*ямо*) [7] проводили разведку, они иногда путешествовали по фермерским полям и, чтобы избежать обнаружения, одевались как чучело и принимали убедительную позу при приближении людей [6]. Как только этот метод был раскрыт, местные жители начали регулярно проверять чучела, нападали на них и даже били ножом. Независимо от того, насколько убедительна была маскировка синоби или насколько искусен он в пантомиме, техника стала слишком рискованной, и синоби приходилось либо разрабатывать новые способы прятаться у всех на виду, либо вообще избегать полей. Навык был утерян.

Еще один пример: некоторые синоби научились искусно имитировать звуки, издаваемые кошками и собаками, и если синоби во время миссии выдавал свое присутствие, он начинал лаять или мяукать, чтобы убедить цель в том, что звук издает пробегающее мимо животное и беспокоиться не о чем. В какой-то момент эта техника также была раскрыта. Охранники стали проверять, действительно ли подозрительные звуки издает животное, из-за чего синоби очень рисковали [5].

Трактаты также описывают, как нужно действовать, когда укрепление защищали собаки, которых синоби не могли убить, похитить или подкупить, не вызвав подозрений у охранников. В этом случае синоби нужно было воспользоваться китовым жиром, имеющим специфический запах, а затем либо дождаться, пока собака уйдет подальше от охранников, либо выманить ее. Затем синоби бил собаку, и так продолжалось несколько ночей подряд. Собака ассоциировала с резким запахом китового жира боль и наказание и начинала бояться нападать на синоби, которые так пахли. Когда эта техника была раскрыта, охранников научили подмечать особенный запах китового жира или изменение в поведении собаки [7].

Разумеется, большинство секретов синоби оставались нераскрытыми до самого официального опубликования трактатов, когда сами они стали фактически историческим реликтом. Но в те времена защитникам приходилось придумывать, как предотвратить нападение, о котором ничего не известно, причем не только защитникам, но порой и самим злоумышленникам.

Для ситуаций, когда синоби выступали в роли защитников, трактаты предлагали базовые советы. «Руководство для командиров» «Бансэнсюкай» [5] рекомендует использовать различные передовые методы обеспечения безопасности, включая пароли, сертификационные штампы, опознавательные знаки, секретные знаки и сигналы. Трактат также советует командирам задуматься о причинах, лежащих в основе этих мер безопасности, сочетать их с другими стандартными мерами, такими как ночные дежурства и охрана, принимать особые меры предосторожности, например устанавливать ловушки, и самим разрабатывать секретные, индивидуальные и динамические решения безопасности. Все вместе эти техники позволяли защититься от нападающих с низким или средним уровнем мастерства, но от самых искушенных синоби — нет [5].

Например, самый прагматичный совет «Бансэнсюкай» по безопасности заключается в том, что защитник никогда не находится в полной безопасности, даже если он всегда внимателен и безупречно дисциплинирован. Всегда найдутся пробелы, которые синоби сможет использовать. Трактат подчеркивает важность понимания философии, мировоззрения и мышления своих врагов и призывает синоби быть открытыми для испытания новых техник, иногда на ходу: «Трудно точно сказать, как действовать, — все зависит от ситуации, времени и места. Если перечень ваших инструментов ограничен, а форма постоянна, то даже величайший генерал не сумеет одержать победу» [5].

Синоби-защитники использовали творческое мысленное моделирование, например, придумывая обратные сценарии и исследуя возможные пробелы в них. Они черпали вдохновение в природе, представляя, как рыба, птица или обезьяна проникают в замок и как можно имитировать способности животных [5]. Они узнавали новые методы, изучая приемы обычных воров (*нусубито*). Прежде всего они доверяли своему разуму и постоянно учились, решали проблемы, развивали логический анализ и гибкость ума.

Синоби может извлечь из своего опыта миллионы уроков, незаметных и изменчивых, и их нельзя преподать или передать новому поколению. Одно из самых важных для них — всегда стараться знать о любом месте или провинции все, что только можно. Если его разум полностью соответствует порядку вещей, работает стройно и логично, тогда он можете пройти через «врата без ворот». Человеческий ум изумителен и гибок. Это потрясающе. Со временем вы поймете суть вещей, и понимание снизойдет на вас словно по волшебству. «На <пути синоби> ты должен изучать все, что можно... использовать свое воображение и проницательность, чтобы понять и уловить суть всякой вещи» [7].

Дальновидный синоби с острым умом и дисциплинированный может создать сильную оборону, чтобы противостоять неизвестным атакам и заставить врагов тратить время и ресурсы на разработку новых планов атак, прощупывание системы безопасности и борьбу со скрытой защитой, — и все это лишь для того, чтобы испытать разочарование, когда вся система безопасности динамически подстроится под изменения.

В этой главе мы исследуем современный ландшафт угроз нулевого дня и поймем, что из философии и профессионального мастерства синоби мы можем применить в кибербезопасности. Кроме того, рассмотрим различные средства защиты от атак нулевого дня. Упражнение в этой главе предлагает подумать о неизвестном и потенциальном нулевом дне, скрытом в современном вычислительном оборудовании, программном обеспечении, облаках и сетях — и все это в надежде найти новые идеи.

Нулевой день

В кибербезопасности есть термин, который вселяет наибольший страх в сердца защитников, — это *нулевой день* (или *0-день*), эксплойт или атака, которые ранее были неизвестны и с которыми защитники еще не научились бороться. Термин подразумевает, что этот вид атаки известен в течение нуля дней. Поскольку жертвы и защитники не имели возможности изучить угрозу, злоумышленник, использующий атаку нулевого дня, нацеленную на широко применяемую технологию, почти всегда добивается успеха. Например, в STUXNET использовались четыре эксплойта

нулевого дня, чтобы саботировать работу ядерного обогатительного завода в Иране. Этот случай показал силу нулевого дня в нападении даже на самые безопасные и защищенные объекты [48].

Атака нулевого дня ценна тем, что о ней никто ничего не знает. Как только злоумышленник использует ее, жертва может найти доказательства атаки с помощью датчиков и систем мониторинга, провести экспертизу доказательств и проанализировать атаку. Когда она будет раскрыта, специалисты по безопасности смогут разработать меры по снижению рисков, сигнатуры обнаружения и исправления, а также опубликуют номера CVE, чтобы поделиться информацией с сообществом. Не все обращают внимание на такие рекомендации и исправляют свои системы, но все равно атака нулевого дня будет со временем терять эффективность.

Атаки нулевого дня реализуются по-разному в зависимости от мотивов злоумышленника. Киберпреступники, которым нужно быстро добиться результата, могут использовать уязвимость нулевого дня в масштабной и хорошо заметной атаке, получив максимум выгоды здесь и сейчас. Более продвинутые злодеи устанавливают процедуры удаления артефактов, журналов и других наблюдаемых свидетельств атаки нулевого дня, продлевая срок ее существования.

По-настоящему изощренные злоумышленники прибегают к уязвимостям нулевого дня для атаки на надежно защищенные ценные цели, поскольку при нападении на обычные цели секрет атаки может быть продан киберпреступниками на черном рынке за тысячи или даже миллионы долларов правительствам, которые хотят разработать методы защиты.

Некоторые атаки нулевого дня порождаются существующими пробелами в безопасности программного кода, но иногда злоумышленники могут нарочно вводить уязвимости нулевого дня в исходный код программного приложения посредством соглашений или использования скрытых человеческих ресурсов. Под прицел такой атаки могут попасть программные библиотеки, оборудование или компиляторы, в которых появляются ошибки, бэкдоры и другие скрытые уязвимости. Точно так же ниндзя, присоединяющийся к строителям, работающим на возведении замка, может поставить под угрозу проект, создав секретные входы, о которых знает только он (подобные случаи упоминаются в трактатах) [5].

Обычно уязвимости нулевого дня раскрывают исследователи безопасности с большим опытом изучения кода, охотники за угрозами или аналитики, случайно обнаружившие эксплойт, использованный против них. Хотя уязвимости нулевого дня все еще работают, последние технологии, такие как фаззинг, помогли автоматизировать их обнаружение. Фаззеры и подобные инструменты автоматически пробуют применять различные входные данные (случайные, недействительные и неожиданные), пытаясь обнаружить ранее неизвестные уязвимости системы. Появление фаззеров и систем защиты на основе искусственного интеллекта (ИИ) говорит

о появлении новой парадигмы. Подобно тому как изобретение пушки, которая могла пробивать стены замка, заставило менять стратегии защиты, ИИ позволяет рассчитывать на то, что защита когда-нибудь начнет развиваться столь же быстро, как и угрозы. Конечно, системы атаки тоже могут научиться преодолевать любые защитные барьеры, изменяя не только защиту от атак нулевого дня, но и взгляд на кибербезопасность в целом.

А пока модель использования пробелов в защите и обнаружения атак циклична. Злоумышленники выявляют различные эксплойты и уязвимости, такие как SQL-инъекции, XSS или утечки памяти. Постепенно защитники вырабатывают методы борьбы с этими угрозами, а злоумышленники начинают использовать другие способы и технологии, и цикл продолжается. По прошествии времени, когда защитники и злоумышленники уволятся, новое поколение злоумышленников вновь обнаружит те же самые распространенные слабости в новом программном обеспечении и технологиях, что приведет к возрождению старых нулевых дней — цикл начнется заново.

Защита от атак нулевого дня

Обнаружение атак нулевого дня и защита от них часто используются новичками на рынке кибербезопасности как козырь, поскольку они любят наобещать получение фантастических результатов. Это не значит, что их решения не работают. Но можно нарваться и на шарлатанов. Будьте уверены, я не пытаюсь продать вам ничего, кроме практических рекомендаций, приведенных далее.

1. **Используйте передовой опыт.** От атак нулевого дня, как и от безумия, сложно защититься, но это не означает, что нужно опустить руки. Пользуйтесь лучшими отраслевыми практиками. Полностью нейтрализовать такие атаки нельзя, но можно усложнить попытки злоумышленников напасть на вашу среду и дать организации больше шансов обнаружить атаку и отреагировать на нее. Вместо того чтобы праздно волноваться о возможных уязвимостях нулевого дня, исправьте и смягчите последствия более старых, известных атак и минимизируйте время, в течение которого ваша организация остается уязвимой для них.
2. **Используйте команды охотников и «синие команды».** Соберите или наймите команду охотников и «синюю команду» для работы над стратегиями защиты нулевого дня.
3. **Команда охотников состоит из особых защитников, которые не полагаются на стандартную защиту на основе сигнатур.** Вместо этого они постоянно делают предположения о том, как злоумышленники могут использовать уязвимости нулевого дня или другие методы проникновения в сети. Основываясь

на этих предположениях, они охотятся на угрозы с помощью приманок, поведенческого и статистического анализа, прогнозирования угроз и других специальных методов.

«Синяя команда» состоит из особых защитников, которые проектируют, тестируют и реализуют настоящую защиту. Сначала они документируют информационный поток системы или сети, а затем создают модели угроз, описывающие реальные и воображаемые атаки, которые могут оказаться успешными против существующей схемы. В отличие от охотничьей команды, «синяя команда» не занимается отловом атак нулевого дня. Вместо этого она оценивает свои модели информации и угроз с точки зрения атаки нулевого дня, чтобы определить, как эффективно уменьшить ущерб, обезопасить, укрепить и защитить свои системы. «Синяя команда» действует отдельно от обычной службы безопасности, эксплуатации и реагирования на инциденты, но должна проверять имеющиеся отчеты по реагированию на инциденты, чтобы определить, где оборона была пробита и как построить более действенную защиту от подобных атак в будущем.

4. **Реализуйте динамическую защиту… но аккуратно.** В последние годы специалисты в области безопасности приложили немало усилий к внедрению сложных мер защиты, которые:

   - пытаются сделать сеть подвижной целью, например, с помощью ночных обновлений;
   - вводят рандомизацию, например, адресного пространства (address space layout randomization, ASLR);
   - динамически изменяют систему при взаимодействии — например, с помощью квантовой криптографии;
   - инициируют нечеткие защитные условия или иммунный ответ.

   Некоторые из этих динамических мер защиты изначально были довольно успешными, но затем противники разработали способы их преодоления, превратив их в практически статические со стратегической точки зрения.

   Поговорите со специалистами в области кибербезопасности и изучите литературу по современным средствам динамической защиты, чтобы определить, какие средства подойдут вашей организации. Однако действуйте осторожно, поскольку сегодняшняя динамическая защита завтра может стать стандартным уровнем безопасности, который легко обойти.

5. **Создайте более скучную защиту.** Подумайте об использовании скучных систем, методов кодирования и реализаций. Скучная защита, чье начало было положено проектом с открытым исходным кодом Google BoringSSL [12], предлагает упростить и уменьшить плоскость атаки, размер, зависимости

и сложность вашего кода. Короче, система становится скучной, но, вероятно, это позволит устранить важные или критические уязвимости. В соответствии с этой практикой (которая может быть эффективной на уровне кода, приложения или системы) код не должен быть сложным или красивым, а скорее самым занудным образом защищен и неизменен по структуре, написан скучными и простыми реализациями. Теоретически упрощение кода для чтения людьми и машинами, а также тестирования и интерпретации снижает вероятность того, что неожиданные входные данные или события обнаружат уязвимость нулевого дня.

6. **Практикуйте отрицание и обман (denial and deception, D&D).** Концепция D&D предотвращает получение злоумышленниками информации о вашей среде, системах, сети, людях, данных и других наблюдаемых объектах и может обманом заставить их предпринять действия, которые вам выгодны. Поскольку злоумышленники усложняют разведку, вооружение и доставку эксплойтов, они вынуждены тратить больше времени на тестирование, изучение и проверку того, что дыра, которую они подозревают в вашей среде, действительно существует. Например, вы можете обманным путем модифицировать свои системы так, словно на них стоит другая ОС или ПО, допустим, изменив экземпляр Solaris, чтобы он выглядел как ОС SELinux (в идеале стоило бы и вовсе перейти на SELinux, но логистика устаревших ИТ-систем может вынуждать вашу организацию полагаться на старое программное обеспечение дольше, чем хотелось бы). Если обман окажется эффективным, злоумышленники будут пытаться атаковать ваш экземпляр SELinux, а это не получится, потому что SELinux там и в помине нет.

   Обратите внимание на то, что концепцию D&D следует применять не саму по себе, а как дополнение к передовым методам обеспечения безопасности, чтобы улучшить их. D&D — это эндшпиль в области безопасности для очень зрелых организаций, ищущих дополнительные способы защищать систему от злоумышленников, как описано в «Бансэнсюкай» [5].

7. **Отключение во благо.** В концепции защиты через отключения «Сёнинки» учит вас отключаться от врага мысленно, стратегически, физически и любым другим способом [7]. В сфере кибербезопасности это означает создание изолированной «синей команды», которая обращена внутрь себя, работает в отрыве от мира и игнорирует все новости в сфере безопасности, анализа угроз, исправлений, эксплойтов, новых вредоносных программ, сигнатур и ультрасовременных продуктов. Отключается все, что может повлиять на их разум, изменить их образ мыслей или обеспечить связь с врагом. При правильном применении навык отключения разворачивает мышление защитников в направлении, далеком от отраслевого стандарта. У противников возникают проблемы с тем, чтобы перенять такой способ мышления,

а защитники разрабатывают уникальные секретные стратегии защиты, с которыми противник еще не сталкивался, что чрезвычайно затрудняет работу атак нулевого дня.

Как и D&D, этот метод рекомендуется использовать лишь в том случае, когда все остальные средства кибербезопасности уже задействованы. В противном случае отключение от врага и действия в темноте могут привести к обратным результатам.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Ходят слухи, что синоби проник в группу строителей, возводивших ваш замок, и создал в системе безопасности замка парочку черных ходов и других уязвимых мест. Синоби, знакомые с расположением и механизмами этих уязвимостей, могут свободно входить в замок и выходить из него, минуя охрану и средства безопасности. Вы отправили охранников, архитекторов и даже наемных синоби проверить замок на наличие скрытых уязвимостей, но они ничего не нашли. У вас нет денег, времени или ресурсов, чтобы построить новый замок без черных ходов.

Как бы вы продолжили жить в замке, зная, что в нем есть скрытый недостаток, который синоби может использовать в любое время? Как будете охранять находящиеся в нем сокровища, людей и информацию? Как найти эту скрытую слабость или защититься от нее, не зная, как она выглядит, где находится и как применяется? Как еще вы могли бы управлять риском этой неизвестной уязвимости?

Рекомендуемые меры безопасности и предосторожности

Эти рекомендации следует оценивать с учетом концепции нулевого дня.

1. Создайте для вашей организации настраиваемые, динамические и адаптивные меры безопасности, чтобы дополнить ими передовые методы безопасности. (AC-2. Управление учетной записью | (6) Динамическое управление привилегиями; AC-4. Сопровождение информационных потоков | (3) Управление потоком динамической информации; AC-16. Атрибуты безопасности и конфиденциальности | (1) Ассоциация динамических атрибутов; IA-10. Адаптивная аутентификация; IR-4. Обработка инцидентов | (2) Динамическая

реконфигурация; IR-10. Группа анализа интегрированной информации по безопасности; PL-8. Архитектуры безопасности и конфиденциальности | (1) Глубокая оборона; SA-20. Индивидуальная разработка критических компонентов; SC-7. Граничная защита | (20) Динамическая изоляция и сегрегация; SI-14. Непостоянство.)

2. Сохраняйте записи об атаках нулевого дня, включая то, когда и как они были обнаружены, на какие технологии нацелены, а также результаты сканирования уязвимостей и их корреляцию с прогнозируемыми будущими атаками. (AU-6. Аудиторский обзор, анализ и отчетность | (5) Комплексный анализ записей аудита; SA-15. Процесс разработки, стандарт и инструменты | (8) Повторное использование информации об угрозах и уязвимостях.)
3. Проведите специализированное сканирование уязвимостей, проверку и системное тестирование для оценки безопасности нулевого дня. (CA-2. Оценки | (2) Специализированные оценки.)
4. Обратитесь к специалистам по тестированию на проникновение, поручив им найти уязвимости в вашем программном обеспечении, системах и других технологиях, чтобы вы могли в дальнейшем защищаться от них. (CA-8. Тестирование на проникновение; RA-6. Обзор средств технического наблюдения и противодействия.)
5. Смоделируйте угрозы для своих систем и программного обеспечения, чтобы оценить потенциальные атаки нулевого дня и меры, которые вы можете заранее принять для смягчения их последствий. Подумайте о внедрении скучного кода. (SA-11. Тестирование и оценка разработчика | (2) Моделирование угроз и анализ уязвимостей; SA-15. Процесс разработки, стандарт и инструменты | (5) Уменьшение плоскости атаки; SI-10. Проверка ввода информации | (3) Предсказуемое поведение.)
6. Внедряйте настраиваемые, разнообразные и уникальные средства защиты для снижения вероятности атак нулевого дня. (SC-29. Неоднородность.)
7. Проводите кампании отрицания и обмана, чтобы уменьшить для злоумышленников возможность выполнять разведку, использовать свои инструменты и проводить атаки нулевого дня против вашей организации. (SC-30. Сокрытие и перенаправление.)
8. Организуйте службы охоты и безопасности, которые будут искать индикаторы атак и эксплойтов нулевого дня. (SI-4. Системный мониторинг | (24) Индикаторы компрометации.)
9. Проводите регулярное автоматизированное сканирование доступности, чтобы устранить уязвимые для более старых атак места. (RA-5. Сканирование уязвимостей; SI-2. Устранение недостатков.)

Резюме

В этой главе мы поговорили о секретности техник и ремесла синоби, сохраняемой на протяжении веков, и поняли, как много этих секретных техник похожи на эксплойты и уязвимости нулевого дня, которые мы наблюдаем сегодня. Рассмотрели текущее состояние дел и потенциальное будущее атак нулевого дня с точки зрения кибербезопасности, кибервойны и информационного превосходства. Здесь говорилось о том, что разговоры об атаках нулевого дня могут показаться бессмысленными, но на самом деле они имеют решающее значение для противодействия угрозе.

В следующей главе мы обсудим найм агента для борьбы с атаками нулевого дня и всевозможными угрозами. Рассмотрим рекомендации, которые трактаты предлагают учитывать при рекрутировании новых синоби, и исследуем их применение к привлечению талантов в области кибербезопасности. Все постоянно говорят, что в сфере кибербезопасности не хватает талантов, и я подозреваю, что аналогичная проблема нехватки синоби существовала в периоды раздоров в средневековой Японии. Трактаты синоби объясняют, как определить, кого можно обучить и превратить в хорошего синоби, а эта роль была гораздо более важной, чем сегодняшняя офисная работа. Неудачный рекрут, скорее всего, погибнет, что приведет к потере инвестиций в обучение и поставит под угрозу миссии и жизни членов команды.

23

Найм синоби

При необходимости защиты от вражеских атак или синоби или в случае чрезвычайной ситуации вам может показаться, что нужно просто нанять больше людей. Но на самом деле не стоит брать в армию новичков без тщательного отбора.

Синоби должен соблюдать три основных принципа:
грамотная речь, смелость и стратегия.
«Ёсимори хяку-сю», № 38

Нам известно, что синоби в феодальной Японии выполняли разные миссии, такие как шпионаж и саботаж, организация набегов, сбор информации, убийство и, возможно, самая полезная из всех задач — защита от вражеских синоби. Но чтобы использовать синоби для этих целей, военачальники сначала должны были сделать то же самое, что руководители и менеджеры наших дней, — набрать персонал.

Отдельные крупные отрывки из «Бансэнсюкай» и «Ёсимори хяку-сю» дают советы лордам, зачем им нанимать синоби, как и когда их использовать, а также описывают качества хорошего кандидата в синоби. Согласно трактатам, идеальный синоби должен быть [5]:

- **умным** — логичным, самостоятельно и стратегически мыслящим, с хорошей памятью, острой наблюдательностью и способностью к быстрому обучению;
- **терпеливым** — вдумчивым, но решительным агентом с образцовой силой воли и самообладанием;
- **толковым** — находчивым, творческим и смелым в своей области, с серьезным послужным списком и видением победы даже в ужасных ситуациях;

- **верным** — искренним, благородным и доброжелательным по отношению к другим, способным брать на себя ответственность за свои действия;
- **красноречивым** — способным эффективно общаться с военачальниками и союзниками.

Синоби, желающие занять руководящие должности, в дополнение к этим качествам должны уметь эффективно расставлять приоритеты, успешно реализовывать сложные тактики и сохранять самообладание в сложных ситуациях [5].

В трактатах также отмечаются черты, по которым кандидатов стоит отсеивать, например: эгоизм, глупость, безнравственность (использование своих навыков для личной выгоды), вероятность чрезмерного употребления алкоголя, похоть или жадность [5]. Иногда также возникала проблема кумовства и родственных связей. Хоть вероятность стать успешным синоби увеличивалась, если ребенок родился в деревне синоби (в первую очередь Ига и Кока) и с малых лет обучался ремеслу, все же рождение у родителей-синоби не гарантировало успеха. Такие дети могли стать плохими кандидатами с полным набором перечисленных отрицательных качеств [5].

Важно отметить, что в приведенном списке желательных и нежелательных качеств нет никаких требований к конкретным навыкам, прошлому опыту, образованию, социальному происхождению, званиям или регалиям и даже возрасту и полу. Возможность стать синоби зависела в большей степени от характера, жизненных ценностей, квалификации и способностей человека.

Трактаты не дают каких-либо конкретных указаний по рекрутированию, проведению собеседования или оценке кандидатов, но в «Сёнинки» приводятся советы на тему того, как глубже понять природу человека: его знания, образ мышления, убеждения, желания, недостатки и черты характера. Хотя эти методы обычно используются для шпионажа и преследования, их можно применять и для собеседования с новобранцами.

Например, «Сёнинки» рекомендует заглядывать в места, где кандидат часто бывает, и собирать информацию у местных жителей, которые хорошо его знают. Наиболее точные сведения поступают из мест, где он чувствует себя комфортно или общается с хозяевами или клиентами. Именно в таком месте часто раскрываются секреты [7].

Существует также умение под названием *хито ни курума во какеру* — «растопить сердце лестью». Собеседующий задает кандидату вопросы и хвалит за ответы. Подобная лесть показывает его менее умным и демонстрирует нечто вроде трепета перед способностями кандидата. Если этот прием реализован убедительно, человек расслабится, станет чувствовать себя уверенно и начнет с удовольствием

рассказывать о себе, что позволит получить немало ценных сведений. Например, когда собеседник попривыкнет, можно сменить тему разговора и посмотреть, как он отреагирует на неожиданные вопросы. Так можно понять, есть ли у человека свое мнение или он просто повторяет то, что услышал от других [7].

Вербовка союзников и выбор врагов для синоби являлись вопросами жизни и смерти. Им часто приходилось решать, доверить ли человеку свою жизнь или он ненадежен и подведет команду во время опасной миссии. Необходимость делать такой сложный выбор научила синоби применять описанные и иные техники, распознавать суть человека, быстро и незаметно оценивать способности, знания и характер кандидата [7].

В этой главе мы рассмотрим распространенные практики рекрутинга в современных организациях и узнаем, как можно использовать мудрость синоби при найме и обучении талантов. Многие специалисты по кадрам и даже синоби из прошлого считают, что они способны оценить пригодность человека к определенной деятельности после обстоятельного собеседования. Иногда это так, но многие кандидаты не доходят до собеседования из-за различных сигналов, предварительных условий и маркеров, по которым служба персонала может заранее отсеять их. Мы исследуем процессы найма с точки зрения того, почему они мешают достичь желаемого результата.

Таланты в кибербезопасности

Бурный рост сектора кибербезопасности привел к проблемам с нехваткой людей, достаточно компетентных для выполнения всей необходимой работы. Это отчасти связано с тем, что кибербезопасность — относительно новая область деятельности с высоким порогом вхождения, к тому же сегодняшние методы оценки кандидатов не вполне хороши. В слишком многих частных компаниях при подборе кандидатов смотрят лишь на галочки в правильных полях в резюме или выполнение тестовых задач, при этом иногда такие кандидаты свои повседневные обязанности выполняют плохо. Кандидаты, рекрутеры и программы обучения подстроились под то, что нужно для получения работы, и все вместе позиционируют себя соответствующим образом, снижая эффективность традиционных методов найма и оценки кандидатов. Университеты выпускают с факультетов компьютерных наук студентов, которые не могут решить задачу FizzBuzz, предназначенную для проверки базовых навыков программирования. Кандидаты представляют потенциальным работодателям необъективные или вымышленные рекомендации. Сотрудники ищут бессмысленные должности, которые хорошо смотрятся в резюме, но плохо коррелируют с их опытом работы или способностями. Карьеристы получают кучу сертификатов в области информационных технологий или безопасности, готовясь к тестам (и часто почти сразу же забывают полученную информацию), публикуют мелкие бессмысленные

статьи, чтобы пустить пыль в глаза, подают заявки на патенты, добавляя свои имена к проектам, к которым они почти не имеют отношения.

Способы борьбы с хитростями вроде выдаваемых на дом тестов легко обойти с помощью Google или прямого плагиата. Головоломки, которые предлагается решить прямо на собеседовании, когда-то были новинкой, а теперь стали обычным делом. Кандидаты много практикуются в их решении, а иногда и вовсе точно знают, какие задания дает именно эта компания. Но даже если задача сохраняется в секрете, ни один из перечисленных критериев не позволяет точно оценить способность кандидата выполнять работу по обеспечению кибербезопасности.

Ради справедливости отметим, что у кандидатов тоже есть немало оснований с подозрением относиться к работодателю в сфере кибербезопасности. Даже если организация нанимает невероятного профессионала, достойного звания «кибериндзя», нет никаких гарантий, что работодатель будет использовать его эффективно. Этот риск существует в любой отрасли, но у компаний, занимающихся кибербезопасностью, он становится еще выше по ряду причин, включая малоизвестность высокотехнологичной профессии, эволюцию технологий, непонимание возможностей сотрудника руководством, а также важность креативного мышления. Чтобы хорошо делать свою работу и обеспечивать безопасность организации, сотрудникам нужна поддержка руководства и карт-бланш на то, чтобы полностью реализовать свои навыки, не боясь наказания или откровенного саботажа.

В число крупнейших нанимателей, работодателей и инструкторов для киберспециалистов входят американские военные, которые могут взять почти незнакомых с компьютерами балбесов, бросивших школу, и за 18 месяцев обучить их до уровня специалиста по кибервойне. Конечно, не каждый новобранец проходит обучение, так как существуют определенные требования, по которым отфильтровывают плохих кандидатов (кстати, так же поступали и с новобранцами согласно «Бансэнсюкай») [5].

При найме в армию одной из особенностей является тест на профессиональную пригодность военнослужащих (Armed Services Vocational Aptitude Battery, ASVAB) [46]. В отличие от собеседования в компании, где ценятся прошлые достижения и профессиональные качества, ASVAB оценивает потенциал к обучению, способности и общие технические навыки новобранцев. По специальной системе баллов для кандидатов определяются специальности, в которых они могут продолжить работу в случае успешного обучения. Тест ASVAB оказался очень эффективным для военных, но стоит отметить, что на некоторых должностях встречается неожиданно высокий результат обучения, но низкая производительность в полевых условиях, что, вероятно, связано с определенными качествами, которые ASVAB не всегда проверяет. В организованном и структурированном мире вооруженных сил бывает сложно выявить или обучить людей, которые решают проблемы с применением

творческого, бесстрашного и независимого мышления, как, собственно, работают хакеры.

Работа с талантами

Любая компания стремится нанять профессионала в области кибербезопасности, вот только их не так-то много. Как же тогда каждой компании найти свой талант в области кибербезопасности? Организациям следует сначала определить, хотят ли они развивать новичка самостоятельно или бороться с другими организациями за готового опытного специалиста. Многие из приведенных далее рекомендаций подходят для развития талантов, но могут применяться и при смешанном подходе.

Многие специалисты в области кибербезопасности считают, что современная практика приема на работу устарела и пришло время попробовать что-то новое. В качестве альтернативы попробуйте рассмотреть следующие подходы к найму и поддержанию талантов.

1. **На собеседовании проверяйте практические знания.** Вместо опросов, случайных головоломок на доске, упражнений по программированию в реальном времени или домашних проектов попросите кандидата сделать что-то из реальной работы, которую ему предстоит выполнять. Проведите собеседование в той же среде и в тех же условиях, в которых он будет работать в случае найма. Проверяйте свою систему оценки, давая упражнения нынешним сотрудникам, после чего оценивайте результаты и корреляцию между результатами теста и фактической производительностью труда. Сохраняйте модульность оценок и регулярно изменяйте их, чтобы кандидаты не могли рассказать друг другу, что спрашивают на собеседовании. Регулярно включайте в тест новые проблемы, с которыми столкнулись ваши сотрудники, чтобы тест соответствовал требованиям к работе. В идеале тест должен позволять определить компетенцию кандидата за 30 минут или меньше, и у последнего должно быть достаточно времени для его решения с помощью интернета или методом быстрых проб и ошибок.
2. **Проверьте работу с черным ящиком.** Дайте кандидату модульную полуслучайную псевдотехнологию и попросите его разобраться в том, как она работает, чтобы ее можно было взломать и/или защитить. Это упражнение аналогично тесту DLAB (Defense Language Aptitude Battery) Министерства обороны [23]. Вместо проверки уровня владения кандидатом каким-то конкретным языком DLAB использует вымышленный язык, что позволяет проверить его способность освоить новый язык. Этот подход, вероятно, даже более полезен в сфере технологий, поскольку новые технологии и фреймворки

появляются постоянно. Ключевые критерии теста черного ящика позволят измерить способность кандидата:

- быстро запоминать технические характеристики, команды или инструкции, применяемые в вымышленной технологии;
- использовать логику и критическое мышление для решения проблем и освоения вымышленной технологии;
- проявлять изобретательность для достижения поставленной цели с помощью искусственных барьеров, например в обход безопасности вымышленной технологии.

Вы можете найти и нанять перспективного кандидата, обладающего хорошими способностями, но не имеющего необходимых технических навыков для выполнения работы. В этом случае вам потребуется сделать дорогостоящие долгосрочные инвестиции в обучение кандидата реальным техническим навыкам. В противном случае способности кандидата никак вам не помогут.

3. **Научитесь отсекать кандидатов.** Вам нужно нечто большее, чем обычные тесты на наркотики, справки о здоровье, проверка биографии и криминальной истории и кредитные отчеты, которые рассматривают в большинстве организаций. Эти критерии не всегда дают точную картину чьего-либо характера. Лучше направить усилия на выявление кандидатов, которые часто принимают неверные решения, нанося вред себе и другим. Эти «глупые вредители» могут иметь ученые степени, сертификаты, хорошую кредитную историю, чистые тесты на наркотики и солидный опыт работы, полученный благодаря другим качествам, таким как сила духа, амбиции, трудолюбие, талант и удача. Во время собеседования исследуйте их желания и мотивацию, чтобы отсечь неподходящий вам тип людей (конечно, принятые в прошлом вредно-глупые решения могут не показывать, как мыслит кандидат сейчас и каков его характер, поэтому нужно дать ему возможность проявить себя и посмотреть на результат).
4. **Обучайте сотрудников и реализуйте культуру передового опыта.** Техническим навыкам обучиться можно, но есть и другие, более трудные для развития качества. Определите сотрудников, которые хотят стать «кибернинджя», и помогите им улучшить личные качества, описанные в «Бансэнсюкай», давая им сложные задачи и обучая их. Поручите сотрудникам:
   - ежедневно решать все более и более сложные киберпроблемы;
   - развивать ум с помощью упражнений на запоминание, а также тренировать самодисциплину и терпение с учетом используемых технологий;
   - развивать изобретательность, создавая искусственные ситуации с заданными правилами, а затем, следуя им, пытаться достичь целей.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Вы объявляете о своем желании нанять синоби и обучить их защищаться от вражеских ниндзя. Вы получаете огромное количество анкет. Вы не знаете ни одной академии, гильдии или другой организации, которые могут как-то порекомендовать кандидата, а учитывая скрытный характер профессии, не можете узнать об опыте их работы у предыдущего работодателя. Вы недостаточно хорошо понимаете, какими навыками должен обладать синоби, чтобы проверить или количественно оценить их самостоятельно, а когда просите соискателя продемонстрировать искусство синоби, он либо отказывается, либо требует оплаты.

Как определить, сможет ли тот, кто говорит, что он синоби, защитить ваш замок? Как найти и нанять высококвалифицированного кандидата без опыта синоби, если вы точно не знаете, чем занимаются эти специалисты? Как обучить талантливых кандидатов, не имея под рукой настоящего синоби?

Рекомендуемые меры безопасности и предосторожности

Далее приведены рекомендации с учетом стандартов NIST 800-53 и Cyber Workforce Framework NIST 800-16 [37]. Учитывайте их при оценке потенциальных соискателей на должности специалистов по безопасности.

1. Определите знания, навыки и умения, необходимые для выполнения обязанностей по кибербезопасности в вашей организации. Проверьте эти умения, а также критерии компетентности, навыки персонала и требования к миссии во время набора, найма и обучения сотрудников. (PM-13. Сотрудники службы безопасности.)
2. Определите требования к найму на должности «киберниндзя» путем анализа и документирования знаний в следующих областях:
   - передовые сетевые технологии и протоколы;
   - цифровая криминалистика;
   - разработка программного обеспечения;
   - соответствие;
   - защита компьютерных сетей;
   - управление конфигурацией;
   - криптография и шифрование;
   - безопасность данных;

- базы данных;
- управление идентификацией / конфиденциальность;
- управление инцидентами;
- системы промышленного контроля;
- информационное обеспечение;
- информационные системы;
- ИТ-системы и операции;
- сетевая и телекоммуникационная безопасность;
- безопасность персонала;
- физическая безопасность и безопасность окружающей среды;
- безопасность архитектуры, систем и приложений;
- управление рисками безопасности;
- веб-безопасность.

3. Рассмотрите возможность проводить обучение по следующим сертификатам и протоколам: OV-6, ANTP-*, ARCH-*, COMP-1/5/9/10, CND-*, CM-*, CR-*, DS-*, DB-*, DF-*, IM-*, IR-*, ICS-*, IA-*, WT-*, SI-*, ITOS-*, NTS-*, PS-*, PES-1, RM-*, SW-*, SAS-*.

Резюме

В этой главе мы рассмотрели качества, которые, по мнению синоби, были необходимы для достижения успеха в их ремесле. Кроме того, описали некоторые методы собеседования синоби. Мы рассмотрели процессы найма на работу, используемые современными организациями, и предположили, почему они не столь эффективны, как хотелось бы. Мы перечислили несколько новых подходов к поиску подходящих кандидатов. Упражнение, приведенное в этой главе, актуально и для сегодняшних, и для средневековых командиров, которым нужно было нанять синоби, чтобы защитить себя от вражеских ниндзя.

Наем для борьбы с киберпреступниками даже «не совсем хакера», у которого может не быть хорошего среднего балла, солидного опыта работы или неформально одетого, скорее всего, окажется эффективнее, чем наем обычного человека, пускающего пыль в глаза.

Наняв на работу талантливого и/или опытного защитника, вы должны установить стандарты и процессы, чтобы он мог защищать вашу организацию. Без руководства, которое обозначает четкие ожидания, защитники могут стать слабыми и, следовательно, бесполезными. В следующей главе мы обсудим, как киберзащитник несет службу.

24

Служба киберзащитника

Будьте бдительны даже тогда, когда врага перед вами нет.

На посту запрещается громко разговаривать,
выпивать, петь, приглашать проституток и играть
в азартные игры.
«Ёсимори хяку-сю», № 65

Трактаты синоби изобилуют подробностями о том, как пройти мимо охраны атакуемой цели. Для синоби на поле боя никакое защитное препятствие не является таким серьезным или сложным, как вражеская охрана. Трактаты инструктируют синоби работать в слепых зонах, которые охранникам сложно контролировать или защищать. При этом наиболее уязвимые места возникают не из-за плохой военной стратегии или нехватки кадров, а из-за халатности охранников и отсутствия дисциплины.

Трактаты советуют искать охранников, которые явно устали, ленивы, несобранны, не знают приемов синоби или слишком расслаблены. Существует множество способов оценить и использовать способности отдельно взятого охранника. В числе прочих методов «Бансэнсюкай» рекомендует [5]:

- шептать рядом с охранниками, чтобы проверить их внимательность, а затем наблюдать за их реакцией в течение как минимум часа, чтобы оценить их методы и реакцию;
- находить нерадивых охранников, которые действуют по сигналам скрытых охранников, например слушающих или нюхающих разведчиков, выдавая их присутствие;
- атаковать посты, где охранники громко и много разговаривают, пьянствуют и чрезмерно веселятся, — все это указывает на неопытность или небрежность;

- дождаться момента, когда охранники покинут пост, или самому организовать событие, которое заставит их сделать это.

Трактаты также советуют синоби наблюдать за поведением, движениями, позой и действиями охранников, чтобы получить больше информации об их дисциплине. Например, если ров и окружающий периметр замка содержатся в чистоте, хорошо видны и ярко освещены, то охранники, скорее всего, бдительны и ответственно относятся к защите. Но если типичные точки скрытого проникновения в замок, такие как углы, водосбросы и канализационные отверстия, не защищены, это может быть признаком того, что охранники или их командиры пренебрегают своими обязанностями [5].

Проникновение на вражеские посты позволяет синоби получить важную информацию об уровне дисциплины охранников, их поведении и способностях к самозащите. В трактатах говорится, что халатность и лень охранников — это самые большие проблемы в защите объекта, причем бремя преодоления этих пороков возлагается на командиров, чья строгая дисциплина, жесткое обучение и внимание к деталям могут воспитать в охранниках дисциплину и стойкость для защиты даже от синоби [5]. «Все решает ваш собственный разум и ваш образ мышления, — гласят стихи ниндзя. — Если вы всегда предполагаете, что враг прямо перед вами, вы никогда не ослабите бдительности» [6].

В этой главе мы сравним караульные посты времен синоби с сегодняшними центрами безопасности (SOC). Коснемся модернизации системы безопасности, в рамках которой ответственность за безопасность ложится на всех сотрудников, а не только на относящихся к службе безопасности. Мы рассмотрим способы, которыми злоумышленник может обнаружить недостаточные меры безопасности в сетях. Кроме того, представим теорию о прямом взаимодействии между сотрудниками службы безопасности и противниками, особенно если злоумышленник может проникнуть в систему тикетов SOC/IR. А также рассмотрим, как злоумышленники могут оценивать бдительность SOC.

Важнее всего будет разговор о том, почему именно работа сотрудников службы безопасности так важна, почему она может со временем ухудшаться и как довести культуру безопасности до совершенства.

Проблемы и ожидания отдела безопасности

Специалисты в сфере кибербезопасности и ИТ особенно склонны к лени, расслабленности, халатности, усталости или выгоранию на работе. Почему? Тому есть множество причин.

Самая главная причина — это треклятая человеческая натура: если никто не смотрит в монитор через плечо, многие работники просто перестают выполнять свои

обязанности. Ленивые специалисты в области кибербезопасности могут совершенно незаметно заниматься ерундой. Их задачи в основном невидимы для коллег и даже для руководителей. Многие отделы безопасности находятся за закрытыми дверями, где их сотрудники могут работать, отдыхать или даже спать, а разницы никто и не заметит. Их сети и машины существуют в отдельных VLAN или исследовательских блоках, что позволяет им свободно пользоваться интернетом без регистрации, проверок или фильтрации.

Присущая отрасли чрезмерная зависимость от процесса постепенно приводит сотрудников в состояние халатности и самоуспокоения. После многократного повторения процедур у сотрудников службы безопасности вырабатываются привычки и суженные представления о том, из чего состоит процесс защиты организации. Эта тенденция проистекает из необходимых процедур повседневной работы, и она же приводит к появлению узкоспециализированных защитников, использующих один-единственный подход и не рассматривающих методы и инструменты злоумышленников за пределами собственного повседневного опыта. Такой ограниченный образ мышления оставляет значительные бреши в системе безопасности организации.

У увлеченных сотрудников возникает противоположная проблема. Для них работа в конкурентной сфере, требующей глубоких специализированных знаний, способностей и амбиций, повышает риск выгорания. После утомительных месяцев, потраченных на поиск угроз и инцидентов, очень легко потерять концентрацию, начать полагаться на известные концепции, ожидать появления предупреждений системы безопасности или программного обеспечения или узнавать только то, что необходимо для данного конкретного инцидента, когда он уже возник.

Не только специалисты по кибербезопасности должны обладать знаниями в области компьютерной грамотности и безопасности — это касается всех сотрудников. К сожалению, это также означает, что лень и халатность нетехнических сотрудников часто даже более опасна для организации, чем злонамеренные внешние субъекты. Такие сотрудники могут непреднамеренно подвергнуть сеть или системы своей компании угрозам, неосторожно щелкнув по фишинговому сообщению электронной почты или вставив в разъем USB-накопитель, найденный на парковке. Если руководство не усиливает бдительность и дисциплину, когда это необходимо, добросовестные сотрудники будут вынуждены работать среди множества нерадивых и даже получать за это премии. Успех в такой организации превращается в игру на истощение, в которой сотрудников повышают за то, что они просто выжили дольше всех, не выгорели и не уволились. Такая среда ставит под угрозу трудовую этику, дисциплину и репутацию эффективных работников и унижает персонал, позволяя злоумышленникам использовать многочисленные дыры, оставляемые беспечными сотрудниками.

Лидерские качества и компетентность значительно повышают моральный дух и бдительность сотрудников. А неправильные решения руководства или организационные

стратегии могут ослабить безопасность и подорвать доверие сотрудников. Попытки укрепить слепые зоны или слабые места в защите обычно требуют общей работы отделов, совместного использования бюджетов, работы в выходные дни и причиняют другие неудобства, которые вызывают недовольство сотрудников и сопротивление инициативам. В результате измученные и не сумевшие ничего наладить инженеры по безопасности начинают безразлично относиться к улучшениям безопасности и закрывать глаза на существующие недостатки. Иногда они даже специально дожидаются возникновения инцидента, зная, что пассивность организации все равно не даст вносить улучшения, пока жареный петух не клюнет.

Злоумышленник может легко оценить бдительность организации по приведенным далее индикаторам.

- Слишком много информации раскрывается в сообщениях об ошибках на веб-сайтах.
- При входе в систему раскрываются детали политики паролей.
- Отсутствует содержимое заголовка политики безопасности.
- Используются неподходящие самоподписанные сертификаты.
- Неправильно настроена проверка подлинности сообщений электронной почты, создание отчетов и определение соответствия по доменному имени (Domain-Based Message Authentication, Reporting and Conformance, DMARC) либо инфраструктура политики отправителя (Sender Policy Framework, SPF).
- Неправильно настроены записи DNS.
- Раскрывается информация об интерфейсах управления на серверах с выходом в интернет, устройствах безопасности или сетевом оборудовании.
- Раскрывается информация об используемых версиях технологий или инструментах обеспечения безопасности.

Чтобы бороться со снижением бдительности, защитники должны постоянно оценивать свою работу и стремиться к ее совершенствованию. Менеджеры не всегда хвалят или награждают сотрудников, которые внедряют дополнительные меры безопасности, но поддержка высокой бдительности говорит злоумышленникам, что первая линия защиты организации серьезно укреплена, а значит, внутренняя защита может быть еще сильнее.

Регулировка поведения

Отношение сотрудников к своей работе зависит от их собственных убеждений, рабочей культуры и приобретенного ими ранее опыта. Формирование культуры

труда путем улучшения поведения и постоянной обратной связи между сотрудником и начальством поощряет сотрудников к самосовершенствованию. Отсутствие в сфере безопасности обратной связи, особенно положительной, — это самая сложная проблема, которую необходимо решить, поскольку поведение защитника может легко скатиться к апатии по отношению к безопасности. Это может быть результатом отсутствия похвалы за хорошую работу.

Часто сотрудники службы безопасности видят результаты своей работы только в виде аудитов соответствия и показателей KPI, которые не отражают полезности их действий. Результаты хорошей работы, например не дать злоумышленникам украсть у компании интеллектуальную собственность или деньги, могут проявляться через годы, таким образом, оценить их не представляется возможным. Далее приведено руководство по улучшению поведения и его поддержке в области безопасности.

1. **Установите стандарты и развивайте культуру.** Министерство обороны США занималось развитием культуры, в которой во главу угла ставится бдительность. Бывшие сотрудники Министерства обороны, которые переходят в другие организации, говорят, что испытывают шок, когда сталкиваются с пренебрежением к безопасности на новом рабочем месте (и в конечном итоге снижают свои стандарты, принимая новую культуру). Почитайте «Инициативу по культуре и соответствию в кибербезопасности» [20] Министерства обороны США и определите, какие из ее тезисов могут помочь вашей организации развить культуру бдительности в отношении безопасности. Это могут быть, например:

   - **целостность** — заставьте сотрудников сообщать обо всех ошибках, когда они случаются. Например, сотрудник, который случайно нарушает безопасность сети, не должен немедленно бежать и скрывать происшествие из-за страха потерять работу. Он должен знать, что можно без опаски признать ошибку и помочь организации заделать брешь в безопасности;
   - **конкуренция** — установите базовый образовательный стандарт для всех, кто работает в киберпространстве. Он должен определять принципы повседневного поведения сотрудников, давать людям возможность выявлять риски для безопасности и способствовать принятию разумных решений посредством непрерывного обучения в сфере кибербезопасности. Обратите внимание на то, что формирование основной компетенции может привести к тому, что не владеющие ею сотрудники лишатся возможности занимать определенные должности;
   - **профессионализм** — поддержание стандартов качества и культуры бдительности требует, чтобы сотрудники несли ответственность за свою работу и не вешали на других ярлыки;

- **вопросы, а не ответы** — нанимайте людей, которые не принимают вещи такими, какие они есть, а задают вопросы, анализируют и интерпретируют результаты наблюдений. Сотрудники чувствуют себя в безопасности, когда высказывают свое мнение, не боятся увольнения и не ощущают себя глупыми.

2. **Принуждайте к дисциплине.** Небрежность в отношении безопасности влияет не на работу одного человека или качество одного продукта, а ставит под угрозу целые организации. В «Бансэнсюкай» в «Шести пунктах о поведении охранника» написано: «Следует придерживаться строгих правил, и в случае, если кто-то не соблюдает их, его нужно строго наказать» [5]. Установите формальные процедуры для выявления и наказания нарушителей правил в области кибербезопасности и бдительности со стороны пользователей, службы безопасности, отдела ИТ и руководства. Избегайте соблазна в случае инцидента, связанного с безопасностью, делать козлом отпущения начальника службы безопасности (CISO) или других сотрудников, поскольку это не дает развивать культуру, в которой каждый чувствует себя ответственным.
3. **Установите формальные процессы, процедуры и соответствие.** Определите, задокументируйте и распространите задачи, правила и политики, которые ваш отдел безопасности должен выполнять и применять. Найдите способы проверять, соблюдают ли сотрудники эти стандарты. Избегайте использования формальных ключевых показателей эффективности (KPI), таких как количество поданных заявок или расследованных инцидентов безопасности, поскольку они не позволяют судить о работе. Назначьте руководство, которое понимает важность безопасности и заботится о ней, уделяет время повышению бдительности и выявляет несоблюдение требований.
4. **Поощряйте вовлеченность.** Сотрудники компаний часто не чувствуют себя вовлеченными в работу. Они не участвуют в принятии решений, не действуют в интересах организации и не инвестируют в успех компании (или в свой собственный). Скука — обычная проблема в сфере безопасности, которую часто можно уменьшить, устранив препятствия, которые не дают работникам внедрять упреждающие меры безопасности. Расширьте возможности сотрудников службы безопасности, позволив им:
   - экспериментировать с новыми мерами безопасности, процедурами и концепциями;
   - изучать новые технологии, методы и инструменты;
   - находить смысл в их работе;
   - получать положительные результаты, например профессионально расти или получать повышение;
   - участвовать в принятии решений о стратегических рисках;

- проводить тесты с «красной/синей командой» или другие симуляции и упражнения, чтобы учиться друг у друга;
- отмечать успехи в поиске дыр в системе безопасности.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Патрулируя замок, вы замечаете, что копья в некоторых сторожевых помещениях стоят как-то странно, и подозреваете, что некоторые из ночных стражников изобрели способ опираться на древко, чтобы расслабиться или поспать, стоя на посту. Вы не получали сообщений о спящих охранниках или о каких-то их неправомерных действиях, о недавних проблемах с безопасностью тоже не слышали.

Какие доказательства, если таковые имеются, вам нужны, чтобы принять меры по улучшению безопасности, процессов и работы персонала? Как оценить бдительность ваших охранников? Какую информацию можно запросить у охранников во время их смены, чтобы убедиться, что они не спят? Как получить от охранников честный отзыв о том, как повысить их внимательность и вовлеченность в службу? Как бы вы наказали охранника, спящего во время ночного дежурства, и как за то же самое наказать целый полк? Как внедрить культуру доверия и честности, чтобы охранники чувствовали, что они могут сообщить вам, что что-то не так, не опасаясь наказания?

Рекомендуемые меры безопасности и предосторожности

В некоторых случаях можно использовать рекомендации и меры безопасности, приведенные в стандарте NIST 800-53. Их следует оценивать с учетом рассмотренной концепции поведения на посту.

1. Разработайте и задокументируйте процедуры и правила поведения в сфере безопасности для всех сотрудников и проведите по ним обучение. Разработайте специальное обучение и процедуры для лиц, чья работа в значительной степени связана с безопасностью, таких как разработчики, отдел ИТ, отдел безопасности и руководящие должности. Применяйте строгие дисциплинарные меры за несоблюдение политик и процедур безопасности. (AT-1. Политики и процедуры осведомленности и обучения; AT-2. Обучение осведомленности; AT-3. Ролевое обучение; IR-2. Обучение реагированию на инциденты; PL-4. Правила поведения; SA-16. Обучение, проводимое разработчиками.)

2. Выполняя нагрузочное тестирование, проверяйте системы безопасности и возможности инструментов с помощью специальных оценок системы, сканирования, тестов на проникновение и «красных команд». Это позволяет выявить нарушения процессов или процедур, дыры в безопасности и оценить бдительность сотрудников. (CA-2. Оценки | (2) Специализированные оценки; CA-8. Тестирование на проникновение; IR-3. Тесты реагирования на инциденты; RA-5. Сканирование уязвимостей; SC-7. Граничная защита | (10) Тестовая эксфильтрация; СИ-4. Системный мониторинг | Тестирование инструментов и механизмов мониторинга; SI-6. Безопасность и конфиденциальность.)
3. Создавайте обучающие программы и упражнения, чтобы постоянно повышать знания, улучшать навыки и компетенции сотрудников службы безопасности. (CA-8. Тестирование на проникновение; IR-3. Тестирование реагирования на инциденты | (3) Постоянное совершенствование; PM-12. Защита от инсайдерских угроз; PM-13. Отдел безопасности и конфиденциальности; PM-14. Тестирование, обучение и мониторинг; PM-16. Программа осведомленности об угрозах.)
4. Позвольте сотрудникам службы безопасности самим определять, какие конфигурации и элементы управления нужно изменить для повышения безопасности. Возложите на владельцев систем, специалистов по сопровождению и разработчиков задачу представить убедительные и обоснованные аргументы в пользу того, почему изменения, рекомендованные сотрудниками службы безопасности, реализовать не получится. (CM-3. Управление изменениями конфигурации.)
5. Реализуйте политику и процессы рассмотрения жалоб сотрудников службы безопасности. Обратная связь помогает повысить безопасность процессов за счет пересмотра или отмены ненадлежащих элементов управления. Это также дает пользователям возможность выявлять проблемы с безопасностью и предупреждать об этом отдел безопасности, не опасаясь последствий. (PM-28. Управление жалобами.)
6. Требуйте, чтобы сотрудники службы безопасности применяли OPSEC для защиты ключевой информации о работе, конфигурации и развертывании, не раскрывая при этом OPSEC злоумышленникам, которые могут тестировать средства защиты на прочность. (SC-38. Безопасность операций.)

Резюме

В этой главе мы рассмотрели методы, с помощью которых синоби проверяли охранников и посты и оценивали возможности проникновения и то, насколько их цель соблюдает (или не соблюдает) дисциплину, обеспечивающую безопасность.

Мы увидели, что сотни лет назад, как и сегодня, охранники довольно вальяжно относились к своим обязанностям, а опытные лазутчики могли использовать эту расслабленность в своих интересах. Мы коснулись того, как корпоративная культура влияет на способность организации защищаться от угроз. В философии синоби этой концепции придавалось первостепенное значение. Затем сравнивали культуру синоби с культурой современных отделов безопасности, где есть проблемы, которыми, вероятно, могут воспользоваться современные киберпреступники. Мы также описали несколько методов и передовых практик создания и поддержания качественной культуры безопасности.

В следующей главе мы обсудим реализуемый синоби принцип «опасный незнакомец», который требует не подпускать никого подозрительного. Если считать его частью культуры безопасности, а также реализовывать строгие меры контроля, чтобы подозрительные события не превратились в атаку, организация может достичь серьезного уровня безопасности.

25

Борьба с угрозами с помощью недоверия

Если вы входите в дом с черного входа, вас не сочтут злоумышленником. Дело в том, что те, кто приходит с тыла, не считаются ворами или нападавшими.

Никогда не позволяйте посторонним приближаться
к посту, даже если это ваш родственник.

«Ёсимори хяку-сю», № 93

В феодальной Японии странствующие торговцы, монахи, священники, актеры, попрошайки и прочие праздношатающиеся часто работали в разбитом военном лагере, замке или подобном месте, поскольку солдаты регулярно пользовались их услугами [5]. Неудивительно, что такие чужаки часто были засланными агентами, которым платили за сбор информации для врага. Некоторые из них — это замаскированные синоби, которые пользовались близостью замка, чтобы изучить или поразить цель, собрать разведданные, а может, даже проникнуть в лагерь или атаковать его [5].

«Бансэнсюкай» описывает, как командование может бороться с такими угрозами. Самый эффективный подход — запретить подозрительную деятельность и дружеские отношения вблизи лагеря. Эту политику надлежит «строго довести до всеобщего сведения путем многократного повторения», и трактат предупреждает, что никого, кто выглядит подозрительным, никогда нельзя допускать в замок или лагерь, чтобы не рисковать, что подозрительная деятельность превратится в беду [5]. Обученные и дисциплинированные солдаты позволяли находиться в лагере только проверенным торговцам, а ненадежным в защищенную зону хода не было. Синоби во время операции придерживались этой философии в более широком смысле: не доверяй никому, кого не знаешь. «Бансэнсюкай» рекомендует синоби помогать

надежным торговцам защищать их хижины и лавки от огня, будь то случайность или поджог, чтобы снизить риск распространения огня с них на лагерь [5].

В этой главе мы рассмотрим режим «блокировать только угрозы», который может превратиться в бесконечную погоню за новыми доменами, IP-адресами, URL-адресами и файлами, считающимися вредоносными. Мы рассмотрим причины, по которым многие организации (и сфера безопасности в целом) предпочитают гоняться за нескончаемым потоком угроз, а не работать в режиме «блокировать все подозрительное». Мы также опишем стратегии и рекомендации для преодоления технических трудностей этого подхода. Кроме того, в упражнении по теории за́мка исследуем способы, которыми те, кто там служит, может попытаться обойти блокировку всего подозрительного.

Возможность угрозы

Что касается кибербезопасности, представьте, что лагерь — это ваша организация, а продавцы, актеры и все остальные люди за пределами периметра — это сервисы и приложения, доступные в интернете. Все законные соединения с внешними сайтами, которые помогают вашим сотрудникам выполнять их работу, не говоря уже о новостях, социальных сетях и развлекательных сайтах, которые они листают во время перерывов, позволяют подозрительным объектам подключаться к организации и работать под видом обычных бизнес-задач. Злоумышленникам, которым требуется начальный доступ, доставка и эксплуатация, часто нужно, чтобы внешние связи оставались незамеченными, непроверенными и неотфильтрованными. Дальнейшая тактика заключается в компрометации соединений с сайтами, которые посещают ваши сотрудники, отправке фишинговых писем со ссылками или вложениями, сканировании сети с ненадежных адресов и использовании C2 для сбора информации и отправки инструкций имплантатам на зараженных машинах (и это лишь малая часть списка).

Для борьбы с этими атаками отрасль кибербезопасности установила функциональные средства управления безопасностью, политики и системы, которые заносят в белый список известных и надежных партнеров и другие проверенные сторонние бизнес-структуры. Организации могут создавать белые списки доменных имен, IP-секторов, серверов имен, адресов электронной почты, веб-сайтов и центров сертификации, чтобы сотрудники могли общаться только с доверенными партнерами и наоборот. При наличии строгого белого списка злоумышленники должны сначала потратить силы на атаку доверенных партнеров, чтобы затем взломать целевую организацию.

Но даже если технические проблемы решены, человеческий фактор остается. Для человека вполне естественно искать стимулы во внешних отношениях, а также

в развлечениях и новостях. Следовательно, внедрение политики блокирования подозрительного может оказаться сложной задачей для руководства, поскольку она способна привести к значительным культурным и поведенческим изменениям во всей организации.

Для примера предположим, что вы заметили, что большая часть интернет-трафика вашей организации уходит на просмотр видео на развлекательных сайтах. Очевидно, эта деятельность не соответствует ничьим должностным обязанностям, и вы решаете заблокировать доступ ко всем крупным развлекательным сайтам с помощью средств обнаружения уровня 7.

Хоть эта мера и соответствует потребностям вашего бизнеса, а может, даже задокументирована в ИТ-политике, многие организации, внедрившие подобные меры, сожалеют об этом. Сотрудники, скорее всего, будут жаловаться на вас или оказывать социальное давление, вынуждая разблокировать запрещенный трафик, а некоторые наверняка попытаются обойти запрет с помощью технологии шифрования или туннелирования, прокси-серверов или посещения развлекательных сайтов, которые содержат похожий контент, но не фильтруются, из-за чего ваша сеть и системы подвергаются еще большему риску.

Одно из популярных решений — это организация некоммерческого интернета или сети из персональных устройств (bring your own device, BYOD), в которой сотрудники могут смотреть видео с личных устройств. Вы даже можете настроить отдельные машины, на которых сотрудники могли бы заниматься личными делами в интернете во время перерывов. Министерство обороны США использует этот подход, предоставляя сотрудникам выделенную систему для неконфиденциального доступа в интернет (NIPRnet). Охрана сети физически и логически отделяет эту систему для целей управления информационными потоками [33]. Министерство обороны также вносит в белый список все известные невредоносные интернет-ресурсы и отклоняет большие IP-блоки и ASN, которые считает подозрительными или хотя бы ненужными.

За последние десять с лишним лет организации многократно подвергались атакам с известных вредоносных IP-адресов, доменов и URL-адресов, поэтому их блокирование (занесение в черный список) выполнить довольно просто. Блокировка всего *подозрительного* не дает неизвестному вредоносному трафику попасть в сеть, но ее значительно труднее организовать, и часто по уважительным причинам. Создание белого списка всех известных безопасных интернет-ресурсов, сайтов и IP-адресов, которые будут нужны вашим сотрудникам, может оказаться чрезвычайно трудной задачей. В этой области Министерство обороны является идеальным практиком, поскольку оно активно устанавливает политики блокирования и предотвращения этих сценариев угроз. Министерство также постоянно напоминает персоналу об этих политиках с помощью плакатов, обязательного обучения, условий использования

и предупреждений в системах. Обходить политики или меры контроля запрещается, поскольку это может поставить под угрозу безопасность сети, системы и данных.

Блокировка подозрительного

«Опасный незнакомец» — это простая концепция, которую многие дети усваивают в раннем возрасте. Потенциальные угрозы для ребенка часто предотвращаются за счет того, что он не допускает приближения посторонних. «Опасный незнакомец» — это не идеальная стратегия, но она может быть эффективной, если предположить, что любые известные сущности (незнакомцы) проверены и признаны заслуживающими доверия. Преимущество этой стратегии заключается в том, что в ней реакция на угрозу, ранее признанную подозрительной, не зависит от дополнительных уровней безопасности. Поскольку дети и многие организации оказываются беззащитными, если злонамеренной угрозе разрешается взаимодействовать с ними, применение политики безопасности «блокировать все подозрительное» может оказаться первой и единственной защитой, которая у них вообще будет. Далее приведено руководство по применению этих концепций в вашей среде.

1. **Практикуйте идентификацию, бдительность и понимание.** Все заинтересованные стороны должны понять, что подозрительные сайты необходимо блокировать. Для начала вы можете проверить соединение или запрос на внешний DNS-сервер в Иране, Северной Корее (175.45.178.129) или сервер другой известной, но маловероятной для вашей организации угрозы. Если получаете положительный ответ, значит, ваша сеть позволила вам общаться с подозрительной системой без уважительной на то причины. Эта методика обычно работает. Организации чаще блокируют «злонамеренные», а не подозрительные ресурсы, и если в этих странах нет известных IP-адресов, на которых размещалось вредоносное ПО или с которых проводились атаки, в черных списках этих адресов нет.

   Теперь, когда вы знаете, что какой-то ресурс должен быть заблокирован, ваша организация может заблокировать его IP-адрес или, возможно, сетевой блок, которому он принадлежит, если отдел безопасности внесет нужные изменения. Но обратите внимание: в этом случае придется оценить и заблокировать более 14,3 млн подсетей IPv4/24, и у вашей организации может не хватить времени, желания или возможностей для создания списка всех подозрительных ресурсов. Лучше составить белый список, который, даже если приведет к ложным срабатываниям, одновременно станет блокировать вредоносные и подозрительные программы.

2. **Создайте центр обмена информацией и анализа (ISAC).** Облегчите задачу создания белого списка для организации, создав ISAC для обмена с другими

компаниями, работающими в той же отрасли, информацией о доверенных сайтах, IP-адресах и доменах, которые используют их сотрудники в своей работе. У компании, которая разрабатывает систему профилирования, есть возможность формировать белые списки в интернете. Другие компании могут применять эти списки для ограничения количества обнаруживаемых подозрительных сайтов, что упрощает создание и обслуживание безопасных сетей.

3. **Ищите взаимную защиту.** Проводите взаимное сканирование уязвимостей и объединение доверенных организаций, с которыми ваша организация ведет бизнес. Этот подход согласуется с рекомендациями «Бансэнсюкай», который советует защищать лавки надежных торговцев от огня для взаимной защиты. Реализуйте эту меру для организаций, которые входят в надежную экстрасеть, создают прямые соединения или используют другие технологии прямого туннелирования, которые обходят обычные меры безопасности.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Вы замечаете, что у стен замка становятся на привал, слоняются и занимаются своими делами разные незнакомцы. Вы не узнаёте многих из них, и ваши охранники жалуются, что их присутствие не только отвлекает, но и затрудняет выявление потенциальных вражеских агентов, действующих рядом с замком. Вы запрещаете разбивать какие-либо палатки рядом с замком и создаете большой чистый периметр, но после этого командиры сообщают, что солдаты чувствуют себя словно в изоляции. Кроме того, в надежде обойти запрет торговцы приходят к замку ночью и тайком продают товары вашим воинам в условленных тайных местах. Случается, солдаты выходят из замка после комендантского часа, а неизвестные люди украдкой подходят к замку.

Как вы можете отрегулировать свой запрет, чтобы предотвратить ночные контакты? Какие дополнительные приемы или наказания вы могли бы применить, чтобы политика «блокировать подозрительное» соблюдалась строже, но не наносила вреда вашей организации? Как можно позволить незнакомцам приближаться к замку, но не дать возможности вражеским синоби тайно проникнуть в него или атаковать?

Рекомендуемые меры безопасности и предосторожности

В некоторых случаях можно использовать рекомендации и меры безопасности, приведенные в стандарте NIST 800-53. Их следует оценивать с учетом концепции блокировки подозрительных объектов.

1. Внедрите политику применения собственного устройства (BYOD), чтобы пользователи могли выйти в интернет по нерабочим причинам, или предоставьте сотрудникам отдельную рабочую станцию для внешних подключений к сети. (CA-3. Системные соединения | (1) Несекретные соединения системы национальной безопасности; SC-7. Граничная защита | (1) Физически разделенные подсети.)
2. Создайте для входящих и исходящих подключений белые списки, запрещающие все, за исключением задокументированных исключений. (CA-3. Системные соединения | (4) Подключение к общественным сетям | (5) Ограничения на подключения к внешней системе; SC-7. Граничная защита | (5) Запрет по умолчанию, разрешение по исключению.)
3. Обменивайтесь информацией с похожими организациями, чтобы создать главный белый список. (PA-4. Обмен информацией с внешними сторонами.)

Резюме

В этой главе мы рассмотрели, как командиры укреплений синоби вводили особую политику безопасности, которая значительно усложняла работу вражеских синоби. Также мы обсудили, сложно ли современным организациям вводить такие стратегии, а также привели примеры проблем, которые организациям приходилось преодолевать, чтобы внедрить аналогичный подход к сетевой безопасности. Мы рассмотрели несколько идей, как применять концепцию «блокировать подозрительное» на практике.

В следующей главе мы объединим концепции, которые почерпнули из предыдущих глав, и применим их к анализу угроз. Последняя глава станет венцом всей книги и объединит все, что вы узнали о синоби, с реальными киберугрозами, рассмотренными в предыдущих главах.

26

Мастерство синоби

Секретные методы проникновения требуют хитрости, они разнообразны и гибки и реализуются в зависимости от имеющихся возможностей. Таким образом, за основу вы должны взять старые методики синоби, служивших под началом великих древних генералов, но помните, что нужно не только придерживаться их методик, но и адаптировать их под текущую ситуацию и момент.

Даже если снаружи шумно, помните, что пост
нельзя оставлять без присмотра. Вы должны
прислушиваться к любым звукам.
«Ёсимори хяку-сю», № 66

Синоби иногда нанимали для охраны замков и других укреплений, как описано в «Сёнинки» [7], но чаще всего на постах в феодальной Японии стояли обычные солдаты или наемники, не являющиеся синоби и обученные лишь борьбе с обычными проблемами. Но «Бансэнсюкай» и «Гумпо дзиёсю» советуют командирам для защиты от синоби нанимать своих синоби, поскольку они могут обучить обычных охранников распознавать секретные тактики и приемы синоби (ТТП) [6]. Многие приемы были описаны в трактатах, но они постоянно развивались и совершенствовались, и у разных кланов были свои секретные техники, о которых не знали другие синоби.

Тактики и приемы синоби были продуманными и часто решали сразу несколько задач. Например, синоби мог воткнуть обычный зонт в землю и открыть его на виду у охранников замка. Он мог что-то спрятать от охранников под зонтом, вдобавок любая активность поблизости могла отвлечь охранника от наблюдения [5]. В этом методе также использовалось распространенное суеверие того времени, что забытые или потерянные зонтики становились одержимыми и преследовали своего предыдущего владельца. Это явление называют *цукумогами*, *каса-обаке*, а также *ёкай* [15].

Синоби, нанятые для обучения охранников, сталкивались с педагогической проблемой: им категорически запрещалось записывать свои ТТП или делиться ими с посторонними, поскольку это могло поставить под угрозу секретность навыка и подвергнуть опасности жизни других синоби. Иногда в трактатах даже советовали синоби убить любого наблюдателя или жертву, которые видели тактику или прием [5].

Таким образом, вместо того чтобы рассказывать о конкретных техниках, синоби подчеркивали необходимость правильного мышления, бдительности и тщательного анализа обстановки, необходимых для поимки синоби [6]. Напряжение ума усиливалось оценкой рисков в лагере, знанием врага и видением наиболее вероятных и действенных сценариев угроз, которые может реализовать противник. Скорее всего, синоби действительно давали охранникам общее представление о том, на что способны другие синоби, и приводили примеры различных сценариев угроз, но описывали их таким образом, чтобы не слишком раскрывать профессиональные секреты [5]. Они учили охранников находить признаки присутствия синоби (видимые, слышимые и другие наблюдаемые объекты, на которые стоит обратить внимание, стоя на посту) и определяли правила, позволяющие избежать ошибок.

Из-за огромного многообразия техник, которые нужно было изучить, а также из-за того, что многим охранникам не хватало формального образования, синоби передавали знания через стихи, чтобы информацию было легче запомнить. (Этим объясняется большое количество стихов о работе охранников в «100 стихотворениях ниндзя». Они предназначались не для самих синоби, а скорее для обучения охранников.) К тому же стихи содержали достаточно подробностей, чтобы описать тактику синоби и дать понять, как с ней бороться, но не настолько, чтобы перегружать стражников информацией. Например, стихотворение № 66, цитируемое в начале этой главы, дает простой совет: не оставляйте свой пост и прислушивайтесь к любым звукам, включая шум, который привлек ваше внимание, особенно шаги, приближающиеся сзади [6]. Стихи были сгруппированы по темам. Стихи № 64–67, 78, 79, 91, 93 и 94 рассказывают о том, как сохранять бдительность и избегать грубых оплошностей. В них описывается, как нести дежурство ночью, когда одолевает усталость, в каком направлении смотреть и почему пить, петь и вызывать проституток на дежурстве — плохая идея.

Конечно, если вражеский синоби замечал, что охранники хорошо распознают его тактики, то он применял контрмеры. Яркий пример, который появляется во всех трех основных трактатах, описывает ситуацию, когда синоби прячется в кустах или высокой траве либо ползет по полю. Действия синоби беспокоят насекомых, которые замолкают, чтобы спрятаться. Для обученного охранника отсутствие гудения, жужжания или щебетания указывает на скрытное приближение человека. Обычно, если охранник внезапно настораживается и начинает искать незваного гостя и синоби знает, что его разоблачили, он тихо уходит [5]. Вот здесь и вступает в действие контрмера. Перед следующей попыткой проникновения синоби посадит

в коробку несколько сверчков. Насекомые при этом спокойны, они стрекочут, заполняя тишину вокруг синоби, приближающегося к посту охраны. У охранников не будет причин подозревать приближение опасности [22].

Стихотворение № 68 наглядно иллюстрирует проблемы обнаружения тактик синоби и противодействия им: «Вам следует провести тщательный осмотр охраняемой области, следуя за отрядом ночного патруля. Это называется *камарицуке* (обнаружение засады)» [6]. Ночью командир для патрулирования периметра отправлял основной поисковый отряд с обычными фонарями и другими приспособлениями, а вслед за ним — тайный поисковый отряд [5]. Синоби давал охранникам команду осмотреть периметр на предмет всего, что привлекает внимание, особенно звуков, движения и людей [6]. Конечно, вражеский синоби об этом знал. Трактаты описывают, как атакующие синоби могли прятаться в кустах, канавах или других темных местах, дожидаясь, пока патруль уйдет, а затем продолжить работу [5]. Однако в некоторых случаях противник может следовать за патрульной группой, маскируя собственные движения исходящим от нее звуком и светом, и даже атаковать патруль сзади [6]. Таким образом, наличие второго, скрытого патруля позади первого поможет поймать спрятавшихся вражеских синоби. Эта группа хорошо вооруженных воинов обыскивала вероятные укрытия и оставалась начеку, не пропуская врага, который мог следовать за основной группой [5]. Однако синоби, знакомый с техникой *камарицуке*, может подождать в тени, пропустить вперед второй, тайный патруль или переместиться в то место, которое этот патруль не будет обыскивать. Для борьбы с этим (это уже контр-контр-контрмера) были добавлены стихи № 69 и 70 [6]:

- 69: «После проведения ночного патрулирования важно проводить камарицуке еще раз, а потом еще раз».
- 70: «При выполнении камарицуке нужно проводить несколько патрулей через определенные промежутки времени, чтобы найти вражеских агентов синоби».

Это руководство поощряло проводить *камарицуке* с непостоянной частотой, чтобы помешать противнику действовать свободно. Частые и частично непредсказуемые патрули с одним или несколькими *камарицуке* оставляли вражеским синоби мало возможностей для работы с укреплениями или патрульными группами защитников [6].

Оптимальный подход с обнаружением ТТП синоби и контрмерами может привести к стычке и в конечном итоге становится слишком опасным или непрактичным для проведения атаки. Такой результат часто является лучшим вариантом, на который можно рассчитывать в борьбе с вражеским синоби.

В этой главе мы обсудим, как философия, лежащая в основе мастерства синоби, применима к пониманию ТТП субъектов киберугроз. Коснемся того, как разведка

киберугроз может направлять группу реагирования, инженеров по безопасности и охотников за угрозами на защиту своей организации аналогично тому, как синоби могли повысить эффективность обычных охранников замка и солдат с помощью разведки. Мы исследуем некоторые часто используемые для описания ТТП киберугроз фреймворки. Их сочетание со знаниями синоби упрощает понимание угроз и того, почему ТТП полезны. Поговорим о том, почему точные процедуры, реализуемые злоумышленниками, часто остаются загадкой и, вероятно, будут таковыми всегда, а также рассмотрим процедуры, которые рациональный противник выполнил бы, зная, как работали синоби. Наконец, мы дадим рекомендации, как включить аналитику киберугроз в стратегию защиты вашей организации, и коснемся того, почему это может быть очень сложно.

Техники, тактика и процедуры

В кибербезопасности ТТП описывают подходы к анализу моделей поведения, действий и методов конкретного субъекта угрозы или группы. *Тактика* описывает маневры противника, такие как разведка, боковое движение и развертывание бэкдоров. *Техники* — это конкретные технические методы, которые противник применяет для решения задач, такие как использование определенного инструмента или программного обеспечения для создания оружия или его эксплуатации. *Процедуры* подробно описывают стандартные правила и последовательности действий, которые необходимо выполнить, например: предварительная проверка того, что в эксплуатируемой целевой системе есть активные пользователи, запуск вредоносного ПО с помощью анализа строк на предмет ошибок перед развертыванием, реализация профилактической самоочистки после проверки подключения к целевому устройству.

Когда ТТП определены, защитники могут начать искать их индикаторы в своей среде. Они способны даже предсказать, какие именно ТТП могут быть использованы против них для поддержки планирования и реализации упреждающих контрмер. Чтобы распознать и систематизировать ТТП киберпреступников, отрасль кибербезопасности разработала несколько концепций, моделей, анализов и методов совместного использования, включая следующие:

- пирамида боли [39];
- фреймворк ATT&CK™ [11];
- модель жизненного цикла атаки [9];
- фреймворк Cyber Kill Chain [47];
- алмазная модель анализа вторжений [16];
- STIX (выражение структурированной информации об угрозах) [41].

Пирамида боли

Пирамида боли (рис. 26.1) — это отличная модель для визуализации того, как осведомленность об индикаторах, инструментах и ТТП злоумышленника может повлиять на уровень безопасности защитника.

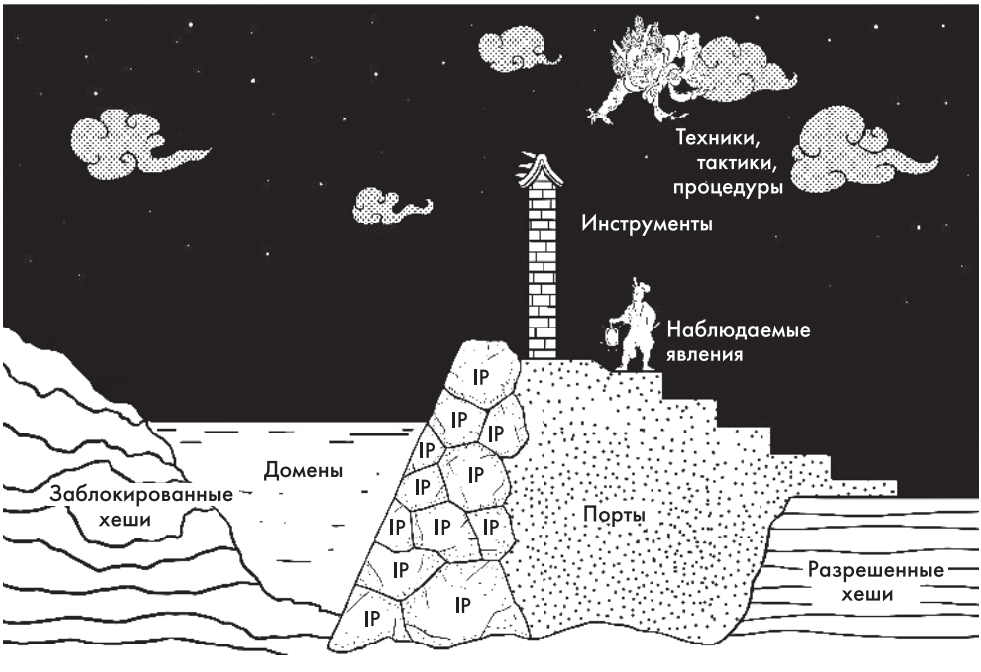

Рис. 26.1. Укрепление индикаторов компрометации
(из книги Дэвида Бьянко «Пирамида боли» [19])

Суть названия «пирамида боли» в том, что не существует способа гарантировать абсолютную безопасность или предотвратить все атаки, но злоумышленник с меньшей вероятностью нападет на вашу организацию, если затраты времени, сил и ресурсов на атаку окажутся для него слишком велики.

В нижней части пирамиды находятся индикаторы компрометации (indicators of compromise, IoC) — домены, IP-адреса, хеши файлов и URL-адреса, которые позволяют точно идентифицировать известные вредоносные индикаторы. Защитники могут блокировать эти индикаторы или предупреждать о них, но противник способен их изменять.

На уровень выше атомарных индикаторов расположены индикаторы хоста, такие как ключи реестра, остаточные файлы и артефакты. Можно обнаружить их или

отреагировать на них, но обнаружение или устранение угроз может не быть автоматическим, и противник может изменять используемые индикаторы в зависимости от цели.

Следующий уровень — это инструменты, а именно программное обеспечение или устройства, с помощью которых противник проводит наступательные действия. Защитники могут обнаружить поиск, запретить доступ или отключить функции известных вредоносных инструментов в среде и тем предотвратить работу злоумышленника.

На вершине пирамиды находятся тактика, техники и процедуры противника. Если вы можете выявить эти методы или смягчить последствия их применения, противнику станет сложно создавать или осваивать направленные против вас новые ТТП, хотя, конечно, вам как защитнику тоже будет сложно разрабатывать меры защиты или противодействия.

Фреймворк ATT&CK

Фреймворк MITRE's Adversarial Tactics, Techniques, and Common Knowledge (структура тактики, техники и общих знаний, сокращенно ATT&CK) заимствует многие тактики из структуры Cyber Kill Chain от Lockheed Martin (рис. 26.2). Структура Cyber Kill Chain описывает семь этапов жизненного цикла атаки: разведка, вооружение, доставка, эксплуатация, установка, управление и контроль, действия над целью. Каждая тактика, определенная в структуре ATT&CK, содержит список техник и методов с примерами, которые можно обнаруживать и которым можно противодействовать.

Обратите внимание на то, что слово «процедуры» в структуре ATT&CK отсутствует. Это понятно, поскольку для их выявления, вероятно, потребуется украсть и проанализировать журнал наступательных кибероперации у государства или вооруженных сил. Поэтому в «Бансэнсюкай», «Нимпидэн» и «Сёнинки» описывается работа атакующей группы шпионажа, от чего обсуждение становится богаче.

Аналитика угроз

Если ваша группа безопасности понимает эти тактики и методы, определила плоскости атаки, оценила имеющиеся средства управления безопасностью и проанализировала предыдущие инциденты, оценив защитную эффективность организации, то вы можете начать прогнозировать, в какой точке злоумышленники смогут атаковать ваше окружение. Имея на руках хороший набор прогнозов угроз, вы можете начать поиск угроз, а именно индикаторов и свидетельств, оставшихся после атаки. Тем не менее без глубокого понимания того, как именно действуют злоумышленники, трудно эффективно выследить их или обнаружить их присутствие.

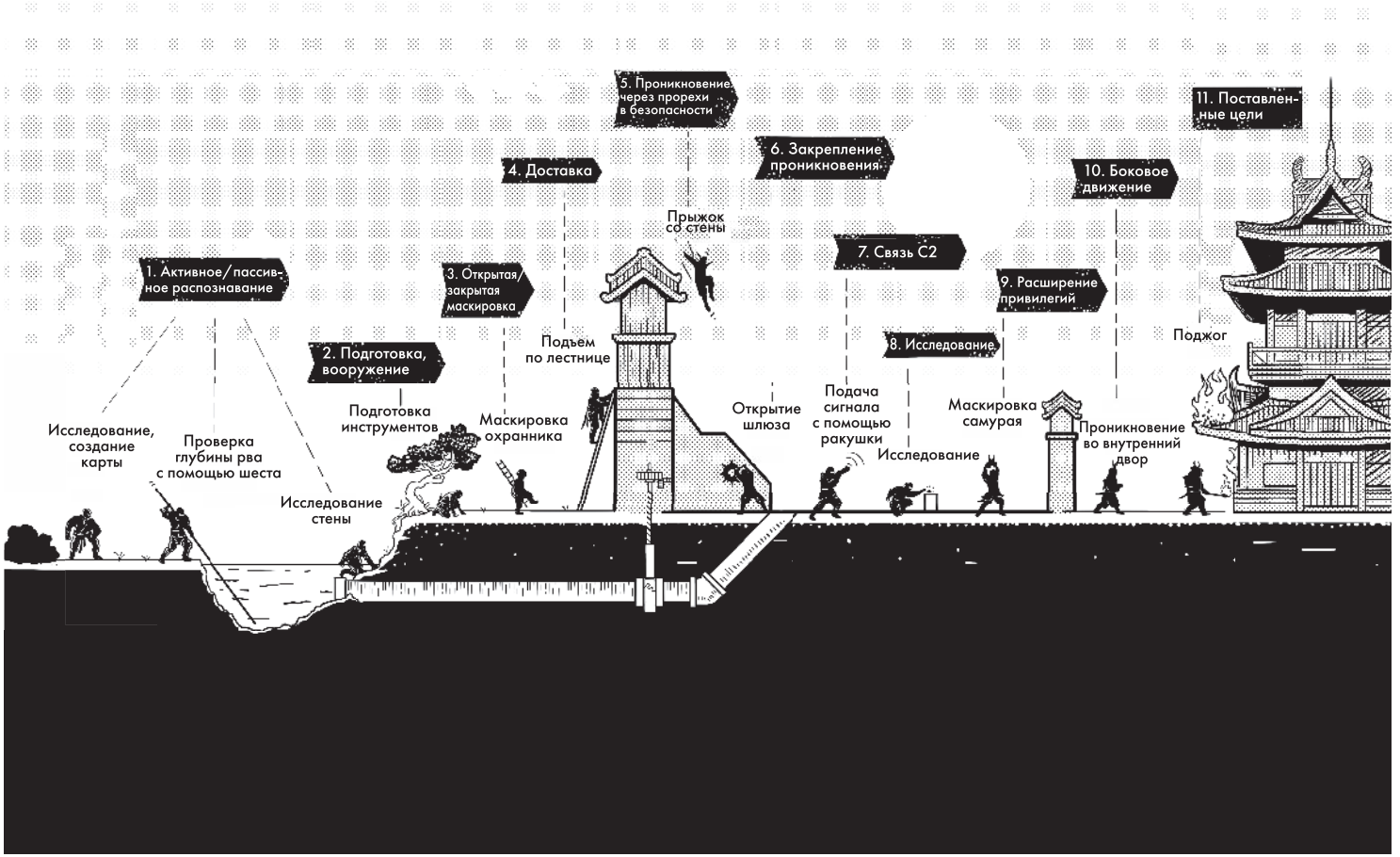

Рис. 26.2. Цепочка атак ниндзя (применительно к MITRE's ATT&CK [2])

Именно здесь полезной становится аналитика угроз. *Разведка угроз* не обязательно означает просмотр списков новых IP-адресов, доменов, URL-адресов и хешей файлов, связанных с вредоносным ПО, хакерской инфраструктурой или группами угроз. Разведка киберугроз (*cyber threat intelligence, CTI*) скорее похожа на традиционную разведку — анализ киберугроз, вредоносного ПО, хакерских атак, государств, преступников, DDoS-атак и многого другого. При правильном использовании CTI предоставляет полезную информацию и оценку того, что угроза делает, каковы ее мотивации и ТТП. Проще говоря, CTI — это один из лучших способов понять угрозы и эффективно защититься от них, поскольку в этом случае лица, принимающие решения, должны искать информацию и предпринимать защитные действия.

К сожалению, многие пользователи CTI обращают внимание только на IoC, поскольку их легко задействовать в SIEM, межсетевых экранах и других устройствах безопасности для блокировки угроз. Такой подход отрицает реальную ценность CTI, поскольку подробные наблюдения и оценки аналитиков CTI описывают поведение, шаблоны, методы, атрибуцию и контекст. Хотя производители CTI не всегда раскрывают, как они собирают информацию об угрозе, они часто стремятся давать прозрачные оценки того, как и почему угроза приводит к определенным действиям.

Конечно, использование отчетов разведки для понимания угроз приведет к тому, что вы однажды поймете: от вашей среды многое требуется. Для реализации этого процесса нужен большой набор навыков, включая способность быстро учиться и принимать стратегические решения. Но если потребитель CTI сумеет найти время на разбор каждого шага, кода, тактики и техники угрозы, он сможет принять решения, которые позволят ему успешно смягчать угрозы, обнаруживать их, реагировать на них и даже предсказать их будущие действия.

Разведка киберугроз

Уже купив десятки готовых решений по безопасности и наняв штатных сотрудников службы безопасности для обработки многочисленных векторов угроз, компании иногда рассматривают расходы на CTI как окончание значительного финансирования модели безопасности. Но CTI может позволить вам улучшить стратегии безопасности и повысить эффективность всех других уровней безопасности, и затраты будут оправданны. К сожалению, часто эффективное использование CTI сводится к чтению отчетов о новейших научных открытиях в данной области, но для этого требуется, чтобы вы понимали значение этих открытий и подстраивали под них свою культуру, бизнес-стратегии и технологии. Это возможно, но в то же время интенсивность потребления, синтеза и действия кажется чрезмерной. В этом и заключается самая большая проблема CTI — это не хрустальный шар, который дает простые и понятные ответы. Ознакомьтесь с приведенным далее руководством, чтобы принять правильное решение по вашей программе CTI.

1. **Развивайте разведку киберугроз и охоту за ними.** Рассмотрите возможность оформления подписки на бесплатные или платные отчеты CTI. Кроме того, вы можете начать разработку собственной внутренней CTI, собрав данные об угрозах для вашего окружения, существующих в данный момент. Создайте команду CTI, которая будет собирать и анализировать результаты и сообщать о них заинтересованным сторонам в сфере ИТ, безопасности и бизнеса. Эти стороны должны понимать, кто атакует организацию, как было осуществлено проникновение, что злоумышленник собирается делать в сети, каковы его предполагаемые цели и как их планируется достичь. Внедрите в свои информационные системы стратегические и оперативные меры безопасности, меры смягчения последствий и контрмеры, чтобы защитить себя от конкретных тактик.

   Обучите сотрудников службы безопасности и разведки находить угрозы. Поскольку не всякую угрозу можно структурировать или заблокировать, специальная группа поиска должна постоянно искать следы угроз в вашей сети, руководствуясь данными вашего партнера CTI, поставщика или команды. Охоту за угрозами можно дополнять тренировками «фиолетовой команды», когда «красная команда» выполняет враждебные действия в вашей сети, а «синяя команда» пытается их выследить, попутно разбираясь в том, как противостоять угрозе.

2. **Используйте CTI.** Проведите тренировку с ИТ-отделом и службами безопасности для моделирования TTП угроз и оценки реакции на них. Предположим, вам стало известно, что некая фишинговая компания собирается атаковать организации вроде вашей посредством сервиса коротких ссылок Google (http://goo.gl/). Вы не можете просто взять и заблокировать IP-адреса, URL-адреса или домен Google, не нарушая работу бизнеса, ведь многие сотрудники организаций используют сервис коротких ссылок по вполне нормальным причинам. Ваш CTI говорит, что злоумышленник, вероятно, применяет ссылку goo.gl, потому что ваше антивирусное программное обеспечение, прокси-сервер или фишинговый протокол не считают ее вредоносной. Системы безопасности говорят, что Google находится в белом списке.

   В первую очередь нужно найти доказательства наличия этой ссылки в поступающих к вам электронных письмах. Многие организации сталкиваются с такой проблемой на заре своей работы, поскольку их почтовый администратор либо не хочет предпринимать меры для поиска соответствующих гиперссылок, либо не имеет необходимого доступа или ресурсов для просмотра входящей электронной почты. Дополнительно злоумышленнику может помешать карантин потенциальных фишинговых атак, информирование о наличии угрозы для сотрудников, не связанных с ИТ и безопасностью, и их обучение тому, как обнаруживать угрозы и избегать их.

Подобно тому как злоумышленник использует различные инструменты, тактики и методы для атаки на организацию, ваши собственные инструменты тоже должны строиться на понимании, изобретательности и инженерии, чтобы эффективно блокировать угрозы и реагировать на них. Конечно, ваш администратор электронной почты может создать правило для обнаружения сокращенной ссылки goo.gl, но как насчет других? Стоит надеяться, что ваша команда CTI определит угрозу фишинга с помощью ссылок и сокращенных ссылок и порекомендует методы их обнаружения, блокирования или смягчения угроз от них. Кроме того, команда должна информировать сотрудников вашей организации о самом существовании такой тактики. Сотрудники в этом случае должны обращать внимание не только на goo.gl, но и на все короткие ссылки. Наконец, лица, принимающие решения, должны стратегически противостоять этой угрозе с помощью новой архитектуры, политик или мер контроля.

Реализация этого процесса, каким бы болезненным он ни был, необходима для того, чтобы определить, где в вашей организации необходимо улучшить меры обнаружения угроз, реагирования на них и смягчения их последствий.

УПРАЖНЕНИЕ ПО ТЕОРИИ ЗА́МКА

Допустим, вы — правитель средневекового замка, в котором хранятся ценности. Вам стало известно, что ваш протокол безопасности, согласно которому охранники должны расценивать внезапную тишину как присутствие злоумышленника, удалось обойти синоби, который использовал коробку со сверчками. Сверчки в коробке синоби вводят охранников в заблуждение, заставляя их думать, что все в порядке.

Подумайте, как вы могли бы научить своих охранников распознавать обман, когда и тишина, и шум могут указывать на присутствие злоумышленника-синоби. Какие методы охоты или наблюдения могут помочь охранникам обнаруживать приближающихся лазутчиков? Как бы вы могли определить наличие коробки со сверчками или принять меры против них? Наконец, как вражеские синоби могут отреагировать на ваши новые контрмеры и меры безопасности?

Рекомендуемые меры безопасности и предосторожности

Приведенные далее рекомендации составлены в соответствии со стандартом NIST 800-53 и должны оцениваться с учетом понимания безопасности, TTП и CTI.

1. Проведите обучение по вопросам безопасности для всех сотрудников вашей организации, чтобы помочь им понять, как быстро реагировать на угрозы. (AT-2. Обучение по вопросам безопасности; PM-13. Отдел информационной безопасности.)
2. Создайте команду для анализа угроз, инцидентов, разведданных и TTП противника, а также разработки контрмер и мер безопасности для борьбы с угрозами. (IR-10. Группа комплексного анализа информационной безопасности.)
3. Сотрудничайте с внешними группами безопасности и организациями, обменивайтесь с ними информацией об угрозах, относящихся к вашей организации. (PM-15. Общение с группами безопасности и компаниями.)
4. Внедрите программу осведомленности об угрозах, которая содержит подробную информацию об угрозах, способах их смягчения и индикаторах атаки. (PM-16. Программа осведомленности об угрозах.)
5. Используйте достоверную информацию об угрозах для их поиска, мониторинга активности, поведения, шаблонов и других наблюдаемых признаков, указывающих на угрозу. (SI-4. Мониторинг информационной системы.)

Резюме

В этой главе мы рассмотрели несколько TTП синоби, в частности тактику *камарицуке* и ее развитие с точки зрения атакующего и защитника. Изучили и другие тактики киберугроз, которые тоже могут развиваться, по мере того как каждая сторона пытается обойти другую, пока не появляется надежная мера безопасности. Мы обсудили разведку киберугроз и то, почему недостаточно просто знать, что делает злоумышленник, как он это делает и что собирается предпринять. Для получения максимальной пользы CTI следует задействовать с прицелом на то, чтобы каким-то образом устранить угрозу. В упражнении по теории за́мка мы рассмотрели наглядный пример того, как защитники получают новые данные, а затем меняют свою тактику реализации данной угрозы. Это мысленное упражнение можно сравнить с системами спуфинга / сетевыми журналами, с помощью которых можно обмануть охотников за угрозами, детекторы аномалий и даже системы машинного обучения, которые уже вовсю применяются. Самый важный урок этой главы, а возможно и всей книги, заключается в том, что критически важно использовать аналитические данные об угрозах и реагировать на новые угрозы по-новому.

Список использованной литературы

1. *Shostack A.* STRIDE chart, Microsoft Secure (blog), Microsoft Corporation, September 11, 2007 // https://bit.ly/39aeOWy.
2. Adversarial Tactics, Techniques, & Common Knowledge Mobile Profile, ATT&CK, The MITRE Corporation, last modified May 2, 2018 // https://attack.mitre.org.
3. *Liska A., Gallo T.* Ransomware: Defending Against Digital Extortion, Sebastopol, CA: O'Reilly Media, 2017.
4. *Greenberg A.* 'Crash Override': The Malware That Took Down a Power Grid, WIRED, June 12, 2017 // https://bit.ly/38oMhgz.
5. *Cummins A., Minami Y.* The Book of Ninja, London: Watkins Publishing, 2013.
6. *Cummins A., Minami Y.* The Secret Traditions of the Shinobi, Berkeley, CA: Blue Snake Books, 2012.
7. *Cummins A., Minami Y.* True Path of the Ninja, North Clarendon, VT: Tuttle Publishing, 2017.
8. *Cummins A.* In Search of the Ninja: The Historical Truth of Ninjutsu, Stroud, England: The History Press: 2013.
9. APT1: Exposing One of China's Cyber Espionage Units, Mandiant, FireEye, FireEye Inc., February 2013 // https://bit.ly/2LbnPqg.
10. APT17, Advanced Persistent Threat Groups, FireEye Inc., last accessed February 7, 2020 // https://bit.ly/2Xl1QQ7.
11. *Strom B. E.* Adversarial Tactics, Techniques & Common Knowledge, ATT&CK, The MITRE Corporation, September 2015 // https://bit.ly/38oSrNJ.

12. BoringSSL, Git repositories on boringssl, last accessed September 26, 2018 // https://bit.ly/3s1mrHk.
13. *Malin C. H. et al.* Deception in the Digital Age: Exploiting and Defending Human Targets Through Computer-Mediated Communications, London: Elsevier, 2017; Brandon Valeriano et al., Cyber Strategy: The Evolving Character of Power and Coercion, New York: Oxford University Press, 2018.
14. *Osborne C.* Create a single file to protect yourself from the latest ransomware attack, Zero Day (blog), ZDNet, CBS Interactive, June 28, 2017 // https://bit.ly/35lPQ5d.
15. Classiques de l'Orient, 5, 1921.
16. *Carreon C.* Applying Threat Intelligence to the Diamond Model of Intrusion Analysis, Recorded Future Blog, Recorded Future Inc., July 25, 2018 // https://bit.ly/39kPe1c.
17. Cybersecurity Framework, National Institute of Standards and Technology, updated September 2018 // https://www.nist.gov/cyberframework/.
18. *Канеман Д.* Думай медленно... Решай быстро. 2011.
19. *Bianco D.* The Pyramid of Pain, Enterprise Detection & Response (blog), last updated January 17, 2014 // https://bit.ly/3s31prV.
20. Department of Defense Cybersecurity Culture and Compliance Initiative (DC31), U.S. Department of Defense, published September 2015 // https://bit.ly/3s1npTY.
21. *Alperovitch D.* CrowdStrike's work with the Democratic National Committee: Setting the record straight, CrowdStrike Blog, CrowdStrike, last modified January 22, 2020 // https://bit.ly/3rYVHr3.
22. *Draeger D. F.* Ninjutsu: The Art of Invisibility, North Clarendon, VT: Tuttle Publishing, 1989.
23. Entering the Military: DLAB, Military.com, Military Advantage, last accessed February 7, 2020 // https://bit.ly/39fvNXc.
24. *Lyon G.* Nmap: The Network Mapper, Insecure.org, updated March 18, 2018 // https://nmap.org.
25. *Zetter K.* A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever, WIRED, January 8, 2015 // https://bit.ly/3nqx0Aj.
26. *Zetter K.* An Unprotected Look at STUXNET, the World's First Digital Weapon, WIRED, November 3, 2014 // https://bit.ly/3ooEULS.
27. *Hinago M., Coaldrake W.* Japanese Castles, New York: Kodansha USA, 1986.

28. Nmap: The Network Mapper, Insecure.org, Gordon Lyon, updated August 10, 2019 // https://nmap.org.

29. *Ratti O., Westbrook A.* Secrets of the Samurai: The Martial Arts of Feudal Japan, North Clarendon, VT: Tuttle Publishing, 2016.

30. *Paganini P.* BAE Systems report links Taiwan heist to North Korean LAZARUS APT, Cyber Defense Magazine (website), October 18, 2017 // https://bit.ly/3s3PCcS.

31. *Smith R. E.* A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles, IEEE Security & Privacy 10, no. 6, 2012.

32. *Kayser R.* Die exakte Messung der Luftdurchgängigkeit der Nase, Arch. Laryng. Rhinol. 8, 1895.

33. Sensitive but Unclassified IP Data, Network Services, Defense Information Systems Agency, last accessed February 7, 2020 // https://bit.ly/2Xl9s57.

34. *Weinberger S.* How Israel Spoofed Syria's Air Defense System, WIRED, October 4, 2017 // https://bit.ly/35i67Za.

35. Software: China Chopper, ATT&CK, The MITRE Corporation, last modified April 24, 2019 // https://bit.ly/3q019YR.

36. SP 800-154 (DRAFT): Guide to Data-Centric System Threat Modeling, Computer Security Resource Center, National Institute of Standards and Technology, March 2016 // https://bit.ly/3bjQofW.

37. SP 800-16: Information Technology Security Training Requirements: A Role- and Performance-Based Model, Computer Security Resource Center, National Institute of Standards and Technology, published April 1998 // https://bit.ly/3otA9QY.

38. SP 800-53 Rev. 5 (DRAFT): Security and Privacy Controls for Information Systems and Organizations, Computer Security Resource Center, National Institute of Standards and Technology, published August 2017 // https://bit.ly/3hX2MUf.

39. Sqrrl Team, A Framework for Cyber Threat Hunting Part 1: The Pyramid of Pain, Threat Hunting Blog, Sqrrl, July 23, 2015 // https://www.threathunting.net/sqrrl-archive.

40. *Turnbull S.* Ninja AD 1460–1650, Oxford, England: Osprey Publishing, 2003.

41. Structured Threat Information eXpression (STIX) 1.x Archive Website, STIX, The MITRE Corporation, last accessed February 7, 2020 // https://stixproject.github.io.

42. Sword hunt, Wikipedia, Wikimedia Foundation, last modified November 26, 2018 // https://en.wikipedia.org/wiki/Sword_hunt/.

43. Symantec Security Response, Shamoon: Back from the dead and destructive as ever, Symantec Official Blog, November 30, 2016 // https://bit.ly/3oqdkxK.

44. Symantec Security Response, The Shamoon Attacks, Symantec Official Blog, Symantec Corporation, August 16, 2012 // https://bit.ly/2L2Az2z.

45. TEMPEST Equipment Selection Process, NCI Agency, accessed September 25, 2018 // https://bit.ly/2LfB3SK.

46. The ASVAB Test, Military.com, Military Advantage, last accessed February 7, 2020 // https://bit.ly/2Xle3Eu.

47. The Cyber Kill Chain, Lockheed Martin, Lockheed Martin Corporation, last accessed February 7, 2020 // https://bit.ly/2XjYrRN.

48. W32.Stuxnet, Symantec Security Center, Symantec Corporation, last modified September 16, 2017 // https://bit.ly/3bfoW2R.

49. Wireshark, The Wireshark Corporation, last accessed February 7, 2020 // https://www.wireshark.org.

Бен Маккарти

Кибердзюцу: кибербезопасность для современных ниндзя

Перевел с английского *С. Черников*

Руководитель дивизиона	*Ю. Сергиенко*
Руководитель проекта	*А. Питиримов*
Ведущий редактор	*Н. Гринчик*
Научный редактор	*Д. Старков*
Литературный редактор	*Н. Рощина*
Художественный редактор	*В. Мостипан*
Корректоры	*Н. Викторова, М. Молчанова*
Верстка	*Л. Егорова*

Изготовлено в России. Изготовитель: ООО «Прогресс книга». Место нахождения и фактический адрес: 194044, Россия, г. Санкт-Петербург, Б. Сампсониевский пр., д. 29А, пом. 52. Тел.: +78127037373.

Дата изготовления: 08.2022. Наименование: книжная продукция. Срок годности: не ограничен.

Налоговая льгота — общероссийский классификатор продукции ОК 034-2014, 58.11.12 — Книги печатные профессиональные, технические и научные.

Импортер в Беларусь: ООО «ПИТЕР М», 220020, РБ, г. Минск, ул. Тимирязева, д. 121/3, к. 214, тел./факс: 208 80 01.

Подписано в печать 24.06.22. Формат 70×100/16. Бумага офсетная. Усл. п. л. 18,060. Тираж 700. Заказ 0000.