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