Cisco 2018

Годовой отчет по информационной безопасности

Содержание

Краткий обзор

Что если бы защитники могли заглянуть в будущее? Если бы они знали, что атака на подходе, они могли бы остановить ее или как минимум ослабить ее последствия и обеспечить надежную защиту того, что для них наиболее важно. На самом деле защитники *могут* видеть, что там происходит на горизонте. Это можно понять по многим признакам, в том числе и очевидным.

Злоумышленники и преступники, действующие в государственных масштабах, уже обладают необходимым опытом и инструментами для вывода из строя критически важной инфраструктуры и систем и нанесения ущерба целым регионам. Но когда появляются новости о разрушительных, деструктивных кибератаках, как например недавние атаки в Украине, или где-нибудь еще в мире, первая мысль, которая посещает некоторых специалистов в области безопасности: «Ну, эта атака не была нацелена на рынок/регион/технологическую среду, где работает наша компания, поэтому нам, скорее всего, ничего не грозит».

Однако не обращая внимания на такие, казалось бы, отдаленные кампании или отдавая все силы только на решение текущих ежедневных задач по предотвращению атак, защитники рискуют будущим, так как от их внимания ускользает то, с какой скоростью и в каком масштабе злоумышленники наращивают и совершенствуют свой военный киберпотенциал.

Уже многие годы Cisco предупреждает защитников об эскалации киберпреступной активности по всему миру. В этом последнем ежегодном отчете по кибербезопасности мы представляем данные и анализ от исследователей Cisco в области угроз и нескольких наших технологических партнеров касательно поведения злоумышленников, наблюдаемого в последние год-полтора. Большинство тем, изучаемых в отчете, объединяют следующие три общих вопроса:

1. **Злоумышленники продолжают совершенствовать вредоносное ПО и выводят его на непревзойденные уровни сложности и силы поражения.**

   Эволюция вредоносного ПО (стр. 6) стала одним из наиболее значительных событий в ландшафте атак в 2017 году. С появлением сетевых крипточервей-вымогателей пропала потребность в использовании человеческих ресурсов для запуска кампаний с требованием выкупа. Кроме того, для некоторых злоумышленников целью является не выкуп, а уничтожение систем и данных, что доказал вирус Nyetya – вредоносная программа по стиранию данных, замаскированная под программу-вымогатель (см. стр. 6). По мнению исследователей угроз Cisco, самораспространяющееся вредоносное ПО очень опасно и потенциально может привести к «падению» всего Интернета.

2. **У злоумышленников все лучше получается обходить препятствия и применять в качестве оружия облачные сервисы и другие технологии, используемые в легитимных целях.**

   Помимо создания угроз, которые могут **обходить все более сложные среды песочниц** (стр. 22), разработчики вредоносного ПО **начинают все больше использовать шифрование, чтобы избежать обнаружения** (стр. 9). Цель шифрования – повышение безопасности, но с его помощью злоумышленники также получают эффективные инструменты для скрытия своей деятельности по командованию и управлению (command-and-control, C2), что дает им больше времени для работы и нанесения ущерба.

   Для осуществления такой своей деятельности киберпреступники также используют **легитимные веб-сервисы, такие как** Google, Dropbox и GitHub (см. стр. 24). Такая практика делает обнаружение вредоносного трафика практически невыполнимой задачей.

   Кроме того, многие злоумышленники начинают **запускать множественные кампании из одного домена** (стр. 26), что позволяет им увеличить возврат по инвестициям. Они также повторно используют ресурсы инфраструктуры, такие как зарегистрированные адреса эл. почты, номера в автономной системе (autonomous system numbers, ASN) и сервера имен.

3. **Атаки осуществляются через бреши в обороне, которые в основном появляются в связи с расширением Интернета вещей (IoT) и использованием облачных сервисов.**

   Защитники очень быстро развертывают IoT-устройства, но часто не уделяют должного внимания безопасности этих систем. **IoT-устройства, в которые вовремя не вносятся исправления и которые не контролируются должным образом, предоставляют злоумышленникам прекрасные возможности для проникновения в сети** (стр. 34). Кроме того, по мнению исследователей, организации с IoT-устройствами, подверженными атакам, кажутся **не заинтересованными в скором устранении последствий** (стр. 42). Что еще хуже, в ИТ-средах этих организаций имеется еще больше уязвимых IoT-устройств, о которых эти организации даже не подозревают.

Тем временем **наряду с ростом популярности IoT расширяются и IoT-ботнеты** – они становятся более зрелыми и автоматизированными. По мере роста этих сетей злоумышленники начинают использовать их для запуска еще более сложных распределенных атак отказа в обслуживании (DDoS) (стр. 31).

Злоумышленники также успешно пользуются тем фактом, что группам по обеспечению безопасности сложно одновременно защищать **и IoT, и облачные среды**. Одна из причин связана с недостаточной ясностью в плане того, кто же фактически ответственен за защиту этих сред (см. стр. 42).

Рекомендации для защитников

Нападение злоумышленников на любую организацию неизбежно, но будут ли готовы к этому ее защитники и как быстро они смогут устранить последствия нападения? Результаты **Сравнительного исследования Cisco возможностей в области информационной безопасности за 2018 год**, в котором подробно рассмотрены лучшие практические методики в области безопасности от 3600 респондентов из 26 стран, говорят о том, что защитникам приходится преодолевать массу трудностей (см. стр. 46).

Тем не менее защитники должны понимать, что стратегическое усовершенствование систем безопасности и следование распространенным лучшим практикам позволит снизить риски, замедлить прогресс злоумышленников и обеспечить лучший мониторинг ландшафта угроз. Рекомендуются следующие действия:

- Внедрение инструментов первой линии обороны, которые можно масштабировать, как например облачные платформы безопасности
- Гарантия соблюдения корпоративных политик и следование лучшим практикам для своевременного внесения исправлений в приложения, системы и устройства
- Внедрение сегментации сети для снижения рисков проникновения
- Применение инструментов мониторинга и обработки оконечных устройств нового поколения
- Своевременный доступ к точным данным и процессам анализа угроз, которые позволяют встраивать эти данные в процессы мониторинга и обработки событий безопасности
- Выполнение более глубокого и сложного анализа
- Анализ и практическое использование процедур реагирования на события безопасности
- Регулярное резервное копирование данных и тестирование процедур восстановления – это критически важные процессы в мире быстро перемещающихся сетевых червей-вымогателей и мощного разрушительного кибероружия
- Анализ эффективных практик третьих сторон и тестирование технологий безопасности для снижения риска атак на цепочки поставок
- Сканирование безопасности микросервисов, облачных сервисов и систем администрирования приложений
- Анализ систем безопасности и исследование использования SSL-аналитики и, при возможности, SSL-дешифрования

Защитники также должны рассмотреть возможность применения усовершенствованных технологий безопасности, включающих машинное обучение и способности искусственного интеллекта. С учетом того, что вредоносные программы умеют прятать свои коммуникации внутри зашифрованного веб-трафика, а внутренние нарушители могут отправлять конфиденциальные данные через корпоративные облачные системы, группам безопасности необходимы эффективные инструменты для предотвращения или обнаружения использования шифрования в целях сокрытия вредоносной деятельности.

Краткая информация о настоящем отчете

В отчете Cisco по информационной безопасности за 2018 год представлены наши последние достижения в сфере информационной безопасности для защиты организаций и пользователей от атак. Здесь также рассматриваются техники и стратегии, которые используют злоумышленники для преодоления этих защитных барьеров и уклонения от обнаружения.

В отчете также представлены основные выводы из **Сравнительного исследования Cisco возможностей в области информационной безопасности за 2018 год**, в котором изучается ситуация с информационной безопасностью на предприятиях и приводится оценка самих предприятий своей готовности к отражению атак.

Часть I.
Ландшафт атак

Часть I. Ландшафт атак

Злоумышленники продолжают совершенствовать вредоносное ПО и выводят его на непревзойденные уровни сложности и силы поражения. Растущее число и разнообразие типов и семейств вредоносного ПО продолжают усугублять хаос в ландшафте атак и практически сводят на нет усилия защитников по предотвращению и сдерживанию угроз.

ЭВОЛЮЦИЯ ВРЕДОНОСНОГО ПО

Одним из наиболее важных явлений в ландшафте атак в 2017 году стала эволюция программ-вымогателей. С появлением сетевых червей-вымогателей пропала потребность в использовании человеческих ресурсов для запуска кампаний с требованием выкупа. Кроме того, для некоторых злоумышленников целью является не выкуп, а уничтожение систем и данных. В следующем году мы ожидаем, что такого рода атак станет еще больше.

Таким образом, в 2018 году защитники должны быть готовы противостоять новым самораспространяющимся сетевым угрозам

В 2017 году злоумышленники вывели вредоносное ПО на новый уровень – как это и ожидалось. После кампании SamSam в марте 2016 года[1] – первой крупномасштабной атаки, в которой для распространения программ-вымогателей использовался сетевой вектор – исследователи угроз Cisco прекрасно понимали, что пройдет совсем немного времени и злоумышленники найдут способ автоматизировать эту технику. Нарушители смогут сделать свое вредоносное ПО еще более мощным за счет объединения его с функциями, характерными для червя, с целью нанесения повсеместного ущерба.

И такая эволюция произошла очень быстро. В мае 2017 года в Интернете появился и с невиданной скоростью распространился крипточервь-вымогатель WannaCry[2]. Он распространялся через уязвимость в системе безопасности Microsoft Windows, которая называется EternalBlue и которая была обнаружена хакерской группировкой Shadow Brokers в середине апреля 2017 года.

На момент вывода средств из электронных кошельков WannaCry удалось заработать более 143 000 долл. США посредством платежей биткоинами. За определенный временной интервал и с учетом первоначальных поступлений в биткоинах в кошельки – 93 531 долл. США, по оценкам исследователей Cisco, по выкупам было совершено около 312 платежей. Для сравнения: набору эксплойтов Angler, когда тот был активен, удалось заработать около 100 миллионов долл. США за год по всему миру.

WannaCry не отслеживал ущерб от шифрования и платежи, сделанные пораженными пользователями. Сколько пользователей получили ключи для дешифрования после совершения платежа, также неизвестно. (WannaCry продолжает распространяться до сих пор, и до сих пор пользователи продолжают впустую платить выкуп.) Так как на самом деле WannaCry как программа-вымогатель проявила себя достаточно слабо, правительство США и большинство исследователей в области кибербезопасности считают, что элемент вымогательства – это лишь прикрытие, за которым кроется настоящая цель WannaCry – стирание данных.

В июне 2017 года появился новый вирус Nyetya (который также называется NotPetya)[3]. Эта вредоносная программа-стиратель также маскируется под программу-вымогатель и также использует уязвимость, с целью выполнения удаленного кода, которая называется EternalBlue, а также уязвимость EternalRomance (также обнаруженную группировкой Shadow Brokers) и другие векторы, включая сохранение учетных записей,

1 *SamSam: The Doctor Will See You, After He Pays the Ransom,* блог Cisco Talos, март 2016 г.: blog.talosintelligence.com/2016/03/samsam-ransomware.html.
2 *Player 3 Has Entered the Game: Say Hello to 'WannaCry,'* блог Cisco Talos, май 2017 г.: blog.talosintelligence.com/2017/05/wannacry.html.
3 *New Ransomware Variant 'Nyetya' Compromises Systems Worldwide,* блог Cisco Talos, июнь 2017 г.: blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html.

не связанных с выпуском Shadow Brokers[4].Вирус Nyetya распространялся через системы программного обновления для пакета налоговых программ, используемого более чем 80% компаний в Украине, и был установлен на более чем 1 миллион компьютеров[5].Киберполиция Украины подтвердила, что этот вирус поразил более 2000 украинских компаний[6].

До появления самораспространяющихся программ-вымогателей вредоносное ПО распространялось тремя способами: через загрузку с сайтов, по эл. почте или с физических носителей, например с вредоносных USB-устройств. Поэтому чтобы инфицировать устройство или систему программой-вымогателем, в любом случае в той или иной мере требовалось участие человека. Теперь же с появлением этих новых векторов все, что нужно для запуска успешной сетевой кампании-вымогателя, – это наличие активной рабочей станции, на которой нет последних программных исправлений.

Специалистам по безопасности черви могут представляться «устаревшим» типом угроз, так как по мере совершенствования базовых продуктов по безопасности число уязвимостей и рисков со структурой червя в общем списке (Common Vulnerabilities and Exposures, CVE) уменьшилось. Однако, по мнению исследователей Cisco, самораспространяющееся вредоносное ПО не только представляет собой релевантную угрозу, но также в потенциале может вывести из строя весь Интернет. WannaCry и Nyetya – это только начало, за которым могут последовать более серьезные вещи, поэтому защитники должны быть во всеоружии.

Если бы больше организаций применяли базовые лучшие практики в сфере кибербезопасности, такие как исправление уязвимостей, внедрение соответствующих процессов и политик для реагирования на инциденты и выполнение сегментации сети, то можно было бы если не предотвратить распространение вирусов WannaCry и Nyetya, то значительно снизить их последствия.

Более подробные рекомендации по борьбе с автоматизированными сетевыми червями-вымогателями см. в статье *Back to Basics: Worm Defense in the Ransomware Age* в блоге Cisco Talos.

Слабое место системы безопасности: цепочка поставок

Кампания Nyetya также представляла собой атаку на цепочку поставок, одну из многих, которые наблюдали исследователи Cisco в 2017 году. Почему Nyetya смог так быстро поразить столько машин? Одна из причин была в том, что пользователи не рассматривали автоматическое обновление программ как риск для безопасности, а в некоторых случаях даже и не понимали, что получаемые ими обновления – вредоносны.

Еще одна атака на цепочку поставок, которая произошла в сентябре 2017 года, была реализована через сервера загрузки, используемые поставщиком ПО для распространения легитимного программного пакета CCleaner[7].Двоичные файлы CCleaner, которые включали программную закладку (бэкдор) с троянской программой, были подписаны с использованием действительного сертификата и создавали у пользователей ложную уверенность в том, что используемое ими ПО безопасно. Целью злоумышленников, проводящих эту кампанию, были крупные технологические компании, где это ПО использовалось как официально, так и неофициально, в виде так называемых теневых ИТ-ресурсов.

Скорость развития и сложность атак на цепочки поставок все увеличиваются. Такие атаки могут поражать компьютеры в массовых масштабах и действовать в них месяцами и даже годами. Защитники должны учитывать потенциальный риск использования аппаратного или программного обеспечения от организаций, не имеющих надежных практик и средств обеспечения безопасности. Рекомендуется работать с поставщиками, которые выпускают списки CVE, быстро исправляют уязвимости и постоянно прилагают усилия к тому, чтобы их системы сборки кода не были скомпрометированы. Кроме того, пользователи должны не жалеть времени и сканировать новое программное обеспечение прежде, чем его загрузить, чтобы удостовериться, что оно не содержит вредоносных программ.

Чтобы предотвратить ущерб от атак на цепочки поставок и не дать им распространиться по всей организации, полезно использовать сетевую сегментацию ПО, для которого не применяются всеобъемлющие практики обеспечения безопасности.

4 Там же.
5 *Ukraine scrambles to contain new cyber threat after 'NotPetya' attack,* авторы Джек Стабс (Jack Stubbs) и Матиас Уильямс (Matthias Williams), Reuters, июль 2017 г.: reuters.com/article/us-cyber-attack-ukraine-backdoor/ukraine-scrambles-to-contain-new-cyber-threat-after-notpetya-attack-idUSKBN19Q14P.
6 *The MeDoc Connection,* блог Cisco Talos, июль 2017 г.: blog.talosintelligence.com/2017/07/the-medoc-connection.html.
7 *CCleaner Command and Control Causes Concern,* блог Cisco Talos, сентябрь 2017 г.: blog.talosintelligence.com/2017/09/ccleaner-c2-concern.html.

В чем важность целостности аналитических отчетов об угрозах

Все организации, передающие информацию об угрозах клиентам или общественности по любым каналам, должны использовать правила, помогающие обеспечить точность отчетности. Даже если все факты недостаточно очевидны, организации могут передать имеющуюся информацию и не гадать. Лучше быть правым, чем быть первым.

Например, когда в мае 2017 года началась атака WannaCry, сообщество безопасности вначале не могло понять, как червь-вымогатель проникал в системы. Многие организации из государственного и частного сектора сообщали, что источником атаки была фишинговая кампания и вредоносные вложения в электронные письма. Однако это была сетевая угроза, основанная на сканировании и использовании уязвимых общедоступных портов Microsoft Windows Server Message Block (SMB).

Исследователи угроз Cisco быстро сообщили сообществу специалистов по безопасности, что электронные письма, которые они считали связанными с атаками WannaCry, скорее всего, были спамом от бота Necurs и распространяли программу-вымогатель Jaff. Лишь спустя несколько дней сообщество специалистов по безопасности сошлось на мнении, что подозрительные письма действительно содержали программу Jaff, а не WannaCry. В течение этого периода пользователи действовали, основываясь на информации, которая не могла им помочь избежать быстро распространяющихся атак WannaCry.

Хаос, последовавший за серией атак WannaCry, напоминает, что сообществу специалистов безопасности следует избегать передачи неточных фактов о происхождении и характере кибератак. В первые часы атак возникает срочная необходимость быстро остановить злоумышленников и защитить пользователей, и в результате этой срочности возможна публикация информации, которая создаст неразбериху и помешает пользователям защитить свои системы, особенно в социальных сетях.

Дополнительную информацию по этой теме можно найти в документе ***On Conveying Doubt*** в блоге Cisco.

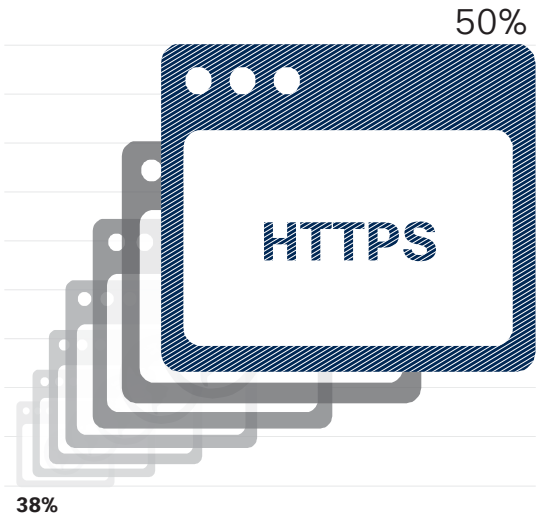
ЗАШИФРОВАННЫЙ ВРЕДОНОСНЫЙ ВЕБ-ТРАФИК

Растущий объем зашифрованного веб-трафика – как легитимного, так и вредоносного – создает еще больше трудностей и путаницы для защитников, старающихся идентифицировать и отслеживать потенциальные угрозы. Цель шифрования – повышение безопасности, но с его помощью злоумышленники также получают эффективные инструменты для скрытия своей деятельности по командованию и управлению (command-and-control, C2), что дает им больше времени для работы и нанесения ущерба. По прогнозам исследователей Cisco, в 2018 году злоумышленники начнут использовать шифрование еще активнее. Чтобы не отставать, защитникам необходимо дополнять свои существующие инструменты предотвращения, обнаружения и устранения последствий угроз более автоматизированными и усовершенствованными возможностями, например использовать машинное обучение и искусственный интеллект.

Темная лошадка: зашифрованный вредоносный веб-трафик

По данным исследователей Cisco, по состоянию на октябрь 2017 года в зашифрованном виде передавалось 50% глобального веб-трафика. Это на 12 пунктов больше в сравнении с 2016 годом (см. рис. 1). Одним из факторов, спровоцировавших такой рост, стала доступность дешевых или вовсе бесплатных SSL-сертификатов. Другой фактор – активное внедрение Google Chrome практики пометки незашифрованных веб-сайтов, работающих с конфиденциальной информацией, например данными кредитных карт клиентов, как «небезопасных». Компаниям приходится выполнять требования Google по HTTPS-шифрованию, если они не хотят потерять свой рейтинг на поисковой странице Google.

Рис. 1 Увеличение объема шифрованного глобального веб-трафика

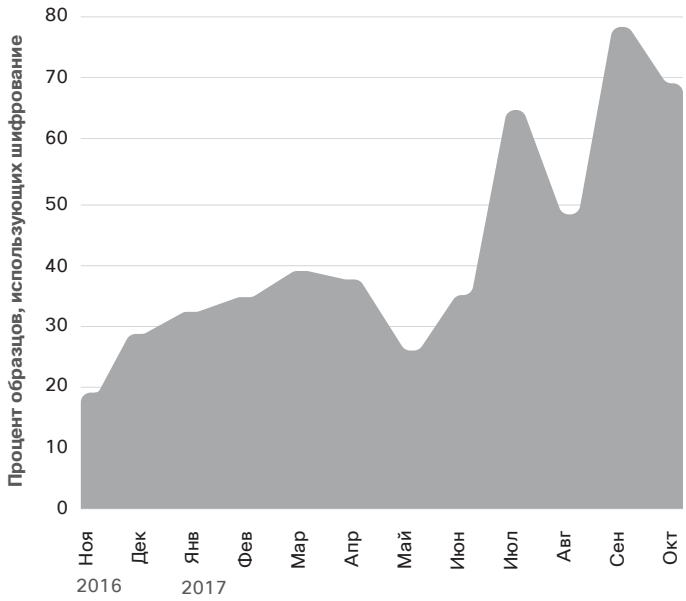


Увеличение глобального веб-трафика на 12 пунктов с ноября 2016 г. по октябрь 2017 г.

Источник: Исследование Cisco в области безопасности.

По мере увеличения объема зашифрованного глобального веб-трафика, злоумышленники все больше начинают использовать шифрование в качестве инструмента для сокрытия своей деятельности по командованию и управлению (command-and-control, C2). За последний год, по наблюдениям исследователей Cisco, число зашифрованных сетевых коммуникаций, используемых проверенными образцами вредоносного ПО, выросло более чем в три раза (см. рис. 2). Наш анализ более чем 400 000 вредоносных двоичных кодов показывает, что в около 70% трафика по состоянию на октябрь 2017 года хотя бы в какой-то степени использовалось шифрование.

Рис. 2 Увеличение объема вредоносных двоичных кодов, использующих шифрованную связь по сети



Источник: Исследование Cisco в области безопасности.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Применение машинного обучения к спектру угроз

Все больше предприятий начинает изучать возможности использования машинного обучения и искусственного интеллекта, чтобы решить проблему сложного мониторинга, которую создает шифрование, и уменьшить время действия злоумышленников. Благодаря усовершенствованным возможностям машинного обучения и AI можно укрепить оборону сети и со временем «обучить» системы безопасности автоматически выявлять нехарактерные модели поведения веб-трафика, которые могут свидетельствовать о вредоносной активности.

Машинное обучение можно использовать для автоматического обнаружения уже известных угроз (так называемые «известные-известные»), т. е. типов заражения, уже замеченных ранее (см. рис. 3). Однако их истинная ценность, особенно в том, что касается мониторинга зашифрованного трафика, связана со способностью обнаруживать «известные-неизвестные» угрозы (т. е. ранее не замеченные вариации известных угроз, подсемейства вредоносного ПО или связанные с ними новые угрозы) и «неизвестные-неизвестные» (абсолютно новые вредоносные) угрозы. Такая технология может обучиться идентифицировать необычные модели поведения в больших объемах зашифрованного веб-трафика и автоматически предупреждать группы по обеспечению безопасности о необходимости проведения дальнейшего расследования.

Последний момент наиболее важен с учетом того, что нехватка опытных обученных специалистов становится препятствием на пути укрепления обороны систем на большинстве предприятий, о чем свидетельствуют результаты, представленные в Сравнительном исследовании Cisco возможностей в области информационной безопасности за 2018 год (см. стр. 35). Автоматические и интеллектуальные средства, такие как машинное обучение и искусственный интеллект, помогут защитникам обойтись без дополнительных навыков и ресурсов, но при этом более эффективно обнаруживать известные и появляющиеся угрозы и реагировать на них.

Рис. 3 Машинное обучение в сетевой безопасности: таксономия

Примечание. Заявления о масштабировании относятся к трудозатратам сотрудников на обслуживание системы обнаружения.
Примечание. На этой схеме представлена упрощенная иллюстрация возможностей машинного обучения в сфере безопасности.

Source: Исследование Cisco в области безопасности.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

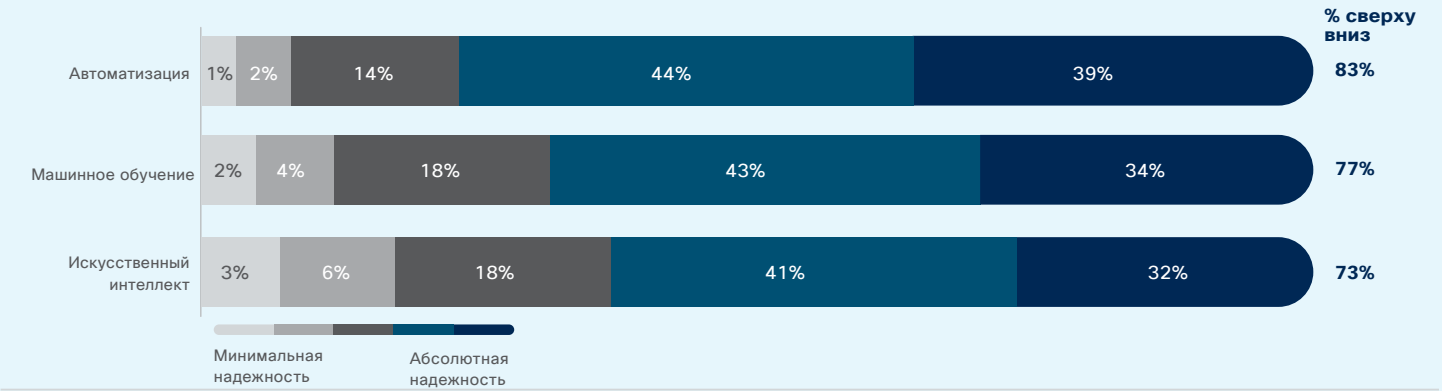
Сравнительное исследование возможностей в области информационной безопасности, проведенное Cisco в 2018 году. Защитники сообщают, что они все больше полагаются на автоматизацию и искусственный интеллект

Директора по информационной безопасности, опрошенные в рамках подготовки отчета Исследование возможностей в области информационной безопасности Cisco в 2018 году, утверждают, что они готовы добавить инструменты, использующие искусственный интеллект и машинное обучение, в связи с ростом сложности и расширением аналитических возможностей инфраструктур безопасности. Однако также они недовольны количеством ложных результатов, которые приносят такие системы, поскольку ложные результаты повышают нагрузку на отделы безопасности. По мере развития технологий машинного обучения и искусственного интеллекта эти проблемы должны стать менее значимыми, и системы безопасности научатся определять «нормальную» активность в исследуемых сетевых средах.

39% специалистов по безопасности полностью полагаются на технологии автоматизации, 34% полностью полагаются на машинное обучение; 32% полностью полагаются на искусственный интеллект (рис. 4).

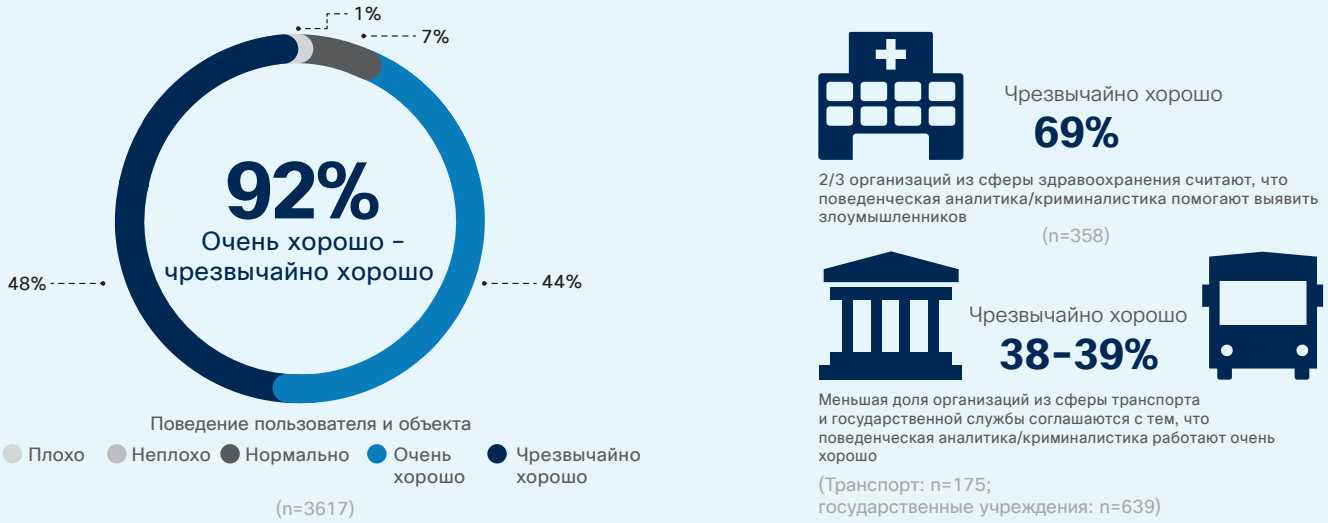
Средства поведенческой аналитики также считаются полезными при обнаружении вредоносных агентов в сетях; 92% специалистов по безопасности говорят, что эти инструменты работают очень хорошо или чрезвычайно хорошо (рис. 5).

Рис. 4 Организации серьезно полагаются на автоматизацию, машинное обучение и искусственный интеллект



Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Рис. 5 Большинство специалистов по безопасности видят ценность средств поведенческой аналитики



Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

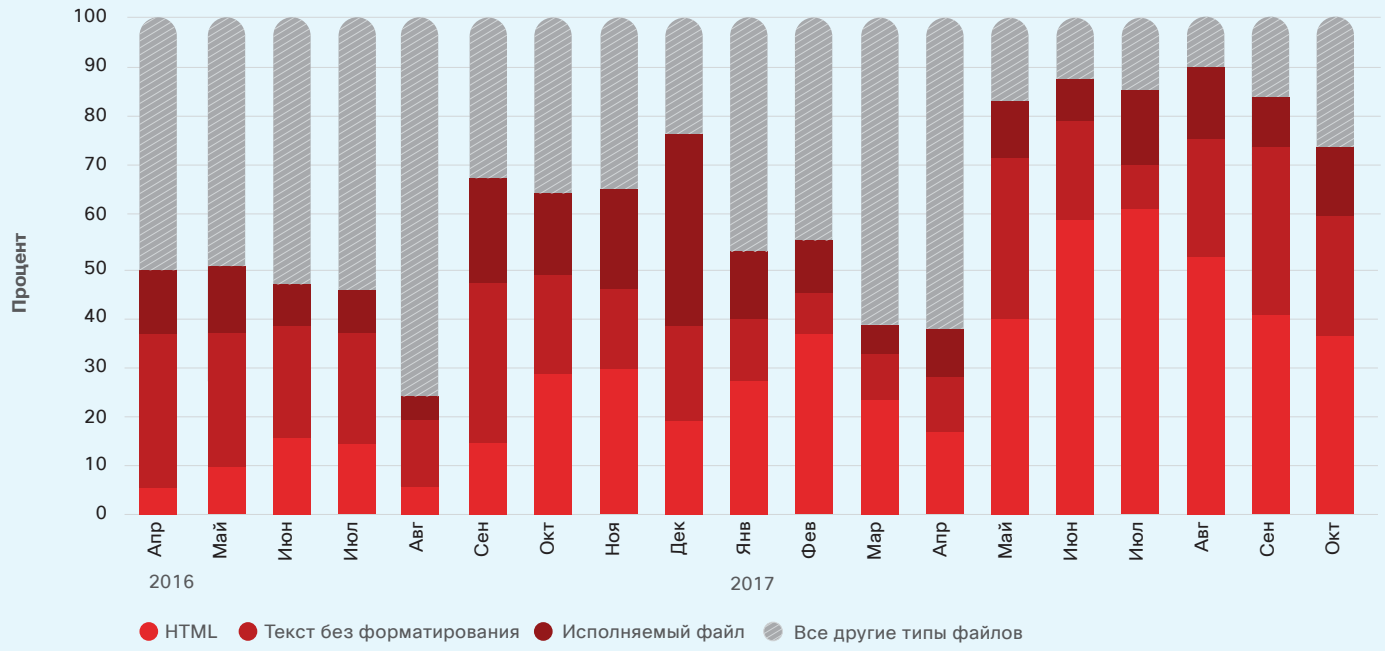
Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Методы, которые выбирают злоумышленники для веб-атак, свидетельствуют об их прицельной фокусировке на компрометации браузеров.

Анализ способов проведения веб-атак за полтора года в период с апреля 2016 по октябрь 2017 года показывает, что злоумышленники стали больше использовать вредоносный веб-контент (рис. 6). Такая тенденция вполне согласуется с агрессивным целенаправленным воздействием на веб-браузер Microsoft Internet Explorer с использованием по-прежнему активных наборов эксплойтов.

Исследователи Cisco наблюдали значительное и постоянное увеличение числа случаев обнаружения вредоносного веб-контента JavaScript. Это говорит об эффективности такой стратегии с целью заражения уязвимых браузеров и облегчения выполнения таких неблаговидных действий, как перенаправление браузера или загрузка троянских программ.

Рис. 6 Активность блоков на базе вредоносного ПО по типу контента, апрель 2016 г. – октябрь 2017 г.

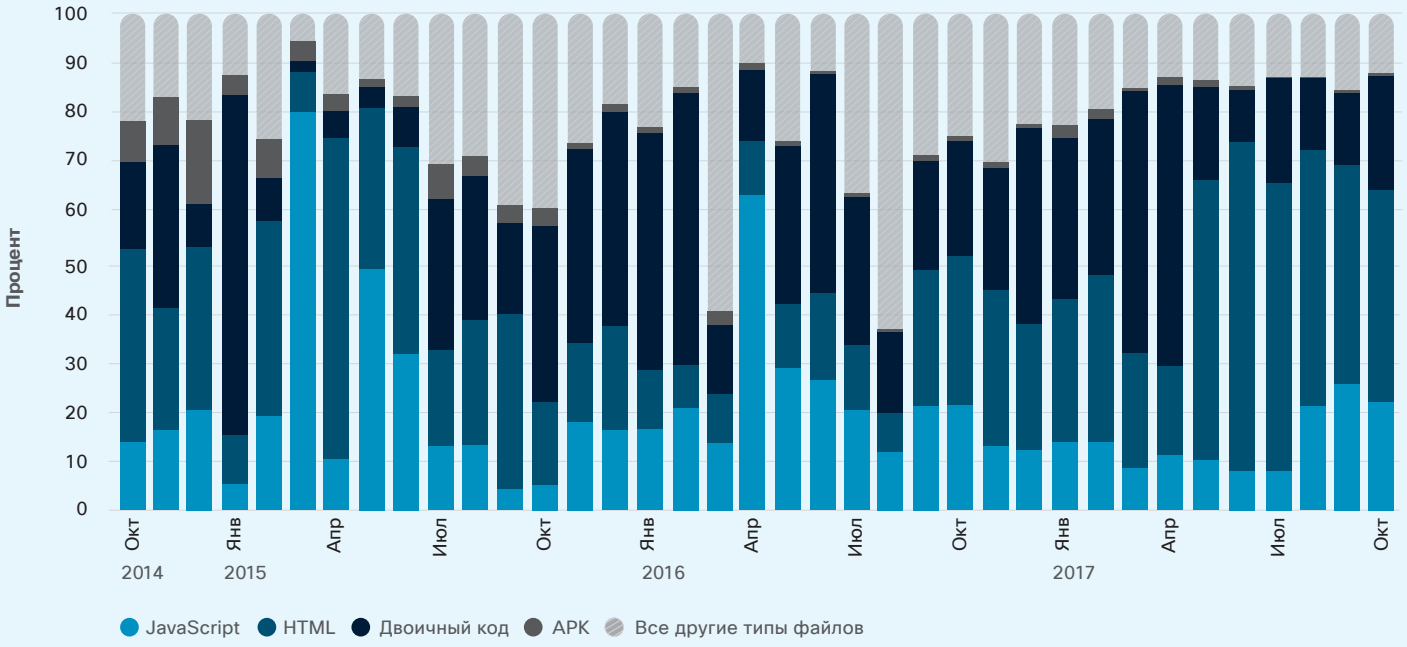


Источник: Исследование Cisco в области безопасности.

На рис. 7 представлен краткий обзор способов проведения веб-атак за трехлетний период, с октября 2014 по октябрь 2017 года. В течение этого периода злоумышленники постоянно внедряли подозрительные двоичные файлы, в основном для доставки рекламного или шпионского ПО. Как уже отмечалось в *Отчете по информационной безопасности Cisco за первое полугодие 2017 года*, такие типы потенциально нежелательных приложений (potentially unwanted applications, PUA) могут представлять собой увеличение заражений вредоносным ПО и кража информации о пользователях или компании[8].

Данные за последние три года, представленные на рис. 7, также показывают, что объем вредоносного веб-контента колеблется во времени по мере того, как злоумышленники запускают и завершают кампании и меняют свои тактики, препятствуя обнаружению.

Рис. 7 Активность блоков на базе вредоносного ПО по типу контента, октябрь 2014 г. – октябрь 2017 г.



Источник: Исследование Cisco в области безопасности.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

8 *Отчет Cisco по информационной безопасности за первое полугодие 2017 года*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

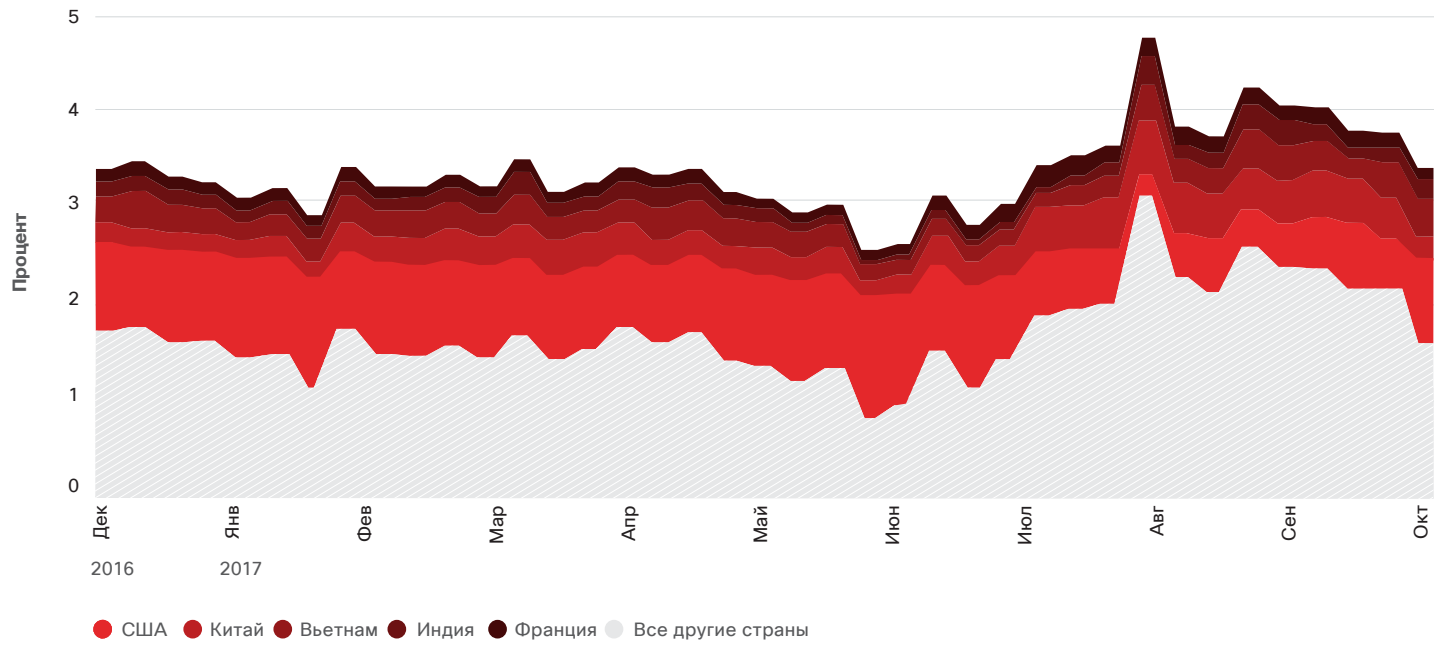
УГРОЗЫ ПО ЭЛЕКТРОННОЙ ПОЧТЕ

Как бы ни менялся ландшафт угроз, вредоносная почта и спам остаются важными инструментами злоумышленников для распространения вредоносного ПО, так как они могут доставить угрозу непосредственно на оконечное устройство. Составив успешную комбинацию из техник социальной инженерии, например внедрив в письмо фишинговые и вредоносные ссылки и вложения, злоумышленникам остается только сидеть и ждать, пока ничего не подозревающие пользователи активируют эти эксплойты.

Колебания активности ботнетов по рассылке спама влияют на общий объем.

В конце 2016 года исследователи Cisco отметили значительное увеличение активности спам-кампаний, которое, похоже, совпало с уменьшением активности наборов эксплойтов. Когда такие известные наборы эксплойтов, как Angler, внезапно исчезли с рынка, большинство пользователей этих наборов в стремлении сохранить свою прибыль обратились (или вернулись) к вектору угроз по эл. почте[9].Однако после первоначального быстрого возврата к эл. почте, объем глобального спама снизился и оставался примерно на одном уровне большую часть первой половины 2017 года. Затем в конце мая – начале июня 2017 года этот объем значительно снизился, прежде чем вновь взлететь вверх в середине-конце лета (см. рис. 8).

Рис. 8 Блоки IP-репутации по странам, декабрь 2016 г. – октябрь 2017 г.



Источник: Исследование Cisco в области безопасности.

9 См. раздел «Возможное влияние снижения активности наборов эксплойтов на глобальные тенденции распространения спама», стр. 18, *Отчет Cisco по информационной безопасности за первое полугодие 2017 года*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Рис. 9 Активность ботнетов для рассылки спама, октябрь 2016 г. – октябрь 2017 г.

Source: Cisco SpamCop

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Уменьшение объема спама с января по апрель 2017 года совпало с временным затишьем в активности ботнетов по рассылке спама, что видно из внутреннего графика, созданного сервисом Cisco® SpamCop (рис. 9).

Исследователи Cisco говорят, что ботнет Necurs, крупнейший поставщик всего спама в мире, был активен, но с января по апрель распространял меньше спама. В мае этот ботнет посредством массовых спам-кампаний распространял программу-вымогатель Jaff. В этих кампаниях рассылался PDF-файл со встроенным вредоносным документом Microsoft Office и начальный загрузчик программы-вымогателя Jaff[10]. Исследователи в области безопасности обнаружили уязвимость в Jaff, которая позволила им создать дешифратор, принуждающий операторов Necurs быстро вернуться к распространению обычной угрозы, программы-вымогателя Locky[11].Время, которое было необходимо злоумышленникам, стоящим за Necurs, чтобы вернуться обратно к Locky, совпало со значительным спадом в объеме глобального спама, наблюдаемого в первые две недели июня (рис. 9).

10 *Jaff Ransomware: Player 2 Has Entered the Game,* авторы Ник Биазини (Nick Biasini), Эдмунд Брумагин (Edmund Brumaghin) и Уоррен Мерсер (Warren Mercer), при участии Колин Грейди (Colin Grady), блог Cisco Talos, май 2017 г.: blog.talosintelligence.com/2017/05/jaff-ransomware.html.

11 *Player 1 Limps Back Into the Ring–Hello Again, Locky!* авторы Алекс Чуи (Alex Chiu), Уоррен Мерсер (Warren Mercer) и Джейсон Шультз (Jaeson Schultz), при участии Шона Байрда (Sean Baird) и Меттью Молиетта (Matthew Molyett, блог Cisco Talos, июнь 2017 г.: blog.talosintelligence.com/2017/06/necurs-locky-campaign.html.

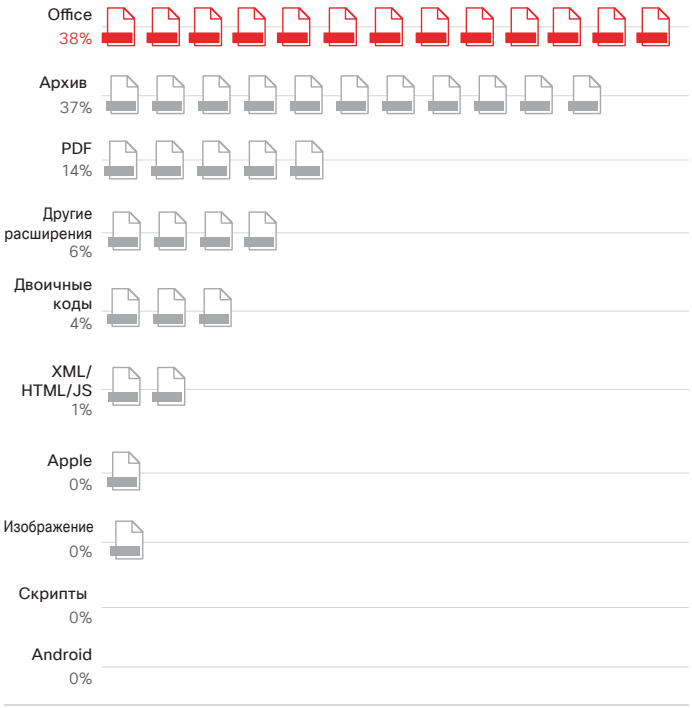
Вложения в эл. почте с вредоносными файлами: 10 самых распространенных инструментов семейств вредоносного ПО

Исследователи Cisco проанализировали телеметрические данные эл. почты в период с января по сентябрь 2017 года на предмет выявления типов расширений вредоносных файлов в документах эл. почты, чаще всего используемых распространенными семействами вредоносного ПО. По данным этого анализа, из 10 типов расширений файлов больше всего (38%) злоумышленники использовали форматы Microsoft Office, такие как Word, PowerPoint и Excel (см. рис. 10).

Далее, на втором месте (37%), шли архивные файлы, такие как .zip и .jar. То, что злоумышленники активно используют архивные файлы, совсем не удивительно – эти файлы уже давно стали излюбленным местом для сокрытия вредоносных программ. Пользователи должны открыть архивные файлы, чтобы посмотреть их содержимое, – а это важный шаг в цепочке заражения для многих угроз. Вредоносные архивные файлы также успешно могут обходить автоматизированные инструменты анализа, особенно когда они содержат угрозы, требующие для их активации участия пользователя. Во избежание обнаружения злоумышленники также могут использовать малоизвестные типы файлов, например .7z и .rar.

Вредоносные файлы с расширением PDF занимают в нашем анализе третье место с 14% от всех типов расширений вредоносных файлов. (Примечание. Категория «Другие расширения» относится к расширениям, замеченным в ходе нашего анализа, которые нельзя с легкостью отнести к известным типам файлов. Некоторые типы вредоносного ПО могут использовать расширения файлов программ-вымогателей.)

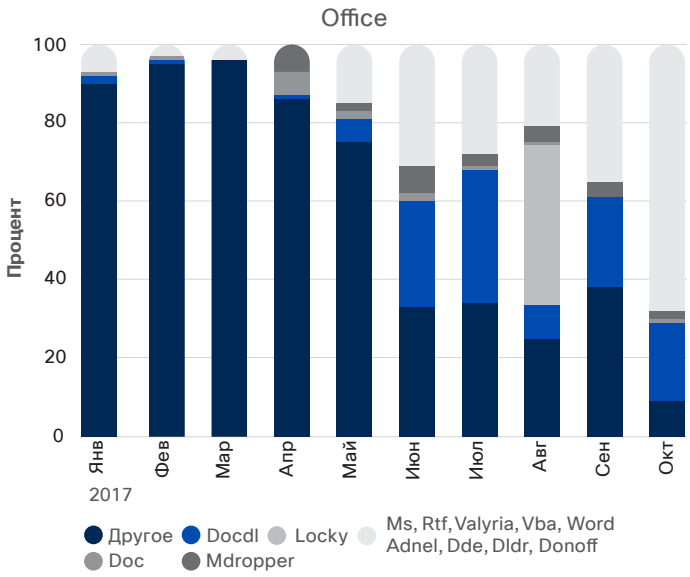
Рис. 10 Основные 10 расширений вредоносных файлов, январь – сентябрь 2017 г.



Источник: Исследование Cisco в области безопасности.

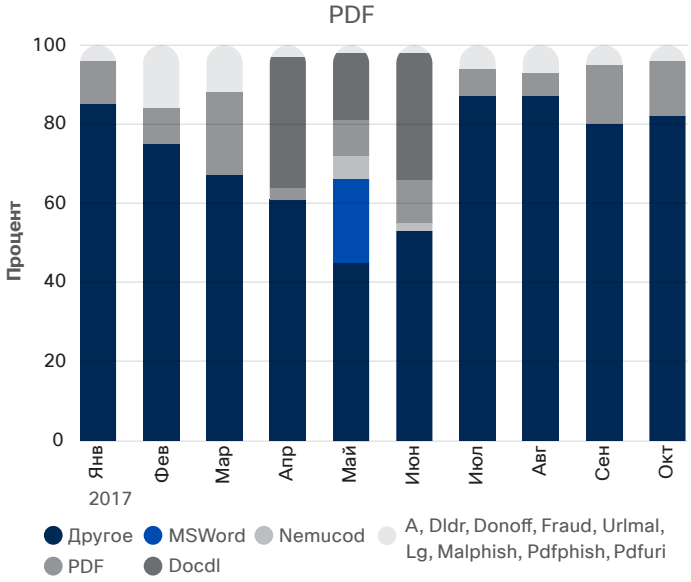
На рисунках 11a–c представлен обзор семейств вредоносного ПО, входящих в наше исследование, которые были связаны с тремя основными типами расширений вредоносных файлов: файлы MS Office, архивы и PDF. На рис. 12 показан процент обнаружения, по семействам, который включает расширение файла с вредоносной нагрузкой. По наблюдениям исследователей Cisco, всплески активности совпадают с кампаниями по распространению спама, наблюдаемыми в эти месяцы. Так, например, в конце лета шли две крупные кампании по распространению вредоносных программ Nemucod и Locky – двух угроз, часто работающих вместе. Nemucod известен тем, что отправляет вредоносные полезные нагрузки в архивных файлах, например .zip, которые содержат вредоносные скрипты, но выглядят как обычные файлы .doc (Dwnldr, также см. на рис. 12, тоже является разновидностью Nemucod).

Рис. 11a 3 главных типа расширений вредоносных файлов и отношения между семействами вредоносных программ



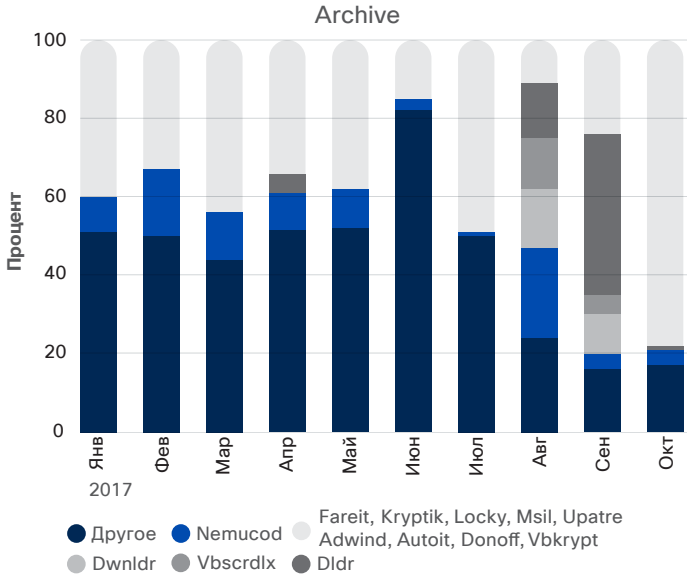
Источник: Исследование Cisco в области безопасности.

Рис. 11b 3 главных типа расширений вредоносных файлов и отношения между семействами вредоносных программ



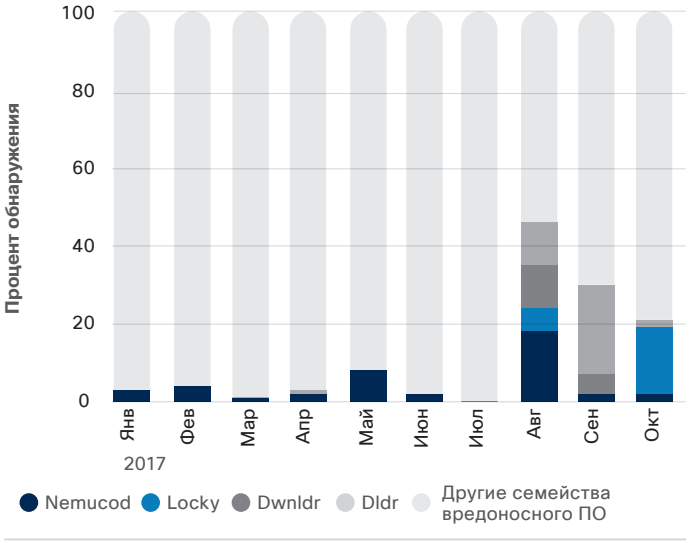
Источник: Исследование Cisco в области безопасности.

Рис. 11c 3 главных типа расширений вредоносных файлов и отношения между семействами вредоносных программ



Источник: Исследование Cisco в области безопасности.

Рис. 12 Шаблоны наиболее часто встречающихся семейств вредоносных программ, январь – октябрь 2017 г.



Источник: Исследование Cisco в области безопасности.

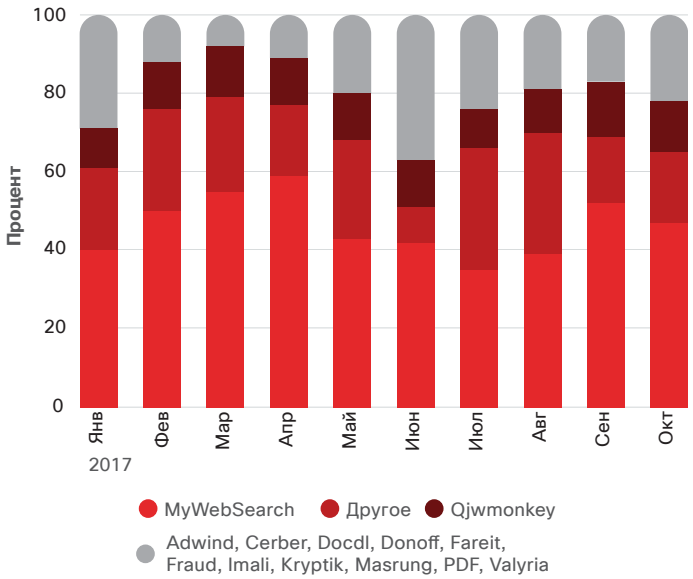
Шпионское ПО MyWebSearch – наиболее активный пользователь «других расширений»

Группа «другие расширения» в нашем исследовании включает несколько хорошо известных типов вредоносных программ. Однако наиболее активным игроком является MyWebSearch, вредоносное рекламное ПО и угонщик браузера, которое позиционируется как полезная панель инструментов (см. рис. 13). Он задействует только расширение файла .exe, иногда используя только один тип в месяц. Потенциально нежелательные приложения (potentially unwanted application, PUA) используются уже много лет и успели заразить самые разные типы браузеров. Они часто поставляются в комплекте с мошенническими программами и могут представлять для пользователей риск, связанный с вредоносной рекламой.

Наш анализ типов расширений вредоносных файлов показывает, что даже в современной технологически продвинутой и сложной среде угроз эл. почта продолжает оставаться важным каналом для распространения вредоносных программ. Базовые стратегии защиты для предприятий включают:

- Внедрение эффективных, комплексных способов защиты эл. почты
- Обучение пользователей, напоминание об угрозах, которые несут в себе вредоносные вложения и ссылки в фишинговых эл. письмах и спаме

Рис. 13 Наиболее активный пользователь MyWebSearch по поиску «других расширений»



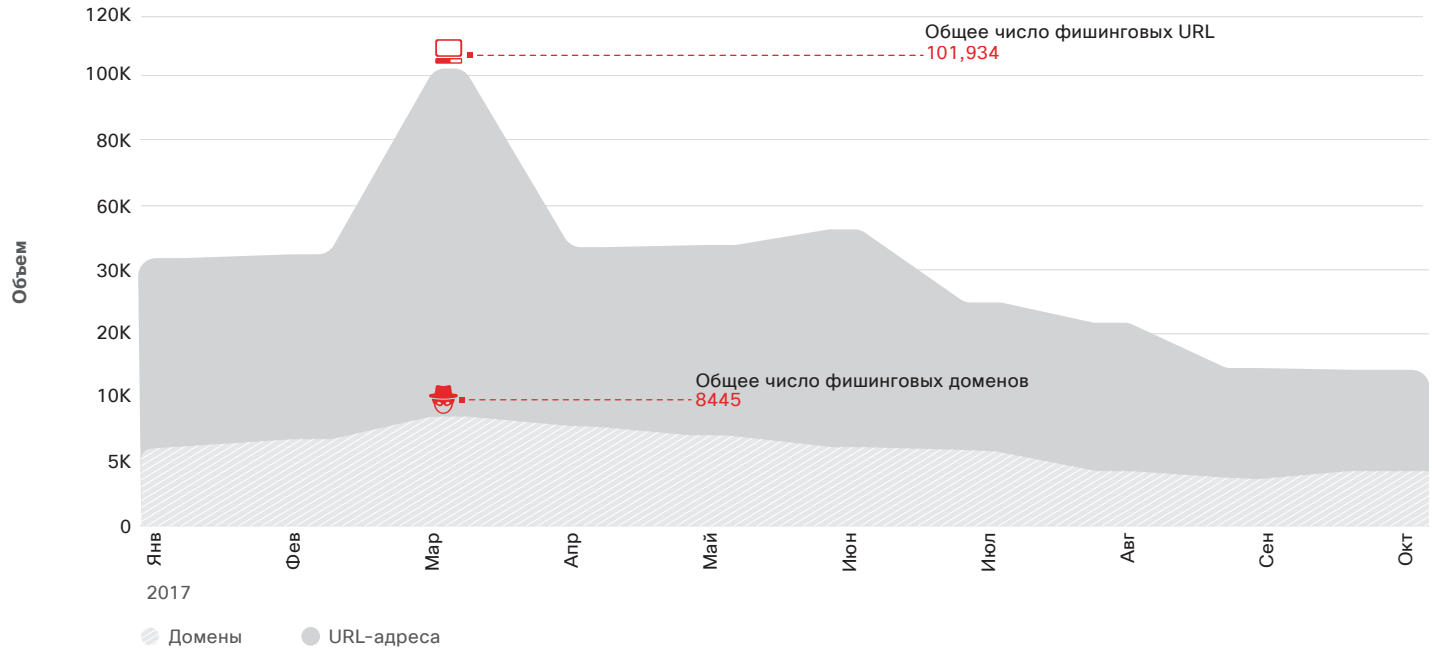
Источник: Исследование Cisco в области безопасности.

Социальная инженерия – по-прежнему важная стартовая площадка для атак по эл. почте

Фишинг и целевой фишинг – известные и уже давно используемые тактики кражи учетных данных и другой конфиденциальной информации пользователей, и это потому, что они очень эффективны. На самом деле, рассылка фишинговых эл. писем и целевой фишинг стали главными причинами самых крупных и известных нарушений безопасности в последние годы. 2017 год был отмечен двумя значимыми примерами: широкой атакой на пользователей Gmail[12] и взломом энергетических систем Ирландии[13].

Чтобы измерить превалирующую роль фишинговых URL-ссылок и доменов в современном Интернете, исследователи Cisco изучили данные из источников, которые исследуют потенциально «фишинговые» эл. письма, отправляемые пользователями, с помощью сообществ и антифишинговых средств анализа угроз. На рис. 14 показано число фишинговых URL-адресов и доменов, зафиксированных в период с января по октябрь 2017 года.

Рис. 14 Количество обнаруженных фишинговых URL и доменов за месяц



Источник: Исследование Cisco в области безопасности.

Всплески, наблюдаемые в марте и июне, связаны с двумя разными кампаниями. Первая кампания была нацелена на пользователей крупнейшего поставщика телекоммуникационных услуг. Эта кампания:

- включала 59 651 URL-адрес с поддоменами aaaainfomation[dot]org;
- включала поддомены, содержащие случайные стоки, состоящие из 50–62 букв.

Каждая длина поддомена (50–62) содержала около 3500 URL-адресов, что позволяло использовать эти поддомены программным образом (например: Cewekonuxykysowegulukozapojygepuqybyteqe johofopefogu[dot]aaaainfomation[dot]org).

Для регистрации доменов, зафиксированных в этой кампании, злоумышленники использовали недорогой частный сервис.

12 *Massive Phishing Attack Targets Gmail Users,* автор Алекс Джонсон (Alex Johnson), NBC News, май 2017 г.: nbcnews.com/tech/security/massive-phishing-attack-targets-millions-gmail-users-n754501.

13 *Hackers target Irish energy networks amid fears of further cyber attacks on UK's crucial infrastructure,* автор Лизи Деардон (Lizzie Deardon), *The Independent*, июль 2017 г.: independent.co.uk/news/world/europe/cyber-attacks-uk-hackers-target-irish-energy-network-russia-putin-electricity-supply-board-nuclear-a7843086.html.

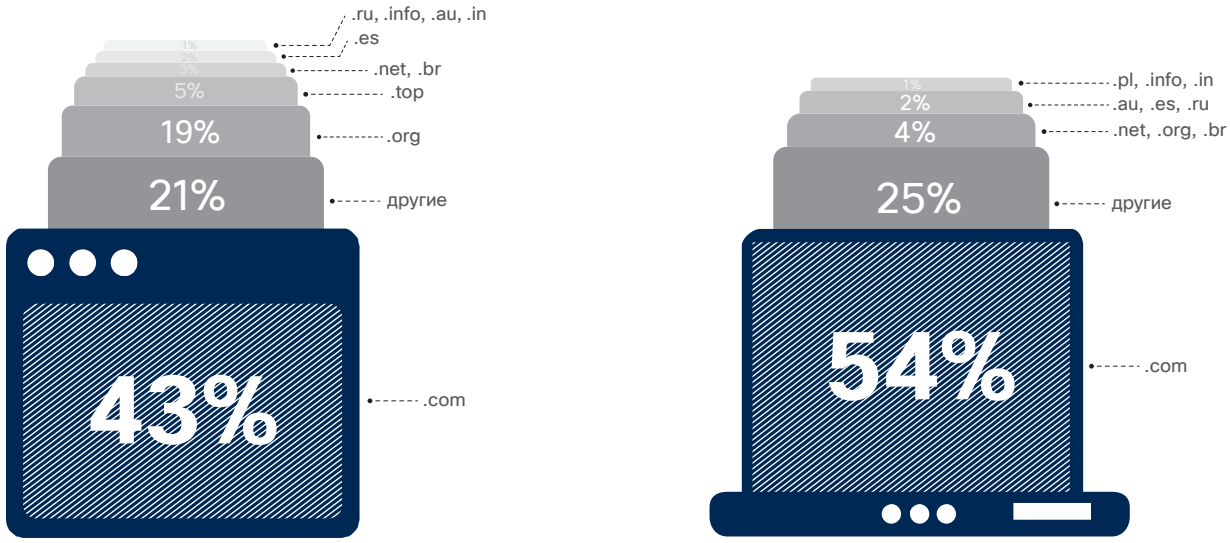
Во второй кампании, которая была наиболее активна в июне, для маскировки своей деятельности злоумышленники использовали название официального налогового органа Великобритании. Они задействовали 12 доменов верхнего уровня (top-level domains, TLD). Одиннадцать из этих доменов были URL-адресами с шестью строками из шести случайных символов (например: jyzwyp[dot] top). И девять из этих доменов были связаны более чем с 1600 фишинговыми узлами каждый.

Как и в мартовской кампании, злоумышленники зарегистрировали эти домены с использованием частного сервиса, чтобы скрыть информацию о регистрации домена. Все домены они зарегистрировали всего за два дня. На второй день было отмечено почти 19 000 URL-адресов, связанных с этой кампанией, и все они были обнаружены в течение пяти часов (более подробно о том, как быстро злоумышленники могут вводить только что зарегистрированные домены в использование, см. в разделе «Неправомерное использование легитимных ресурсов для контроля и управления через бэкдор», на стр. 24).

Распределение TLD по известным фишинговым сайтам

Наш анализ фишинговых сайтов в период с января по август 2017 года показывает, что злоумышленники в своей деятельности использовали 326 уникальных доменов верхнего уровня (TLD), включая .com, .org, .top (в основном в рамках кампании, проводившейся от имени налогового органа Великобритании), а также домены TLD по странам (см. рис. 15). Злоумышленникам выгодно использовать малоизвестные домены TLD, так как они обычно сами недорогие и часто предлагают еще и недорогие возможности для защиты конфиденциальности.

Рис. 15 Распределение TLD по известным фишинговым сайтам



Процент всех сайтов с TLD (все данные)

Процент сайтов с TLD (кроме особых TLD из двух кампаний, ориентированных на налоговые учреждения и телекоммуникационные компании)

Источник: Исследование Cisco в области безопасности.

Защитники должны быть бдительны и не забывать контролировать такую «старую» угрозу

В 2017 году на сервисы сообществ для анализа и борьбы с угрозами, которые мы рассматривали в нашем исследовании, ежемесячно приходили десятки тысяч сообщений о попытках фишинга. Для проведения фишинговых кампаний злоумышленники пользовались следующими широко распространенными тактиками и инструментами:

- **Доменный сквоттинг:** доменам присваивались имена, похожие на имена официальных доменов (например: cisc0[dot]com).
- **Теневое дублирование доменов:** в действующий официальный домен без ведома владельца добавлялись поддомены (например: badstuff[dot]cisco[dot]com).
- **Вредоносные зарегистрированные домены:** домен, создаваемый в злонамеренных целях (например: viqpbe[dot]top).
- **Уменьшители URL-адресов:** вредоносный URL-адрес, замаскированный с помощью уменьшителя URL-адресов (например: bitly[dot]com/random-string).

  Примечание. В изученных нами данных злоумышленниками чаще всего использовался инструмент для укорачивания URL-адресов Bitly.com. Вредоносные укороченные URL-адреса в нашем исследовании представляют 2% от фишинговых сайтов. В августе эта цифра достигла пикового значения в 3,1%.
- **Сервисы поддоменов:** сайт, создаваемый под сервером поддомена (например: mybadpage[dot]000webhost[dot]com).

Злоумышленники, занимающиеся фишингом и целенаправленным фишингом, постоянно совершенствуют методы социальной инженерии, чтобы заставить пользователей щелкнуть по вредоносной ссылке или посетить мошеннические веб-страницы и предоставить свои учетные данные или ценную информацию другого рода. В борьбе с этими угрозами важная роль должна отводиться обучению пользователей и их ответственности, а также применению технологий для защиты эл. почты.

ТАКТИКИ ОБХОДА ПЕСОЧНИЦ

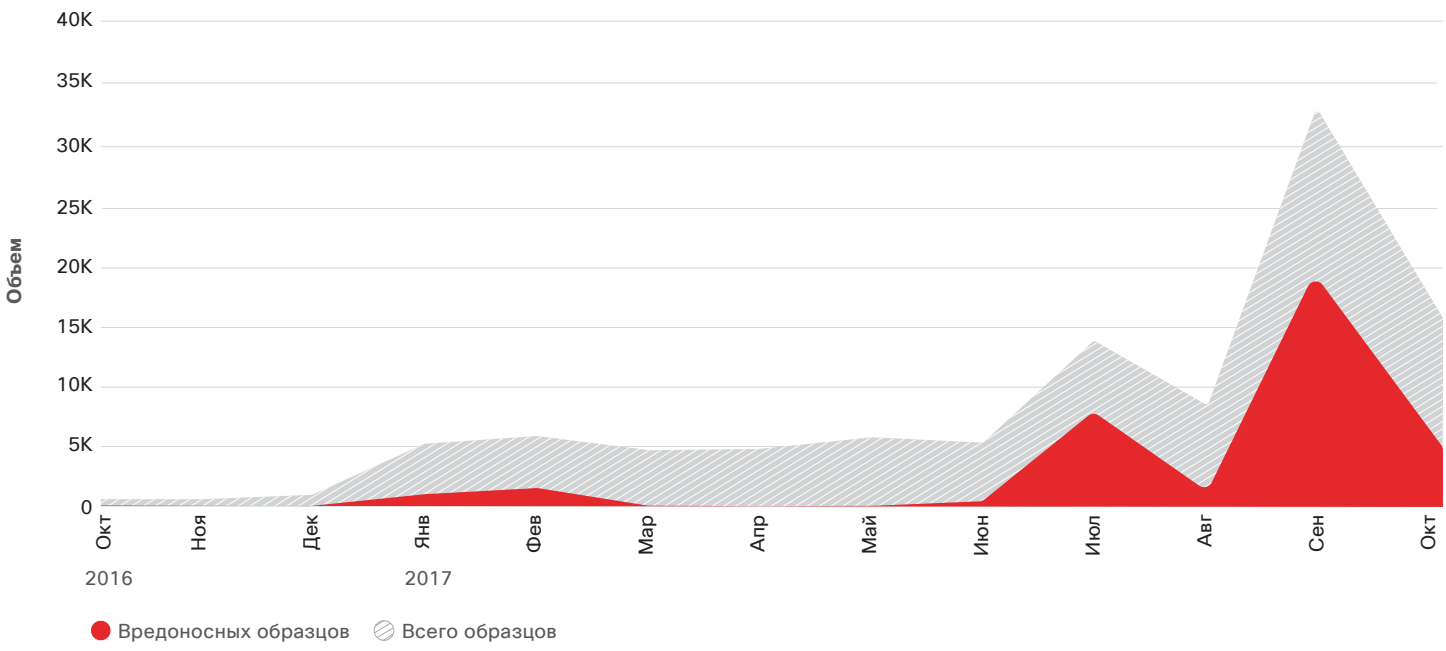
Злоумышленники научились разрабатывать угрозы, которые могут обходить даже самые технологически сложные среды песочниц. Когда исследователи Cisco проанализировали вредоносные вложения эл. почты, оснащенные различными техниками обхода песочниц, они обнаружили, что отдельные образцы вредоносов, использующих конкретную технику обхода, показывали резкий взлет, а затем очень быстрое падение. Это еще один пример того, как атакующие способны быстро наращивать объемы попыток проникновения сквозь защитные барьеры, когда они находят эффективную технику.

Авторы вредоносных программ играют в грязные игры в песочницах защитников

В сентябре 2017 года исследователями Cisco было отмечено большое количество примеров, когда вредоносная полезная нагрузка доставлялась после закрытия документа (рис. 16). В этом случае вредоносная программа инициировалась с использованием события «закрытие_документа». Эта техника в большинстве случаев прекрасно работала потому, что документы не закрывались после того, как документ был открыт и проанализирован в песочнице. Так как песочница явным образом не закрывала документ, вложения казались ей безопасными и доставлялись соответствующим получателям. Но когда получатель открывал вложение в виде документа и позднее закрывал этот документ, происходила доставка вредоносной полезной нагрузки. Таким образом с помощью этой техники можно было обойти те песочницы, которые должным образом не обнаруживали активность, происходящую после закрытия документа.

Использование события «закрытие_документа» – это хорошая возможность для злоумышленников. В данном случае используется макрофункциональность, встроенная в Microsoft Office, а также намерение пользователей открывать вложения, которые им важны. Когда пользователи понимают, что вложение им не нужно, они закрывают документ, инициируя макрос, в котором скрыта вредоносная программа.

Рис. 16 В сентябре 2017 г. наблюдался большой объем документов Microsoft Word, в которых использовались «закрытые вызовы функций»

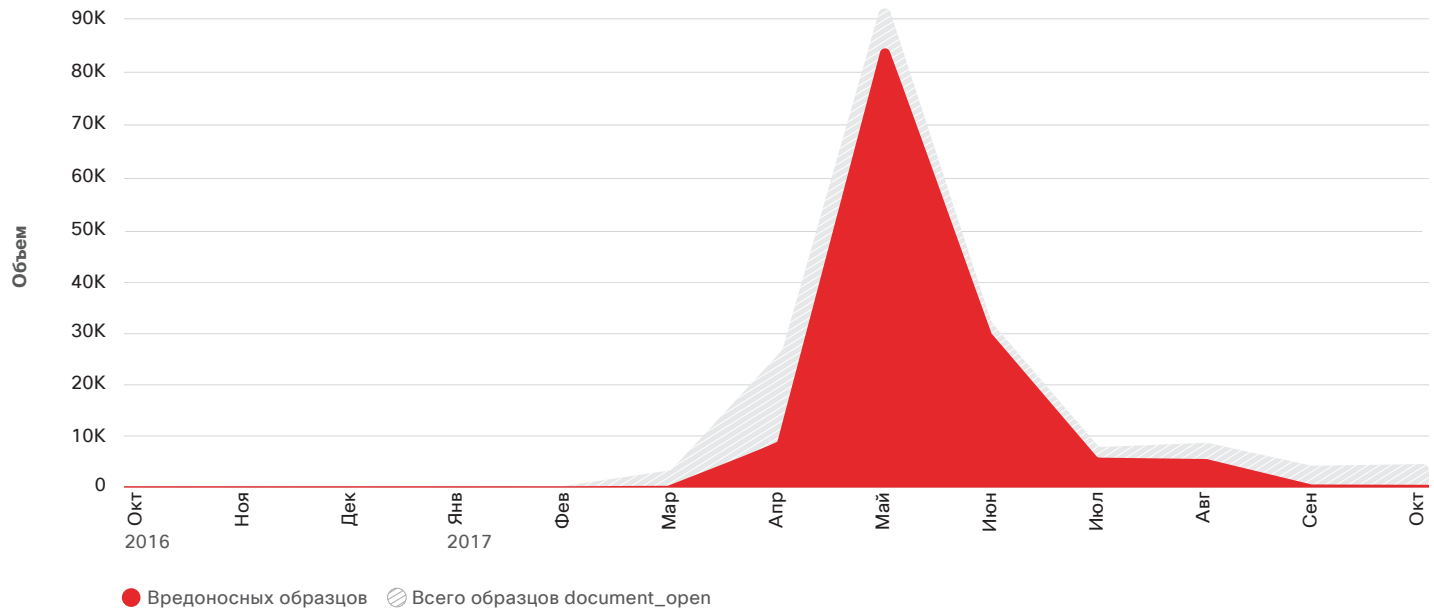


Источник: Исследование Cisco в области безопасности.

Некоторые злоумышленники обходят песочницы, маскируя тип документа, в котором есть вредоносная полезная нагрузка. Как показано на рис. 17, нами была отмечена объемная атака в мае 2017 года, которая была построена вокруг документов Word, встроенных в документы PDF. Такие документы могут обходить песочницы, которые просто обнаруживают и открывают PDF-файлы, вместо того чтобы также открыть и проанализировать встроенный документ Word. Документ PDF обычно содержит призыв к пользователю нажать и открыть документ Word, который инициирует злонамеренные действия. С помощью этой техники можно обойти песочницы, которые не открывают и не анализируют встроенные в PDF-файлы документы.

Пронаблюдав всплеск в появлении таких образцов вредоносных программ с использованием PDF-файлов, наши исследователи усовершенствовали среду песочницы, чтобы точно обнаруживать PDF-файлы, содержащие действия или стимулы для открытия встроенных документов Word.

Рис. 17 Крупная атака в мае 2017 г. была связана с файлами PDF, в которые были встроены вредоносные документы Word



Источник: Исследование Cisco в области безопасности.

Всплески в использовании образцов вредоносных программ с разными техниками обхода песочниц говорят о желании разработчиков вредоносов применять метод, который кажется им (или другим злоумышленникам) наиболее работающим. Кроме того, если при создании вредоносного ПО или связанной с ним инфраструктуры злоумышленники потерпят неудачу, они хотели бы все равно получать возврат по вложенным им средствам и усилиям. Если они понимают, что вредонос может проскользнуть сквозь песочницу, они, конечно, будут увеличивать число попыток атак и зараженных пользователей.

Исследователи Cisco рекомендуют использовать песочницы, имеющие функции анализа контента, чтобы гарантировать, что вредоносные программы, использующие описанные выше техники, не останутся незамеченными аналитическими инструментами песочницы. Так, например, технология песочницы должна понимать функции метаданных анализируемых в песочнице образцов, т. е. должна уметь определять, включает ли образец инициирование какого-либо действия после закрытия документа.

НЕПРАВОМЕРНОЕ ИСПОЛЬЗОВАНИЕ ОБЛАЧНЫХ СЕРВИСОВ И ДРУГИХ ЛЕГИТИМНЫХ РЕСУРСОВ

По мере того как приложения, данные и идентификационная информация перемещаются в облако, группы по обеспечению безопасности должны уметь управлять рисками, связанными с потерей контроля над традиционным периметром сети. Злоумышленники успешно пользуются тем фактом, что группам по обеспечению безопасности сложно одновременно защищать развивающиеся и расширяющиеся IoT и облачные среды. Одна из причин связана с недостаточной ясностью в плане того, кто же фактически ответственен за защиту этих сред.

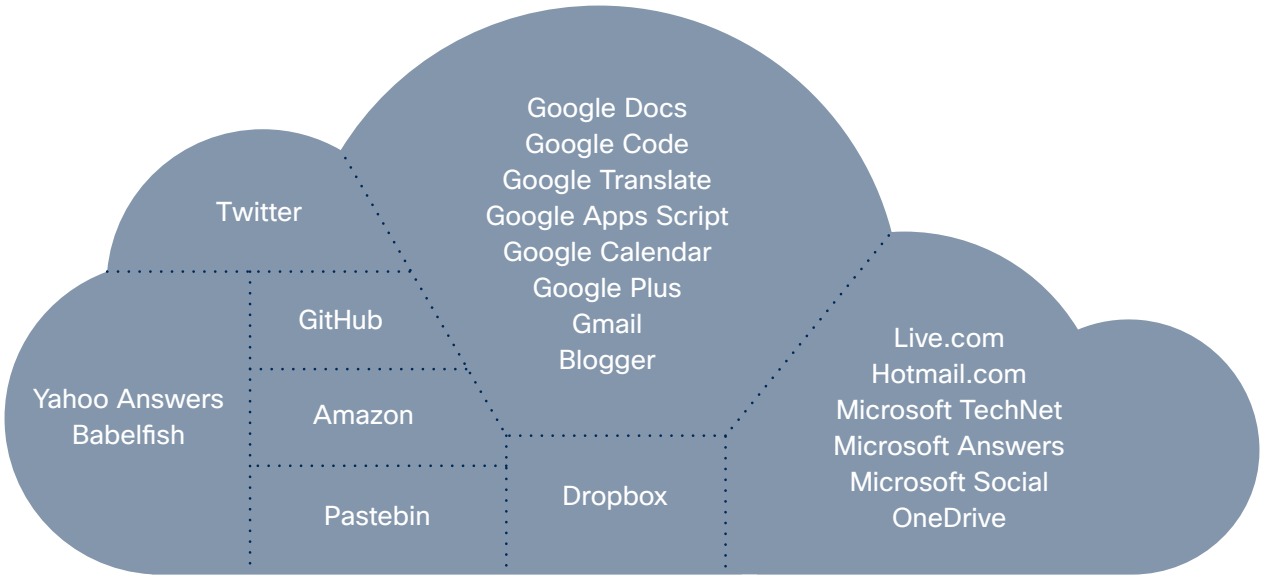
Чтобы решить эти вопросы, предприятиям необходимо комбинировать лучшие практические методики, усовершенствованные технологии обеспечения безопасности, такие как машинное обучение, и даже некоторые отдельные экспериментальные методологии, в зависимости от сервисов, которыми они пользуются для своего бизнеса, и от того, как развиваются угрозы в этом пространстве.

Неправомерное использование легитимных ресурсов для контроля и управления через бэкдор

При использовании разработчиками угроз легитимных сервисов для командования и управления (C2), группам по обеспечению безопасности становится практически невозможно идентифицировать вредоносный сетевой трафик, так как он имитирует свое поведение в полном соответствии с легитимным сетевым трафиком. У злоумышленников есть масса способов прикрытия в Интернете, так как многие сегодня пользуются такими сервисами, как Google Docs и Dropbox, для выполнения своей работы, даже не зависимо от того, предлагаются ли эти сервисы и систематически рекомендуются и проверяются их работодателями или нет.

На рис. 18 представлено несколько хорошо известных легитимных сервисов, в которых наши исследователи в сотрудничестве с компанией Anomali, партнером Cisco и поставщиком аналитических инструментов для борьбы с угрозами[14], наблюдали использование вредоносных схем для тайного контроля и управления через бэкдор за последние несколько лет. (Примечание. Борясь с неправомерным использованием, такие типы сервисов сталкиваются с дилеммой: если сильно усложнять для пользователей процесс настройки аккаунтов и пользования их услугами, это может значительно сказаться на их способности генерировать прибыль.)

Рис. 18 Примеры легитимных сервисов, которые вредоносное ПО использует в злонамеренных целях для C2



Источник: Anomali

всех удаленных систем, являющихся частью... архитектуры коммуникаций» вредоносного ПО.

Согласно исследованию компании Anomali, разработчики сложных постоянных угроз (advanced persistent threat, APT) и группы, спонсируемые государствами, были среди первых, кто использовал легитимные сервисы с целью злонамеренного командования и управления (C2); однако сегодня эта техника применяется еще большим числом разного рода злоумышленников, действующих в теневой экономике. Использование легитимных сервисов для C2 привлекает разработчиков вредоносного ПО, так как в этом случае легко:

- Регистрировать новые аккаунты на этих сервисах.
- Настраивать веб-страницу в публично доступном Интернете.
- Незаконно использовать шифрование для C2-протоколов. (Вместо настройки серверов C2 с шифрованием или встраивания шифрования во вредоносную программу, злоумышленники просто используют SSL-сертификат легитимного сервиса.)
- Оперативно адаптировать и трансформировать ресурсы. (Злоумышленники могут повторно использовать импланты во время атак без повторного использования, например, DNS или IP-адресов.)
- Уменьшать вероятность «засвета» инфраструктуры. (Злоумышленникам, применяющим легитимные сервисы для C2, не нужно жестко кодировать вредоносное ПО с использованием IP-адресов или доменов. По окончании своей работы они могут просто снять свои страницы с легитимных сервисов – и никто никогда не узнает их IP-адреса.)
- Эта техника выгодна для злоумышленников, так как позволяет им сокращать накладные расходы и повышать возврат на инвестиции.

Что касается защитников, то использование злоумышленниками легитимных сервисов для C2 связано для них с рядом значительных трудностей:

Легитимные сервисы трудно блокировать
Могут ли организации, исключительно в бизнес-целях, задумываться о блокировании каких-либо легитимных интернет-сервисов, как Twitter или Google?

Легитимные сервисы обычно зашифрованы, и изначально их трудно проверить
SSL-дешифрование достаточно дорого и не всегда возможно для применения в масштабах предприятия. Таким образом, вредоносное ПО прячется внутри зашифрованного трафика, затрудняя или делая невозможным для групп по обеспечению безопасности обнаружение вредоносного трафика.

Использование легитимных сервисов затрудняет анализ доменов и сертификатов и осложняет установление авторства (атрибуцию)
Злоумышленникам нет необходимости регистрировать домены, так как исходным адресом C2 считается аккаунт легитимного сервиса. Кроме того, они вряд ли продолжат регистрировать для схем C2 SSL-сертификаты или использовать самоподписанные SSL-сертификаты. Очевидно, что обе тенденции негативно скажутся на каналах для фильтрации по репутации индикаторов и составлении черных списков по индикаторам на основе недавно созданных и недавно зарегистрированных доменов и сертификатов и связанных с ними IP-адресов.

Определить использование легитимных сервисов в целях C2 достаточно трудно. Однако исследователи из компании Anomali рекомендуют, чтобы защитники применяли для этого некоторые отдельные экспериментальные технологии. Например, защитники могут идентифицировать вредоносное ПО, использующее легитимные сервисы для C2, обращая внимание на следующие признаки:

- Подключение к легитимным сервисам не через браузер и не через приложение
- Небольшие или единичные размеры ответов страниц с легитимных сервисов
- Частый обмен сертификатами с легитимными сервисами
- Большой объем образцов, попадающих в песочницу, в связи с подозрительными DNS-обращениями на легитимные сервисы

Все вышеприведенные случаи нестандартного поведения говорят о том, что программы и процессы с данного источника подлежат дальнейшей проверке[15].

15 Для получения более подробной информации о данных экспериментальных методологиях и дополнительной информации о том, как злоумышленники могут использовать легитимные сервисы для командования и контроля (C2), см. исследование компании Anomali, *Rise of Legitimate Services for Backdoor Command and Control*, доступное по ссылке: anomali.cdn.rackfoundry.net/files/anomali-labs-reports/legit-services.pdf.

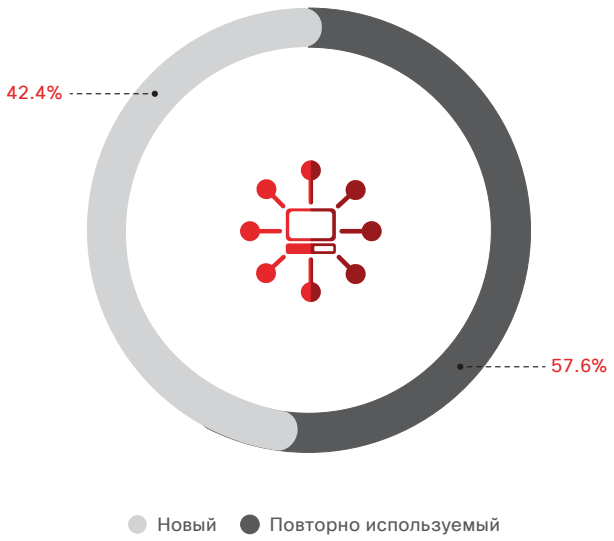
Получение больших преимуществ от ресурсов

Исследователи Cisco в области безопасности проанализировали недавно увиденные уникальные имена запросов (доменов), связанные с DNS-запросами, сделанными в течение 7 дней в августе 2017 года. Обращаем внимание, что под «недавно увиденными» в этом исследовании понимаются домены, которые были впервые «замечены» технологиями обеспечения облачной безопасности Cisco во время периода наблюдения, что не говорит о том, что такие домены были созданы недавно.

Целью исследования было получение более глубокого представления о том, как часто злоумышленники используют (и повторно используют) в своих атаках домены зарегистрированного уровня (registered-level domains, RLD). Поняв, как ведет себя угроза на уровне домена, защитникам будет проще идентифицировать вредоносные домены и связанные с ними поддомены, которые должны быть заблокированы такими средствами первой линии защиты, как облачные платформы безопасности.

Таким образом, чтобы наши исследователи смогли сосредоточиться исключительно на целевой группе уникальных доменов RLD (общим числом около 4 млн), поддомены были исключены из выборки недавно увиденных доменов. Только небольшой процент доменов RLD в этой выборке был отнесен к категории вредоносных. Из доменов RLD, оказавшихся вредоносными, более половины (около 58%) использовались повторно (см. рис. 19).

Рис. 19 Процент новых и повторно используемых доменов



Источник: Исследование Cisco в области безопасности.

Результаты этого исследования показывают, что пока большинство атакующих создают новые домены для своих кампаний, другие целенаправленно стараются получить как можно больший возврат по своим инвестициям, запуская множество кампаний с одного домена. Регистрация домена может стоить дорого, особенно в тех масштабах, которые необходимы большинству злоумышленников для проведения своих кампаний и уклонения от обнаружения.

Одна пятая часть вредоносных доменов начинает использоваться очень быстро

Зарегистрировав домен, злоумышленники могут сидеть на нем дни, месяцы и даже годы, выжидая подходящего времени, чтобы его использовать. Однако исследователи угроз из компании Cisco отмечают, что значительный процент вредоносных доменов – около 20% – был использован для проведения кампаний менее чем через одну неделю после их регистрации (см. рис. 20).

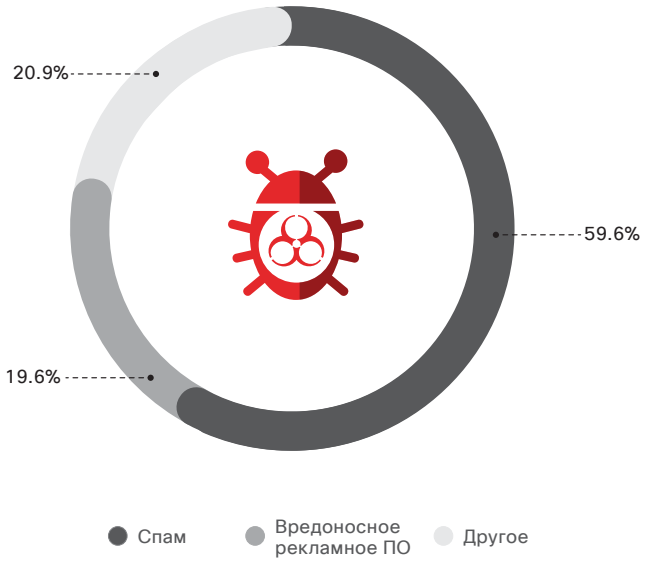
Рис. 20 Время регистрации RLD

Источник: Исследование Cisco в области безопасности.

Многие новые домены связаны с кампаниями вредоносной рекламы

Большая часть проанализированных вредоносных доменов была связана со спам-кампаниями (около 60%). И почти одна пятая из этих доменов была связана с кампаниями по распространению вредоносной рекламы (см. рис. 21). Вредоносная реклама стала важным инструментом для перенаправления пользователей на наборы эксплойтов, включая те, которые распространяют программы-вымогатели.

Рис. 21 Определение категорий вредоносных программ



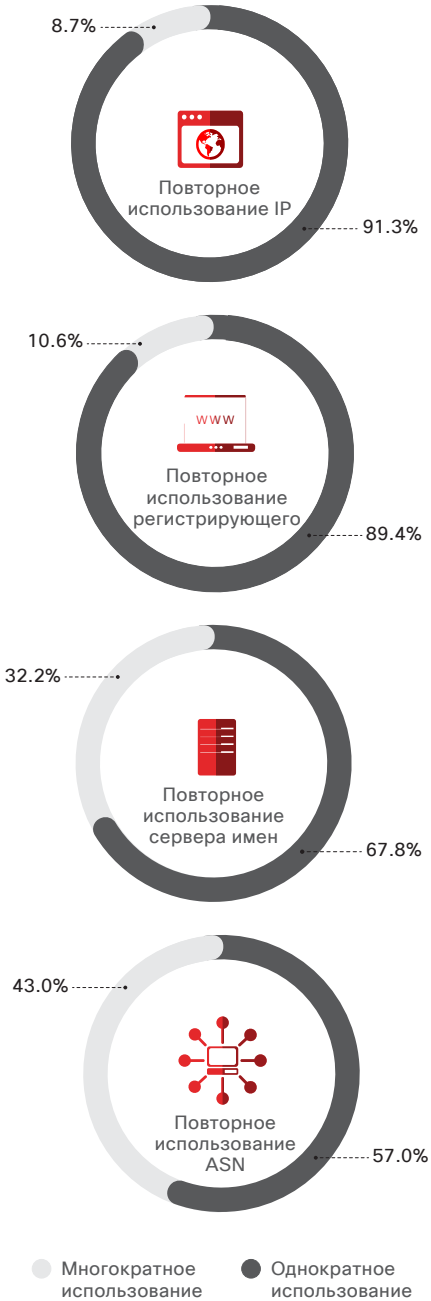
Источник: Исследование Cisco в области безопасности.

Популярные связанные с доменами техники для создания кампаний по распространению вредоносной рекламы включают скрытое копирование доменов. С помощью этой техники злоумышленники крадут учетные данные аккаунта легитимного домена, чтобы создать поддомены, связанные с вредоносными серверами. Еще одной тактикой является неправомерное использование бесплатных динамических DNS-сервисов для создания вредоносных доменов и поддоменов. Это позволяет разработчикам угроз доставлять вредоносные полезные нагрузки с постоянно меняющихся IP-адресов, где они размещаются, или инфицировать компьютеры пользователей или компрометировать публичные веб-сайты.

Домены повторно используют ресурсы инфраструктуры

Вредоносные домены зарегистрированного уровня (RLD) в нашей выборке также повторно использовали ресурсы инфраструктуры, такие как зарегистрированные адреса эл. почты, IP-адреса, номера в автономной системе (autonomous system numbers, ASN) и сервера имен (см. рис. 22). По мнению наших исследователей, это еще одно свидетельство в пользу того, что злоумышленники стараются извлечь максимум выгоды из своих инвестиций в новые домены и сохранить ресурсы. Например, один IP-адрес может использоваться несколькими доменами. Таким образом, злоумышленник, выстраивая свою кампанию, может решить вложить средства в небольшое число IP-адресов и в массив доменных имен, а не в серверы, что дороже.

Рис. 22 Многократное использование инфраструктуры вредоносными программами



Источник: Исследование Cisco в области безопасности.

Ресурсы, которые повторно используют домены RLD, имеют некоторые признаки, по которым можно определить вероятность того, что домен является вредоносным. Например, повторное использование зарегистрированных адресов эл. почты или IP-адресов происходит нечасто, поэтому такой характер повторного использования с той или другой стороны может говорить о подозрительном поведении. Защитники с большей уверенностью смогут блокировать такие домены, зная, что это, вероятно, не скажется отрицательно на деятельности предприятия.

Статическое блокирование номеров ASN и серверов имен в большинстве случаев вряд ли целесообразно. Однако характер повторного использования доменов RLD может говорить о необходимости дальнейшего расследования и принятия решения о блокировке определенных доменов.

Использование аналитических инструментов облачной безопасности первой линии защиты для идентификации и анализа потенциально вредоносных доменов и поддоменов позволяет специалистам по безопасности напасть на след злоумышленника и ответить на такие вопросы, как:

- Какой IP-адрес разрешает этот домен?
- Какой номер ASN связан с этим IP-адресом?
- Кто зарегистрировал домен?
- Какие другие домены связаны с этим доменом?

Ответы на эти вопросы помогут защитникам не только усовершенствовать политики безопасности и блокировать атаки, но также предотвратят подключение пользователей к вредоносным ресурсам в Интернете, когда они находятся в корпоративной сети.

Технологии интеграции разработки и эксплуатации (DevOps) подвергаются риску атак программ-вымогателей

В 2017 году стали появляться атаки программ-вымогателей на технологии DevOps; началось все с январской кампании, нацеленной на платформу базы данных с открытым исходным кодом, MongoDB[16]. Злоумышленники зашифровали публичные экземпляры MongoDB и потребовали выкуп в денежной форме за дешифровку ключей и ПО. Вскоре после этого они занялись компрометацией баз данных, например CouchDB и Elasticsearch, с помощью программ-вымогателей, нацеленных на серверы.

Rapid7 – партнер Cisco и поставщик решений по данным безопасности и аналитике. Как объясняют исследователи Rapid7 в нашем *Отчете Cisco по информационной безопасности за первое полугодие 2017 года*, сервисы DevOps часто разворачиваются неправильно или их намеренно оставляют открытыми для удобства доступа легитимных пользователей – но при этом эти сервисы остаются открытыми и для атак.

Rapid7 регулярно ведет поиск технологий DevOps в Интернете и заносит в каталог как открытые экземпляры, так и экземпляры, требующие выкуп. Некоторые из найденных сервисов DevOps могут содержать данные, идентифицирующие личность (personally identifiable information, PII) на основе имен таблиц, доступных в Интернете.

Чтобы избежать риска подвергнуться атакам на DevOps с требованием выкупа, организации, использующие публичные экземпляры технологий DevOps в Интернете, должны:

- Разрабатывать надежные стандарты для безопасного развертывания технологий DevOps.
- Подробно знать о публичной инфраструктуре, используемой компанией.
- Поддерживать технологии DevOps в актуальном состоянии и вовремя вносить исправления.
- Проводить сканирование уязвимостей.

Более подробную информацию об исследовании Rapid7 см. в разделе «Не позволяйте технологиям интеграции разработки и эксплуатации программного обеспечения делать ваш бизнес уязвимым» в *Cisco 2017 Midyear Cybersecurity Report.*

16 *After MongoDB, Ransomware Groups Hit Exposed Elasticsearch Clusters,* Лучиан Константин (Lucian Constantin), IDG News Service, 13 января 2017 г.: **pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html.**

Внутренние угрозы. Использование преимуществ облака

В прошлых отчетах по информационной безопасности мы обсуждали значение разрешений OAuth и привилегий суперпользователя для определения правил того, кто может входить в сеть и каким образом они могут получать доступ к данным[17].Чтобы еще подробнее изучить, как действия пользователей влияют на информационную безопасность, исследователи угроз из компании Cisco недавно изучили тенденции утечки данных. Они применили алгоритм машинного обучения, чтобы составить профили 150 000 пользователей в 34 странах, пользующихся услугами поставщиков облачных сервисов, с января по июнь 2017 года. Этот алгоритм учитывал не только объем загружаемых документов, но и разные переменные данные, например время загрузки в течение дня, IP-адреса и местоположение.

Профили пользователей составлялись в течение полугода, затем наши исследователи полтора месяца изучали аномалии, 0,5% пользователей было отмечено как совершающие подозрительные действия по скачиванию программ. Конечно, это небольшой процент, но всего эти пользователи смогли скачать 3,9 млн документов из корпоративных облачных систем или, в среднем, 5200 документов на пользователя за 1,5 месяца. Из числа этих подозрительных скачиваний 62% приходилось на стандартные рабочие часы, 40% происходило по выходным.

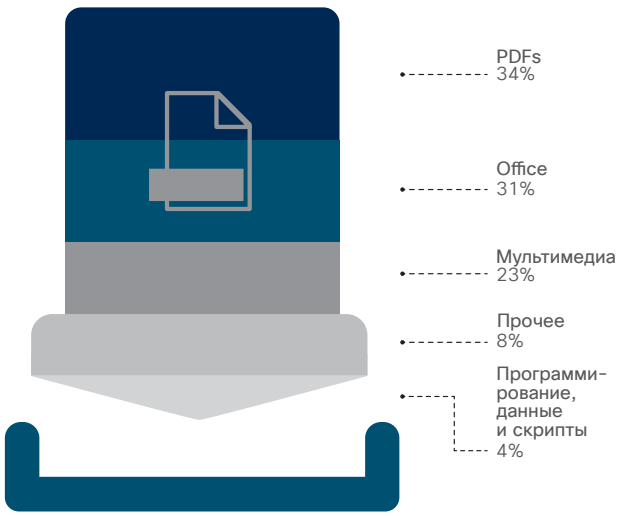
Кроме того, исследователи Cisco также провели интеллектуальный анализ текста, изучив названия 3,9 млн документов, скачивание которых вызвало подозрения.

Одним из самых популярных ключевых слов в названиях документов было слово «данные». Чаще всего рядом со словом «данные» появлялись ключевые слова «сотрудник» и «заказчик». Что касается типов скачиваемых документов, то 34% составляли PDF-файлы и 31% – документы Microsoft Office (см. рис. 23).

Применение алгоритмов машинного обучения позволяет получить более подробное представление об облачной активности пользователей, а не только число скачиваний. В нашем анализе 23% из проанализированных нами пользователей было замечено в том, что они совершали подозрительные действия по скачиванию более трех раз, обычно начиная с небольшого числа документов. С каждым разом объем постепенно увеличивался, и наконец, у таких пользователей отмечался внезапный и значительный всплеск скачиваний (рис. 24).

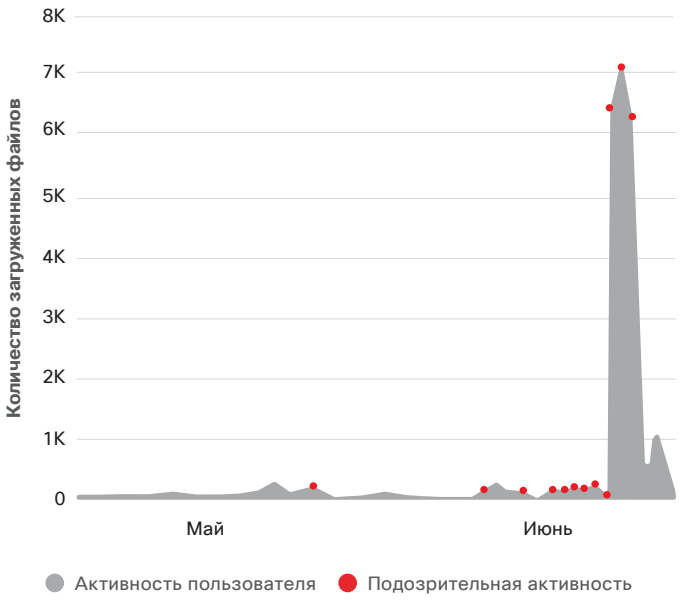
Алгоритмы машинного обучения действительно способны обеспечить лучший мониторинг облака и поведения пользователя в нем. Если защитники начнут прогнозировать поведение пользователей в плане скачивания документов, они сэкономят время, которое можно будет потратить на изучение легитимного поведения. Они также смогут предотвратить потенциальную атаку или инцидент с утечкой данных до того, как это произойдет.

Рис. 23 Самые часто загружаемые документы



Источник: Исследование Cisco в области безопасности.

Рис. 24 Алгоритмы машинного обучения записывают подозрительное поведение пользователей при загрузке файлов



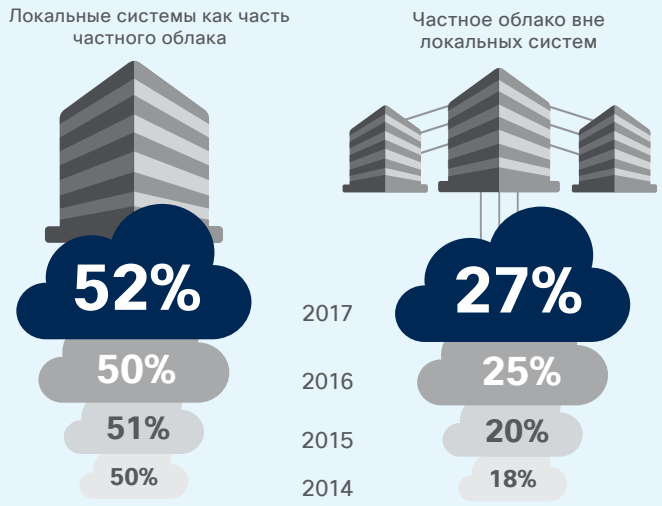
Источник: Исследование Cisco в области безопасности.

17 *Отчет Cisco по информационной безопасности за первую половину 2017 года*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Сравнительное исследование возможностей в области информационной безопасности, проведенное Cisco в 2018 году. Безопасность рассматривается как ключевое преимущество размещения сетей в облаке

Согласно Сравнительному исследованию Cisco решений безопасности в 2018 году, объем использования инфраструктур локальных и публичных облаков растет, хотя многие организации все еще используют локальные сети. В исследовании 2017 года 27% опрошенных специалистов по безопасности сказали, что используют внешние частные облака, в то время как в 2016 году их доля составляла 25%, а в 2015 – 20% (рис. 25). Пятьдесят два процента сообщили, что их сети размещены на локальном частном облаке.

Рис. 25 Большинство организаций используют частные облака



2014 (n=1727), 2015 (n=2417), 2016 (n=2887), 2017 (n=3625)

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Из организаций, использующих облака, 36% размещают в облаке 25–49 процентов своей инфраструктуры, а 35% размещают в облаке 50–74 процента своей инфраструктуры (рис. 26).

Специалисты по безопасности чаще всего называют безопасность как ключевое преимущество размещения сетей в облаке. Из них 57% говорят, что размещают сети в облаке из-за более высокого уровня защиты данных; 48% – из-за масштабируемости, а 46% – из-за удобства использования (см. рис. 27).

Также участники исследования говорят, что по мере перемещения инфраструктуры в облако они начинают рассматривать использование облачных брокеров защиты доступа (cloud access security brokers, CASB) для повышения безопасности облачных сред.

Рис. 26 Пятьдесят три процента организаций держат в облаке не менее половины своей инфраструктуры

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Рис. 27 Пятьдесят семь процентов считают, что облако обеспечивает лучший уровень защиты данных

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

IoT И DDoS-АТАКИ

Интернет вещей (IoT) еще только начинает развиваться, но злоумышленники уже используют недостатки в системах безопасности IoT-устройств, чтобы получить доступ к системам, включая системы промышленного управления, поддерживающие критически важную инфраструктуру. Ботнеты IoT также набирают силу, увеличиваются в размерах и все больше способны запускать мощнейшие атаки, которые могут существенно сказываться на работе Интернета. То, что злоумышленники все больше обращают внимание на уровень приложений, свидетельствует о том, что это и есть их цель. Однако многие профессионалы в области информационной безопасности не осознают или не обращают внимания на угрозу, которую представляют собой ботнеты IoT. Организации продолжают добавлять в свои ИТ-среды IoT-устройства практически не задумываясь о безопасности, и даже более того, не тратя время на оценку того, сколько IoT-устройств связано с их сетями. Таким образом они облегчают злоумышленникам задачу овладения Интернетом вещей.

Немногие организации рассматривают ботнеты IoT как неизбежную угрозу – но они должны быть к этому готовы

По мере расширения и развития IoT, расширяются и развиваются и ботнеты IoT. Чем более сильными и зрелыми становятся ботнеты, тем чаще злоумышленники начинают использовать их для запуска все более масштабных и интенсивных DDoS-атак. В *Отчете Cisco по информационной безопасности за 2017 год* компания Radware, партнер Cisco, предлагает анализ трех крупнейших ботнетов IoT – Mirai, Brickerbot и Hajime – и вновь обращается к теме ботнетов IoT в нашем последнем отчете, чтобы подчеркнуть серьезность этой угрозы[18]. Их исследование показывает, что только 13% организаций считает, что ботнеты IoT станут главной угрозой для их бизнеса в 2018 году.

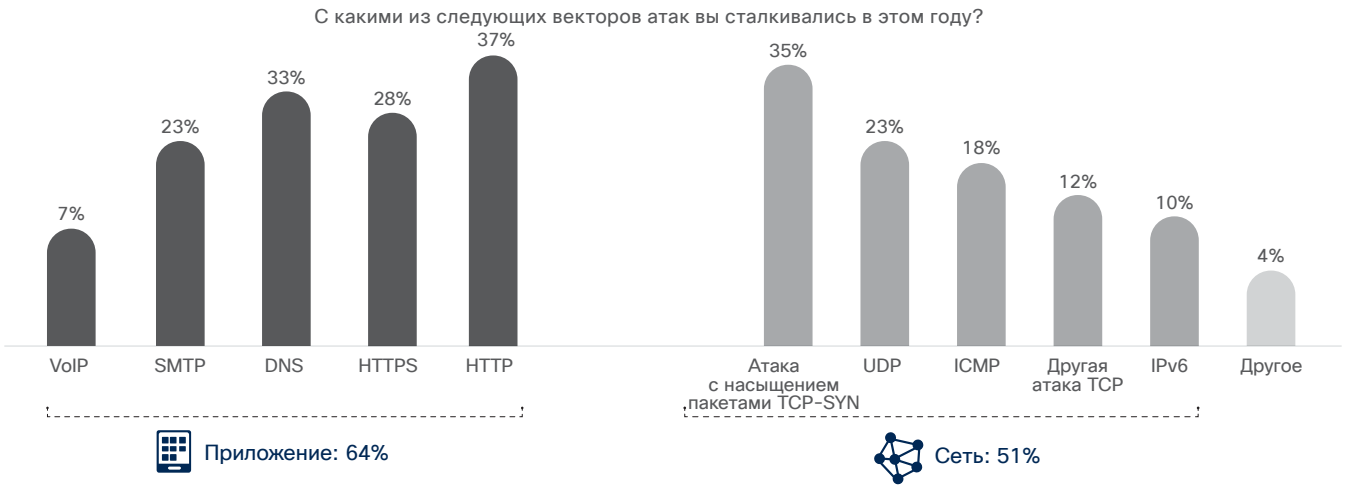
Ботнеты IoT успешно процветают, потому что организации и пользователи развертывают недорогие IoT-устройства быстро и практически не задумываясь о безопасности. IoT-устройства работают под управлением систем Linux и Unix, поэтому они часто становятся целями двоичных кодов формата выполняемого и компонуемого модуля (executable and linkable format, ELF). Их также проще взять под контроль, чем ПК, поэтому злоумышленники легко и быстро могут создать большую армию из этих устройств.

IoT-устройства работают круглосуточно и могут быть введены в действие для выполнения вредоносной активности практически моментально. А по мере того как злоумышленники увеличивают размер своих ботнетов IoT, они инвестируют во все более сложные коды и вредоносное ПО, что позволяет им организовывать еще более усовершенствованные DDoS-атаки.

DDoS-атаки на приложения обходят сетевые DDoS-атаки

Число атак уровня приложений растет, тогда как число атак сетевого уровня снижается (см. рис. 28). Исследователи Radware считают, что такое изменение может быть связано с ростом ботнетов IoT. Эта тенденция настораживает: уровень приложений слишком многообразен, в нем множество устройств, поэтому атаки, нацеленные на этот уровень, потенциально могут вывести из строя большую часть Интернета.

Рис. 28 Количество DDoS-атак на приложения выросло в 2017 г.



Источник: Radware.

18 Более подробную информацию об исследовании ботнетов Radware можно найти в разделе «Интернет вещей еще только появляется, а ботнеты IoT уже здесь», стр. 39, *Отчет Cisco по информационной безопасности за первую половину 2017 года*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

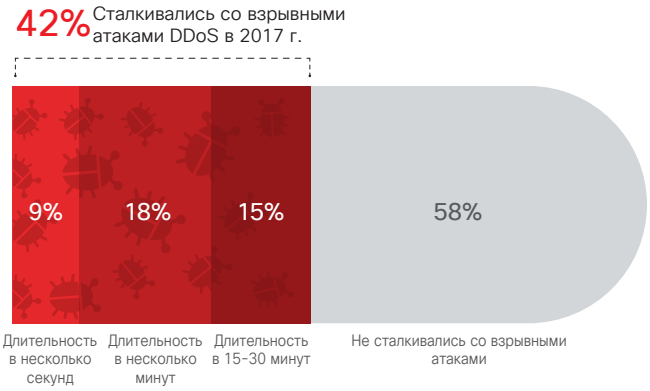
По мнению исследователей Radware, все больше злоумышленников обращается к уровню приложений, так как на сетевом уровне осталось мало доступных «лазеек». Для построения ботнетов IoT также требуется меньше ресурсов, чем для ботнетов из ПК. Таким образом, злоумышленники могут вложить больше ресурсов в разработку сложных кодов и вредоносного ПО. Среди злоумышленников, делающих такого рода вложения, операторы многовекторного ботнета Mirai, известного своими сложными атаками на приложения.

Рост сложности, частоты и продолжительности «взрывных атак»

Одной из наиболее значительных тенденций в DDoS-атаках в 2017 году Radware называет увеличение коротких, взрывных атак, которые становятся более сложными, частыми и устойчивыми. В исследовании Radware сообщается, что в 2017 году такого рода DDoS-атакам подверглось 42% организаций (рис. 29). В большинстве атак повторные вспышки длились всего несколько минут.

Взрывные тактики обычно нацелены на игровые веб-сайты и операторов связи, так как для них особенно важна доступность их

Рис. 29 Опыт с повторяющимися волнами DDoS-атак



Источник: Radware

услуг и они не могут успешно сдерживать маневры таких атак. Периодические или случайные вспышки высокой интенсивности трафика в течение нескольких дней или недель могут привести к тому, что такие организации не будут успевать реагировать на них, и, соответственно, это приведет к прерыванию оказания ими услуг.

Исследователи Radware характеризуют взрывные атаки следующим образом:

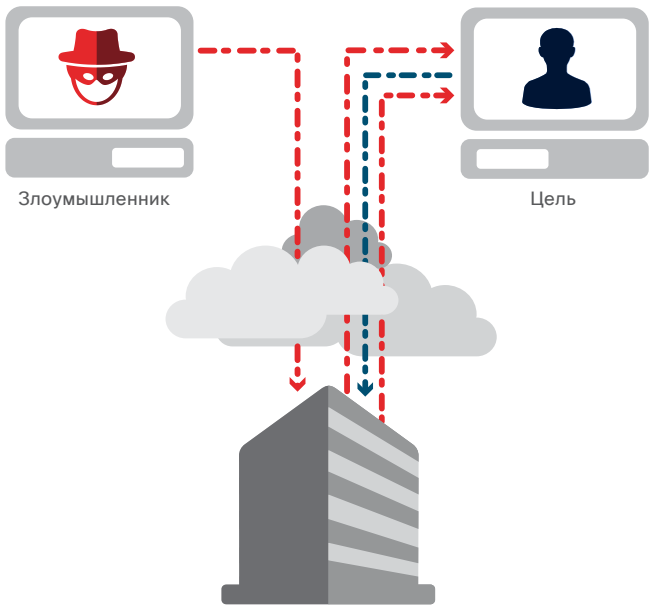
- Эти атаки состоят из множества меняющихся векторов. Эти атаки географически распределены и проявляются непрерывной серией точных и объемных синхронных атак SYN-флуд, ACK-флуд и флуд-атак протокола UDP на множество портов.
- Объединяют атаки большого объема с разной продолжительностью – от 2 до 50 секунд с высокой, взрывной интенсивностью трафика с интервалами примерно по 5–15 минут.
- Часто применяются вместе с другими продолжительными DDoS-атаками.

Рост отраженных DDoS-атак с усилением

Еще одной тенденцией в DDoS-атаках, наблюдаемой исследователями Radware в 2017 году, стал рост отраженных DDoS-атак с усилением как основного вектора, направленного на широкий спектр сервисов. Согласно данным Radware, в 2017 году два из пяти предприятий подверглись отраженной DDoS-атаке с усилением. Одна треть этих организаций не смогла нейтрализовать эти атаки.

В отраженной DDoS-атаке с усилением для отправки трафика атаки на цель используется потенциально легитимный компонент третьей стороны, чтобы скрыть личность злоумышленника. Злоумышленники отправляют пакеты на отражающие сервера с IP-адресом источника, установленным на IP-адрес целевого пользователя. Тем самым они могут косвенным образом переполнить цель ответными пакетами и затруднить ей использование своих ресурсов (см. рис. 30).

Рис. 30 Отраженная DDoS-атака с усилением



Источник: Radware

Для успешного выполнения отраженной DDoS-атаки с усилением необходимо, чтобы пропускная способность полосы частот злоумышленника была больше, чем у его цели. И это становится возможным благодаря отражающим серверам: злоумышленник просто отражает трафик с одной или нескольких машин третьей стороны. Так как это обычные серверы, атаки такого типа обычно сложно нейтрализовать. Стандартные примеры:

Отраженная DNS-атака с усилением
Эта сложная атака типа «отказ в обслуживании» использует преимущества поведения DNS-сервера для усиления атаки. Стандартный DNS-запрос меньше, чем DNS-ответ. В отраженной DNS-атаке с усилением злоумышленник тщательно отбирает DNS-запрос, для которого потребовался бы длинный ответ, например в 80 раз длиннее, чем сам запрос (например, ANY). Злоумышленник отправляет этот запрос, используя ботнет, на DNS-сервера третьей стороны, подменяя IP-адрес источника IP-адресом целевого пользователя. DNS-сервера третьей стороны отправляют свои ответы на целевой IP-адрес. С помощью такого рода техники относительно небольшой ботнет может передавать огромный поток больших ответов на цель.

Отражение через протокол NTP
Такой тип атаки с усилением использует публично доступные сервера сетевого временного протокола (Network Time Protocol, NTP) для переполнения защитников UDP-трафиком и истощения их ресурсов. NTP – это старый сетевой протокол для синхронизации часов между компьютерными системами по сетям с коммутацией пакетов. Он до сих пор широко используется в Интернете настольными компьютерами, серверами и даже телефонами для синхронизации их времени. В нескольких старых версиях серверов NTP есть команда, которая называется monlist: она отправляет запрашивающему лицу список из последних 600 хостов, подключенных к запрашиваемому серверу.

В базовом сценарии злоумышленник постоянно повторно отправляет запрос get monlist на случайный NTP-сервер и фальсифицирует IP-адрес запрашивающего сервера, меняя его на адрес целевого сервера. Затем ответы NTP-сервера направляются на целевой сервер, что вызывает значительное увеличение UDP-трафика с порта источника 123.

Отражение через протокол SSDP
В этой атаке задействуется протокол Simple Service Discovery Protocol (SSDP), который используется для обнаружения подключенных периферийных универсальных устройств Universal-Plug-and-Play (UPnP). Этот протокол также позволяет обнаруживать и управлять сетевыми устройствами и сервисами, такими как камеры, сетевые принтеры и многие другие типы электронного оборудования.

После того как UPnP-устройство подключилось к сети и получило IP-адрес, оно может сообщать о своих сервисах другим компьютерам в сети, отправляя сообщение по IP-адресам многоадресной рассылки. Когда компьютер получает сообщение об обнаружении этого устройства, он делает запрос на полное описание сервисов, предлагаемых устройством. Затем UPnP-устройство отвечает этому компьютеру напрямую и отправляет ему полный список своих сервисов.

В случае с усиленными DDoS-атаками через NTP и DNS, злоумышленник может использовать небольшой ботнет для отправки запроса о сервисах. Злоумышленник затем фальсифицирует IP-адреса источника, т. е. меняет его на IP-адрес целевого пользователя, чтобы направить ответы напрямую на этот целевой адрес.

Защитники должны устранять «пути утечки»

Согласно определению компании Lumeta, партнера Cisco, «путь утечки» – это нарушение политики или сегментации или неавторизованное или неправильно настроенное подключение к Интернету, созданное в корпоративной сети, включая подключение из облака, которое позволяет направлять трафик в какое-либо местоположение в Интернете, например на вредоносный веб-сайт. Такие неожиданные подключения могут также создаваться внутри между двумя разными сегментами сети, которые не должны связываться друг с другом. Так, например, в средах с критически важной инфраструктурой на вредоносную активность может указывать неожиданный путь утечки между ИТ-системами производственного цеха и бизнес-системами. Пути утечки могут также возникнуть из-за неправильно сконфигурированных маршрутизаторов и коммутаторов.

Устройства, у которых неправильно настроены полномочия или которые оставлены открытыми и неуправляемыми, уязвимы для атакующих. Устройства и сети, связанные с посторонними или теневыми ИТ-инфраструктурами, также представляют собой плодородную почву для злоумышленников, на которой они могут проложить пути утечки, так как такие устройства и сети обычно неуправляемые, а исправления в них не вносятся. По оценкам Lumeta, около 40% динамических сетей, оконечных устройств и облачной инфраструктуры на предприятиях представляют собой значительные «слепые зоны» в инфраструктуре, и специалисты по безопасности не владеют информацией о них в реальном времени.

Обнаружение существующих путей утечек очень важно, так как они могут быть использованы в любой момент. Однако также важно обнаружить вновь созданные пути утечки в реальном времени, так как они являются непосредственными индикаторами компрометации и связаны с наиболее сложными, продвинутыми атаками, включая программы-вымогатели.

Недавний анализ ИТ-инфраструктуры, проведенный компанией Lumeta в более чем 200 организациях в нескольких отраслях, свидетельствует о недостаточном мониторинге оконечных устройств. Он показывает, что многие компании значительно недооценивают количество оконечных устройств в их ИТ-средах (см. рис. 31). Часто основной причиной недооценки числа оконечных устройств является недостаточная осведомленность о количестве IoT-устройств с поддержкой IP-адресации, подключенных к сети.

Рис. 31 Обзор «слепых зон» инфраструктуры в различных отраслях

Фактические клиенты Lumeta	Государственные учреждения	Здравоохранение	Технологии	Финансы
Предполагаемые оконечные устройства	150 000	60 000	8000	600 000
Обнаруженные оконечные устройства	170 000	89,860	14 000	1 200 000
Нехватка данных об оконечных устройствах	12%	33%	43%	50%
Неуправляемые сети	3278	24	5	771
Неавторизованные или незащищенные устройства переадресации	520	75	2026	420
Известные, но недоступные сети	33 256	4	16 828	45
Пути утечки в Интернет, обнаруженные при развертывании	3000	120	9400	220

Источник: Lumeta

Исследователи Lumeta предполагают, что путей утечки становится все больше, особенно это касается облачных сред, где мониторинг сети хуже и возможностей для контроля безопасности меньше.

Злоумышленники не всегда немедленно используют созданные ими или найденные пути утечки. Когда они возвращаются к этим каналам, они используют их для установки вредоносных программ или программ-вымогателей, кражи информации и т. д. Исследователи Lumeta говорят о том, что одной из причин, почему пути утечки часто остаются незамеченными, является то, что разработчики угроз достигли высокого мастерства в шифровании и сокрытии своей деятельности, например за счет использования TOR. Они также используют эти пути очень осторожно и рационально, чтобы не вызвать подозрений у сотрудников отделов безопасности.

По словам исследователей Lumeta, нехватка у отдела безопасности необходимых знаний, особенно фундаментальных знаний о сетях, может помешать организациям своевременно расследовать утечки, находить их причины и устранять их. Более тесное взаимодействие между отделом безопасности и сетевым отделом поможет ускорить обнаружение путей утечки и устранить возможные последствия.

Средства автоматизации с сетевым контекстом также дают аналитикам безопасности данные по вероятным причинам утечек. Кроме того, реализация подходящих политик сегментации поможет отделам безопасности быстро определять вредоносный характер неожиданных коммуникаций между сетями или устройствами.

Сравнительное исследование возможностей в области информационной безопасности, проведенное Cisco в 2018 году. Нехватка специалистов в области безопасности мешает многим организациям внедрять новые кибервозможности

Серьезная нехватка персонала остается крупной проблемой для защитников. Как отмечалось выше, недостаток квалификации может помешать организации расследовать и устранять определенные виды угроз.

Без достаточно квалифицированных специалистов защитники не могут развертывать новые технологии и процессы, способные усилить их системы безопасности (рис. 32).

Многие специалисты по безопасности, опрошенные в рамках Сравнительного исследования Cisco решений безопасности в 2018 году, сказали, что в идеале хотели бы автоматизировать или передать на аутсорсинг большинство рутинных задач, чтобы сотрудники могли заниматься более полезной деятельностью.

Рис. 32 Основные возможности, которые добавили бы защитники, если бы имели больше сотрудников

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Download the 2018 graphics at: cisco.com/go/acr2018graphics

Уязвимые места промышленных систем управления создают риски для критически важных инфраструктур

Промышленные системы управления (Industrial control systems, ICS) лежат в основе всех систем управления производством и рабочими процессами. Промышленные системы управления взаимодействуют с другими электронными системами, участвующими в процессе управления, создавая тесно связанную экосистему устройств. Эти устройства уязвимы и представляют собой желанную цель для злоумышленников, так как их легко скомпрометировать.

По данным компании TrapX Security, партнера Cisco, занимающегося защитой от кибератак, основанных на обмане, злоумышленники, желающие использовать промышленные системы управления для вывода из строя критически важной инфраструктуры, активно занимаются исследованиями и создают точки входа для упрощения будущих атак. В число потенциальных злоумышленников входят эксперты с серьезными знаниями ИТ-систем, архитектур промышленных систем управления и поддерживаемых ими процессов. Некоторые из них обладают навыками программирования контроллеров и подсистем управления жизненным циклом продукции (PLM).

Исследователи угроз из компании TrapX недавно расследовали ряд кибератак, нацеленных на промышленные системы управления клиентов, чтобы выявить непредвиденные проблемы кибербезопасности промышленных систем управления. Два из описанных ниже инцидентов произошли в 2017 году, и по ним еще ведется расследование.

Цель: Крупная международная компания, занимающаяся очисткой воды и переработкой отходов

Злоумышленники использовали сервер демилитаризованной зоны (ДМЗ) компании в качестве точки входа для взлома внутренней сети. Отдел безопасности получал уведомления от системы обнаружения обманных кибератак, встроенной в сетевую ДМЗ. Эта физическая или логическая подсеть выступает в качестве моста между внутренними сетями и незащищенными сетями (например, Интернетом), обеспечивая защиту внутренней инфраструктуры. Расследование показало следующее:

- Сервер ДМЗ был взломан из-за неправильной настройки, в результате которой были разрешены соединения RDP.
- Сервер был взломан и управление им осуществлялось с нескольких IP-адресов, связанных с группой хактивистов, враждебно относящихся к заводу.
- Из взломанной внутренней сети злоумышленники организовали ряд крупных атак против нескольких других заводов компании.

Цель: Электростанция

В состав критически важных активов этой электростанции входят очень большая инфраструктура промышленных систем управления и необходимые средства диспетчерского управления и сбора данных (SCADA), отвечающие за управление и выполнение процессов. Электростанция является элементом критически важной национальной инфраструктуры и регулируется и находится под контролем национального агентства по безопасности. В связи с этим она считается установкой с высоким уровнем безопасности.

Главный директор по информационной безопасности принял решение использовать обманную систему для защиты стандартных ИТ-ресурсов электростанции от атак с использованием программ-вымогателей. Также эта технология была внедрена в рамках инфраструктуры промышленной системы управления. Вскоре отдел безопасности получил ряд оповещений о взломе систем в инфраструктуре, отвечающей за критически важные операции электростанции. Расследование было начато немедленно и привело к следующим выводам:

- Устройство в сети управления процессами пыталось взаимодействовать с обманными ловушками, которые были замаскированы под контроллеры PLM. Это была активная попытка составить карту контроллеров PLM в сети и понять точный характер работы каждого контроллера.
- В обычной ситуации взломанное устройство должно было бы быть закрыто, однако выполнявший техобслуживание поставщик не закрыл соединение по окончании работ. Из-за этого упущения сеть управления процессами оказалась уязвимой для атак.
- Злоумышленники собирали именно ту информацию, которая могла бы потребоваться для нарушения работы электростанции и нанести серьезный вред.

Рекомендации

Многие взломы промышленных систем управления начинаются с нарушения безопасности уязвимых серверов и вычислительных ресурсов в корпоративной ИТ-сети. Исследователи угроз из компании TrapX рекомендуют организациям принимать следующие меры для снижения рисков и обеспечения единства производственной деятельности в разных подразделениях:

- Проводить проверку поставщиков и систем, контролировать своевременную установку всех исправлений и обновлений. (При отсутствии исправлений следует подумать о переходе на новую технологию.)
- Сократить использование карт памяти USB и дисков DVD.
- Изолировать промышленные системы управления от ИТ-сетей. Не допускать прямые соединения между этими двумя инфраструктурами. Это относится к сетевым соединениям и подключениям ноутбуков и карт памяти.
- Внедрить политики, строго ограничивающие использование промышленных систем управления, допуская их использование только для необходимых операций. Снизить доступность рабочих станций и мониторов промышленных систем управления с доступом во внешний Интернет через браузер. Предполагать, что политики не будут действовать, и разработать соответствующие планы.
- Устанавливать использование паролей по умолчанию в производственной сети и заменять эти пароли. Использовать двухфакторную аутентификацию везде, где это возможно.
- Проверять планы аварийного восстановления после масштабной кибератаки.

Дополнительные примеры можно найти в исследовательском документе TrapX Security, *Anatomy of an Attack: Industrial Control Systems Under Siege.*

Сравнительное исследование возможностей в области информационной безопасности, проведенное Cisco в 2018 году. Ожидаются новые атаки на производственные инфраструктуры и IoT-устройства

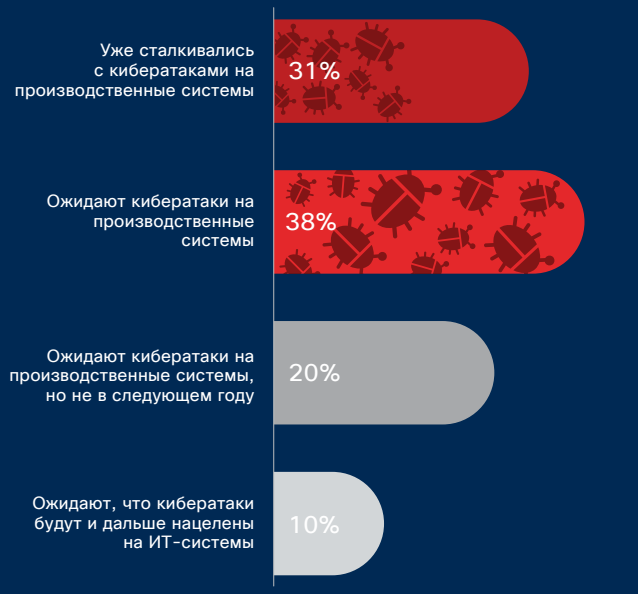
Атаки на операционные инфраструктуры, например на промышленные системы управления, и на IoT-устройства все еще не очень распространены, и многие специалисты по безопасности еще не сталкивались с ними напрямую. Однако, согласно **Сравнительному исследованию Cisco в области безопасности в 2018 году**, специалисты по безопасности ожидают такие атаки и пытаются определить, как реагировать на них.

Специалисты по безопасности понимают, что эти системы обычно слабо защищены и на них используется устаревшее ПО без исправлений, что делает их уязвимыми для атак.

«Мы до сих пор используем устройства старше 25 лет и компрессоры и машины старше 40 лет», – сказал один респондент. «ИТ-специалисты привыкли все планировать. [Они говорят,] " Скажите мне, когда Windows X не будет больше поддерживаться" или " Срок эксплуатации этой версии Oracle подходит к концу" . В производственных инфраструктурах такого нет».

Немногие специалисты по безопасности могут уверенно говорить о проблемах с защитой производственной инфраструктуры своих организаций. Это связано или с тем, что они не обслуживают большого количества производственных систем и не ожидают увеличения их числа, или с тем, что они только недавно внедрили технологии IoT. Из этих специалистов 31% говорят, что их организации уже сталкивались с кибератаками на производственную инфраструктуру, а 38% говорят, что ожидают переход злоумышленников от атак на ИТ-инфраструктуру к атакам на производственную инфраструктуру в течение ближайшего года (рис. 33).

Рис. 33 Тридцать один процент организаций столкнулись с кибератаками на производственную инфраструктуру



Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Download the 2018 graphics at: cisco.com/go/acr2018graphics

УЯЗВИМОСТИ И УСТАНОВКА ИСПРАВЛЕНИЙ

Посреди хаоса проблем безопасности защитники могут упустить из виду некоторые уязвимости используемых технологий. Однако вы можете быть уверены, что злоумышленники обращают внимание на все и рассчитывают использовать возможные слабости в будущих атаках.

Когда-то считалось, что установка исправлений известных уязвимостей в течение 30 дней является оптимальной практикой. Однако такое долгое ожидание может повысить вероятность того, что организация станет целью атаки, поскольку злоумышленники начинают быстрее использовать найденные уязвимости. Организациям также не следует упускать из виду небольшие, но серьезные пробелы безопасности, которые могут принести выгоду злоумышленникам, особенно на этапе разведки, когда злоумышленники ищут пути проникновения в систему.

В число наиболее распространенных уязвимостей в 2017 году вошли ошибки переполнения буфера и уязвимости Apache Struts

Ошибки переполнения буфера заняли верхнюю позицию в списке распространенных уязвимостей Cisco за 2017 год, хотя в других категориях наблюдались изменения. Увеличилось количество уязвимостей на этапе проверки подлинности ввода, а количество уязвимостей из-за ошибок буфера снизилось (рис. 34).

Рис. 34 Активность категорий угроз CWE

Категория угроз	Январь-сентябрь 2016 г.	Январь-сентябрь 2017 г.	Изменение
CWE-119: Ошибки буфера	493	403	(-22%)
CWE-20: Контроль ввода	227	268	+15%
CWE-264: Разрешения, привилегии и доступ	137	163	+18%
CWE-200: Утечка/раскрытие информации	125	250	+100%
CWE-310: Криптографические проблемы	27	17	(-37%)
CWE-78: Внедрение команд ОС	7	15	+114%
CWE-59: Переход по ссылке	5	0	

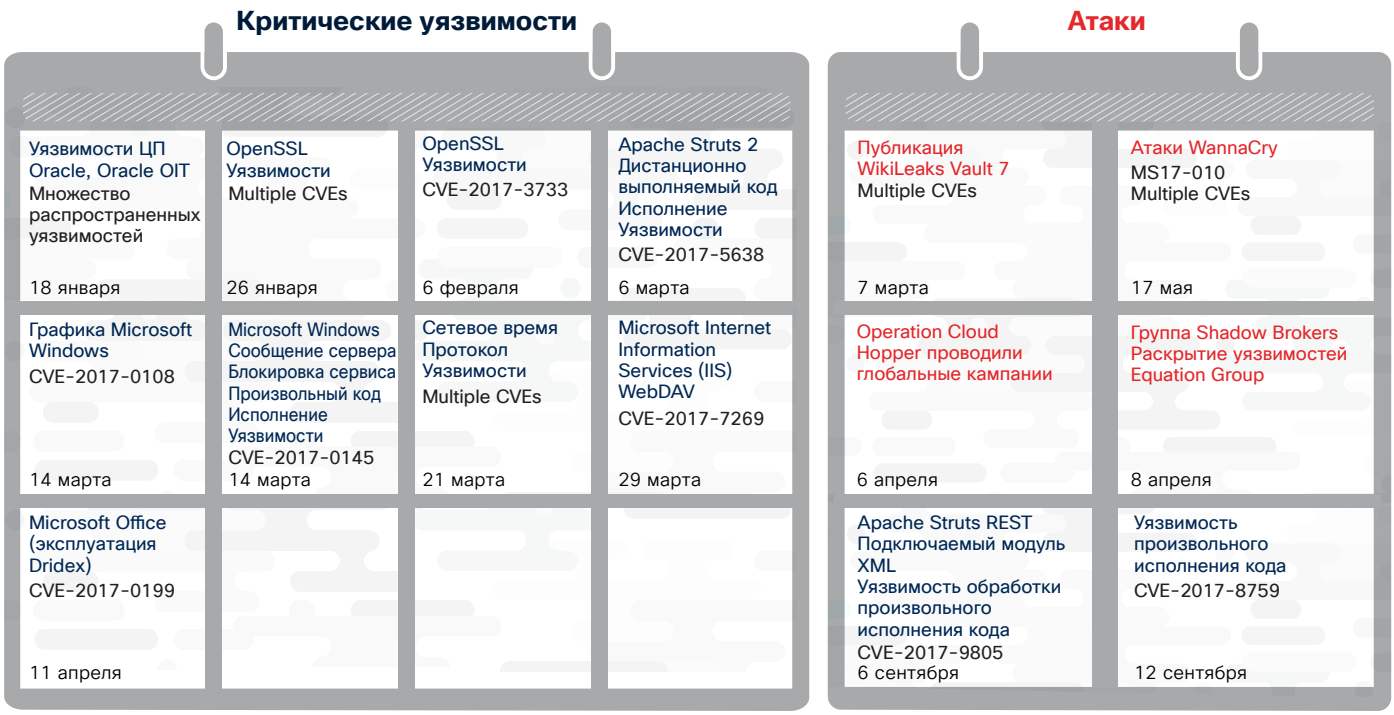
Источник: Исследование Cisco в области безопасности.

Исследование критически важных рекомендаций (рис. 35) показало, что уязвимости Apache Struts продолжали занимать заметное место в 2017 году. Apache Struts – это широко используемая инфраструктура с открытым исходным кодом для создания приложений Java. Уязвимости Apache Struts присутствовали во многих взломанных системах крупнейших брокеров данных в 2017 году.

Хотя в Apache быстро находят уязвимости и выпускают исправления, эти исправления сложно устанавливать на решения сетевой инфраструктуры, такие как Apache Struts, без снижения производительности сети. Как уже говорилось в предыдущих отчетах Cisco по информационной безопасности[19], при обнаружении уязвимостей стороннего ПО или ПО с открытым исходным кодом может потребоваться установка исправлений вручную, а такие операции не получается проводить так же часто, как автоматическую установку исправлений от поставщиков стандартного ПО. Это дает злоумышленникам больше времени для организации атак.

Глубокое сканирование рабочих систем до уровня библиотек и отдельных файлов может помочь организациям составить инвентарные списки компонентов решений с открытым исходным кодом.

Рис. 35 Критически важные рекомендации и действия в ответ на атаки



Источник: Исследование Cisco в области безопасности.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

19 *Отчет Cisco по информационной безопасности за первую половину 2017 года*: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

Число уязвимостей IoT и библиотек в 2017 году выросло

В период с 1 октября 2016 года по 30 сентября 2017 года исследователи угроз Cisco обнаружили 224 новых уязвимости в продуктах других поставщиков. Из них 40 уязвимостей были связаны со сторонними программными библиотеками, используемыми в этих продуктах, а 74 уязвимости были связаны с IoT-устройствами (рис. 36).

Относительно большое число уязвимостей в библиотеках указывает на необходимость более тщательного изучения сторонних решений, лежащих в основе инфраструктуры многих корпоративных сетей. Защитники должны предполагать, что сторонние библиотеки могут оказаться целью злоумышленников. Недостаточно просто использовать самые последние версии программного обеспечения и полагаться на отсутствие распространенных уязвимостей в отчетах. Группы по безопасности должны регулярно проверять наличие исправлений и изучать практики обеспечения безопасности сторонних поставщиков. Например, они могут требовать от поставщиков подтверждения использования защищенного цикла разработки.

Еще одна передовая практика проверки ПО сторонних разработчиков – проверять безопасность функций автоматического обновления и проверки обновлений. Например, при запуске обновления специалисты по безопасности должны быть уверены, что связь с программным обеспечением осуществляется по защищенному каналу (например, SSL) и что программное обеспечение имеет цифровую подпись. Необходимо и то и другое. Если используются только цифровые подписи, но не защищенный канал, злоумышленник может перехватить трафик и заменить обновление старой версией программного обеспечения, которая имеет цифровую подпись, но может содержать уязвимости. Если используется только защищенный канал, злоумышленник может взломать сервер обновлений поставщика и заменить обновление вредоносной программой.

Рис. 36 Сторонние библиотеки и уязвимости IoT

Источник: Исследование Cisco в области безопасности.

Уязвимость к атакам Spectre и Meltdown: проактивная подготовка поможет ускорить восстановление

В январе 2018 года было объявлено об уязвимостях к атакам Spectre и Meltdown, которые позволяют злоумышленникам взломать данные на платформах с процессорами современного поколения. Это вызвало обеспокоенность способностью специалистов по безопасности защитить данные от атак. Уязвимости могут позволить злоумышленникам просматривать данные приложений в памяти на наборе микросхем. Это может нанести серьезный ущерб, поскольку уязвимые микропроцессоры используются везде – от мобильных телефонов до серверного оборудования.

Угрозы уязвимостей Spectre и Meltdown подчеркивают важность взаимодействия с отделами безопасности по поводу решений проблемы, включая установку исправлений, а также обеспечения соблюдения передовых практик устранения проблем безопасности в связи с такими уязвимостями. Рабочие группы по реагированию на инциденты безопасности (например, Cisco PSIRT) создаются для быстрого реагирования на объявления об уязвимостях, разработки патчей и информирования клиентов о том, как предотвращать риски.

При планировании организациям следует учитывать уязвимости перед атаками типа Spectre и Meltdown, а не надеяться, что таких атак не будет. Нужно готовиться к подобным событиям и иметь наготове системы для снижения вероятного ущерба. Например, группам по безопасности следует заблаговременно проводить инвентаризацию устройств, находящихся в их управлении, а также документировать конфигурации используемых функций, поскольку некоторые уязвимости зависят от конфигурации и влияют на безопасность только в случае активации определенных функций.

Группы по безопасности также должны уточнять информацию о процедурах установки обновлений и исправлений у сторонних поставщиков, в том числе у поставщиков облачных решений. Организации должны требовать прозрачной информации о том, как поставщики облачных решений устраняют уязвимости и как быстро они реагируют на оповещения. Однако в конечном итоге вся ответственность за готовность к угрозам лежит на самих организациях. Они должны взаимодействовать с группами PSIRT и подготовить процедуры быстрого реагирования на обнаружение уязвимостей.

Дополнительную информацию можно найти в сообщении в блоге Talos об атаках типа Spectre и Meltdown.

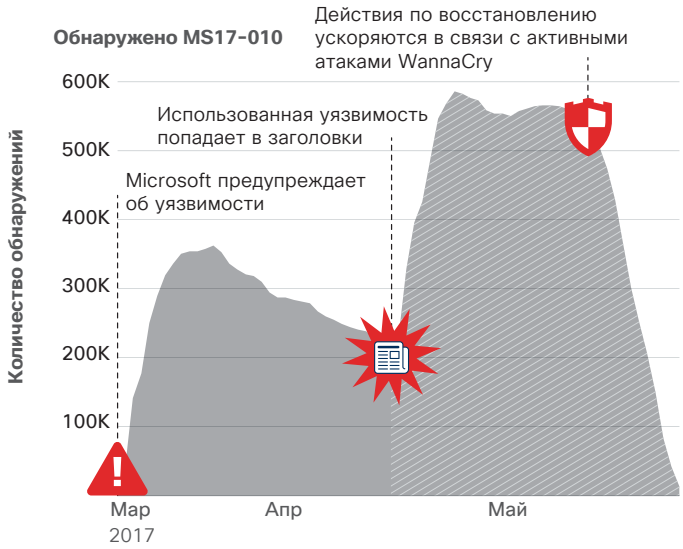
Активные уязвимости требуют срочного устранения, но с IoT-устройствами ситуация обстоит иначе.

Компания Qualys, Inc., партнер Cisco и поставщик облачных решений безопасности и обеспечения соблюдения требований, провела ретроспективное исследование управления установкой исправлений до и после серии атак WannaCry, которым подверглись многие организации по всему миру в мае 2017 года.

Крипточервь-вымогатель WannaCry, который, по мнению многих экспертов по безопасности, был разработан для уничтожения данных, использовал уязвимость безопасности Microsoft Windows под названием EternalBlue, информацию о которой распространила группа хакеров Shadow Brokers в середине апреля 2017 года. (Дополнительную информацию по этой теме можно найти в статье «Они там! В 2018 году защитникам следует готовиться к новым самораспространяющимся сетевым угрозам» на стр. 6.)

14 марта 2017 года корпорация Microsoft выпустила обновление безопасности (MS17-010), предупреждая пользователей о критической уязвимости Microsoft Windows SMB Server. На рис. 37 показан рост количества устройств, в которых была обнаружена уязвимость, а также постепенное снижение этого количества в период с середины марта по середину апреля по мере того, как организации сканировали свои системы и устанавливали исправления.

Рис. 37 Политики установки исправлений до и после серии атак WannaCry



Источник: Qualys

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Однако к середине апреля значительное количество устройств оставалось без исправлений. Затем 14 апреля группа Shadow Brokers выпустила рабочую программу для эксплуатации этой известной уязвимости в различных версиях Microsoft Windows. На рис. 37 показано, что очень скоро количество устройств, где была обнаружена эта уязвимость, практически удвоилось. Это произошло, поскольку организации узнали об уязвимости и о ее влиянии на поддерживаемые и неподдерживаемые версии Windows через удаленную проверку Qualys, в которой использовалась часть кода уязвимости.

Однако даже после публикации информации об уязвимости массовая установка исправлений не началась до середины мая, когда сообщениями об атаке WannaCry пестрели заголовки изданий по всему миру. На рис. 37 показан резкий скачок объема установки исправлений после этой кампании. К концу мая без исправлений осталось лишь небольшое количество устройств.

Проведенное Qualys исследование поведения клиентов в связи с установкой исправлений показывает, что мотивацией для установки исправлений критических уязвимостей может стать только серьезное событие и что даже знания о существовании уязвимости недостаточно, чтобы ускорить устранение. В ситуации с WannaCry у организаций был доступ к исправлениям уязвимости Microsoft в течение двух месяцев, прежде чем начались атаки программ-вымогателей.

Еще один фактор, описанный исследователями Cisco и партнера Qualys, компании Lumeta, был в том, что неизвестные, неуправляемые, случайные и теневые оконечные устройства ИТ-инфраструктуры остались без исправлений. Злоумышленники смогли использовать эти «слепые пятна». Без информации об этих системах средства сканирования уязвимостей не могли оценить их и порекомендовать установку исправлений на этих системах, в результате чего они пали жертвой атак WannaCry.

На IoT-устройства исправления устанавливаются еще медленнее, если устанавливаются вообще

Компания Qualys также изучила тенденции установки исправлений на IoT-устройства. В число рассмотренных устройств вошли системы ОВКВ с поддержкой IP-адресации, дверные замки, панели пожарной сигнализации и устройства чтения карт.

Исследователи специально изучали IoT-устройства, уязвимые для ряда известных угроз, включая вредоносное ПО Devil's Ivy, которое использует уязвимость кода gSOAP, широко используемого в физических системах защиты, а также ботнет Mirai IoT, который подключается к объектам нападения посредством прямых атак на серверы Telnet с использованием метода подбора пароля.

Рис. 38 Тенденции по установке исправлений на IoT-устройства

Источник: Qualys

Всего Qualys изучила 7328 устройств, но исправления были установлены лишь на 1206 из них (см. рис. 38). Это означает, что критические уязвимости сохранились в 83% из исследованных IoT-устройств. Хотя компания Qualys не нашла свидетельств того, что злоумышленники активно нацелились на эти уязвимости, данные организации все равно были уязвимы для атак. Тем не менее, это не мотивировало их ускорить установку исправлений.

По мнению Qualys, существует ряд возможных объяснений медленной установки исправлений. Например, для некоторых устройств возможность обновления может отсутствовать. Другие могут требовать прямой поддержки поставщика. Кроме того, не всегда понятно, кто из сотрудников организации отвечает за обслуживание IoT-устройств. Например, группа инженерного отдела, обслуживающая системы отопления, вентиляции и кондиционирования воздуха, может не знать о рисках информационной безопасности для этой системы и даже не знать о поддержке данной системой IP-адресации.

Еще большее беспокойство вызывает относительно небольшое количество IoT-устройств, обнаруженных Qualys. Фактическое количество таких устройств должно быть намного выше, поскольку организации просто не знают, сколько IoT-устройств подключено к их сети. Такое отсутствие данных создает серьезный риск взлома подобных устройств (дополнительную информацию по этой теме можно найти на стр. 34).

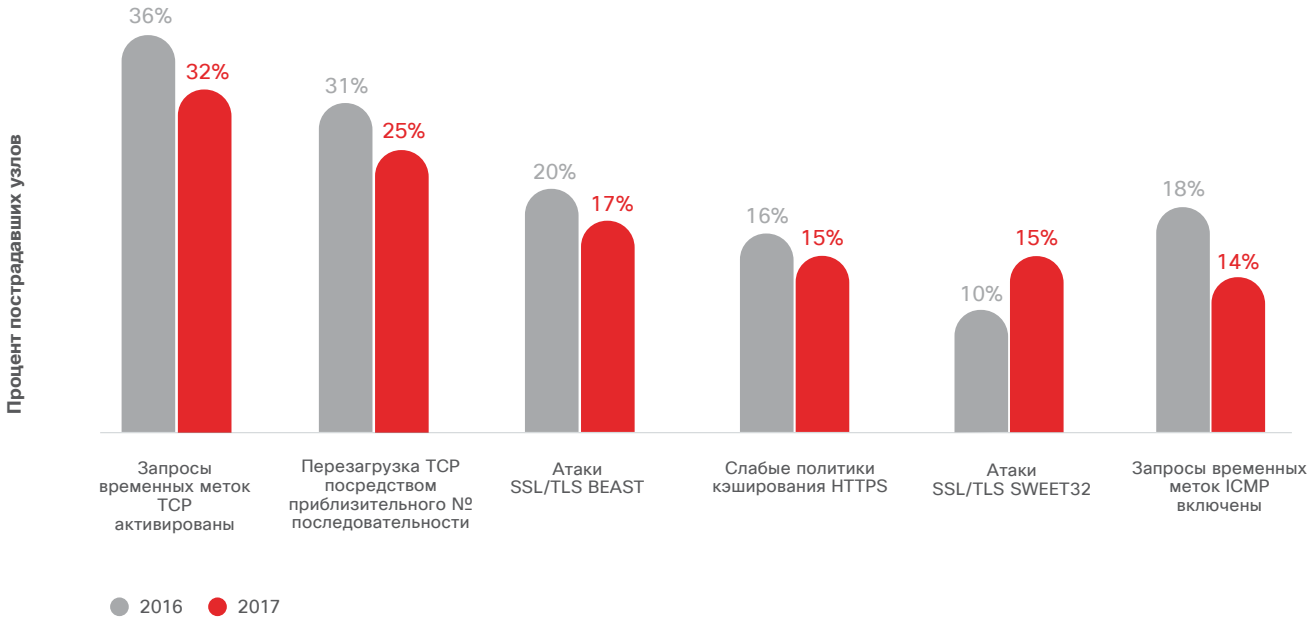
Первый шаг для решения этой проблемы – инвентаризация всех присутствующих в сети IoT-устройств. После инвентаризации организации могут определить возможность сканирования устройств, наличие поддержки со стороны поставщиков и конкретных сотрудников компании, которые отвечают за эти IoT-устройства и используют их. Также организации смогут повысить безопасность инфраструктуры IoT, рассматривая все IoT-устройства как другие вычислительные устройства. В частности, следует обеспечить регулярную установку обновлений микропрограммного обеспечения и исправлений.

Большинство распространенных уязвимостей имеют низкую важность, но высокий риск.

Согласно заключению экспертов по безопасности корпорации SAINT, партнера Cisco, занимающегося решениями по безопасности, уязвимости с низкой важностью часто сохраняются в течение многих лет, поскольку компании не знают об их существовании или не рассматривают их как значительные риски. Однако эти небольшие, но важные упущения в системе защиты могут дать злоумышленникам пути для проникновения в систему.

Исследователи SAINT изучили данные по уязвимостям, собранные с более чем 10 000 хостов в 2016 и 2017 годах. Компания составила список основных уязвимостей, обнаруженных в исследуемых организациях, и этот список показал, что уязвимости низкой важности встречаются чаще всего (см. рис. 39). (Примечание. В некоторых организациях, для которых проводилось исследование, имелось несколько хостов.)

Рис. 39 Чаще всего обнаруживаемые уязвимости с низким уровнем важности, 2016–2017 годы



Источник: Корпорация SAINT.

На рис. 39 представлено три наиболее распространенных уязвимости низкой важности, ниже рассматриваются причины, по которым они могут оказаться ценными для злоумышленников:

Запросы временных меток TCP активированы
Временные метки TCP дают информацию о времени работы машины и времени последней перезагрузки, в результате чего злоумышленники могут узнать, какие уязвимости, для которых имеются исправления, могут присутствовать на данной конкретной машине. Программное обеспечение может использовать временные метки системы для генерации случайных чисел с целью создания ключей шифрования.

Перезагрузка TCP посредством приблизительного номера последовательности
Злоумышленники могут подбирать номера последовательностей и организовывать DoS-атаки против постоянных соединений TCP, непрерывно отправляя пакеты TCP RST, особенно при использовании протоколов с долгосрочными соединениями, например BGP.

Атаки BEAST
Злоумышленник может использовать уязвимость браузера к атакам SSL/TLS (Browser Exploit Against, BEAST) для организации атаки через посредника с целью «считывания» защищенных данных, которыми обмениваются стороны. (Примечание. Это сложная атака, поскольку злоумышленнику также требуется контроль над клиентским браузером для очень быстрого считывания и вставки пакетов данных.)

Во время анализа исследователи безопасности из компании SAINT не обнаружили злоумышленников, активно использующих эти уязвимости низкого уровня важности.

Уязвимости, показанные на рис. 39, известны специалистам по безопасности, но некоторые из них обычно не отмечаются и не требуют автоматических действий при стандартных проверках соблюдения требований, например при проверках соответствия требованиям стандарта безопасности для индустрии платежных карт PCI DSS. В соответствии со стандартами данной отрасли эти уязвимости не считаются критическими. В каждой отрасли важность уязвимостей оценивается по-разному.

Большинство распространенных уязвимостей низкой важности, показанных на рис. 39, нельзя легко устранить или в принципе устранить с помощью управления исправлениями, поскольку они вытекают из проблем с конфигурацией или сертификатами безопасности (например, использование слабых шифров SSL или сертификата SSL с собственной подписью).

Организации должны быстро действовать для устранения уязвимостей низкой важности, которые могут представлять риск. Им следует оценивать и устанавливать приоритеты восстановления в зависимости от их собственного восприятия риска, а не от сторонних рейтингов или системы скоринга (например, от базовых показателей CVSS или рейтинга соответствия требованиям). Только сами организации знают собственные уникальные среды и стратегии управления рисками.

Часть II.
Ландшафт защитников

Часть II. Ландшафт защитников

Мы знаем, что злоумышленники развивают и адаптируют свои методы быстрее, чем защитники. Также они превращают знания об уязвимостях, стратегии обхода и свои навыки в оружие и испытывают их на практике, в результате чего могут организовывать атаки все большего масштаба. Нападение злоумышленников на любую организацию неизбежно, но будут ли готовы к этому ее защитники и как быстро они смогут устранить последствия нападения? Во многом это зависит от того, какие меры они принимают для укрепления своей защиты.

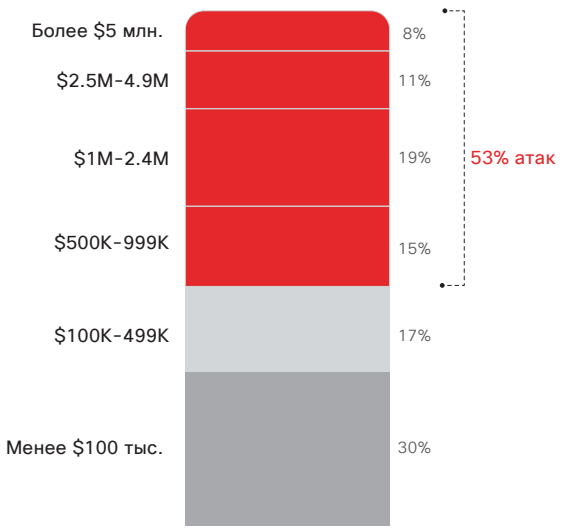
Из **Сравнительного исследования Cisco возможностей в области информационной безопасности за 2018 год** *мы узнали, что перед защитниками стоит большой фронт работ и множество вызовов. Чтобы определить, как защитники оценивают состояние системы безопасности в своих организациях, мы попросили директоров по информационной безопасности (CISOs) и руководителей отделов безопасности (SecOps) из организаций разного размера из нескольких стран оценить свои процедуры и ресурсы безопасности.*

Сравнительное исследование Cisco возможностей в области информационной безопасности, проведенное в 2018 году, позволило определить используемые практики безопасности и сравнить полученные результаты с результатами за 2017, 2016 и 2015 годы. В исследовании участвовали более 3600 респондентов из 26 стран.

Цена атак

Страх перед взломом связан с финансовой стоимостью атак, которая больше не представляет собой гипотетическую цифру. Взломы могут наносить организациям реальный экономический ущерб, на возмещение которого могут уходить месяцы и даже годы. Согласно респондентам, более половины (53%) всех атак привели к финансовому ущербу в размере свыше 500 000 долларов США с учетом упущенной прибыли, потери клиентов, упущенных возможностей, прямых расходов и прочих убытков (рис. 40).

Рис. 40 Пятьдесят три процента атак нанесли ущерб в размере $500 000 или более



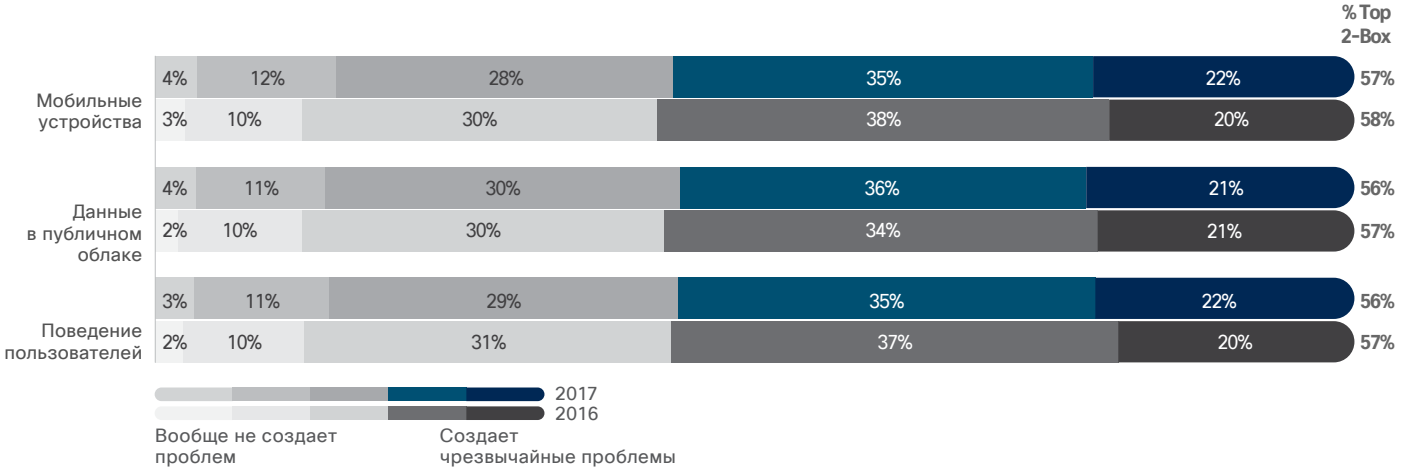
Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Вызовы и препятствия

Перед отделами безопасности, пытающимися защитить свои организации, стоят многие препятствия. Организации должны защищать разные области и функции, что повышает сложность обеспечения безопасности. Самую большую сложность для защиты представляют мобильные устройства, данные в общедоступном облаке и поведение пользователей (рис. 41).

Рис. 41 Наиболее сложные для защиты области: мобильные устройства и данные в облаке

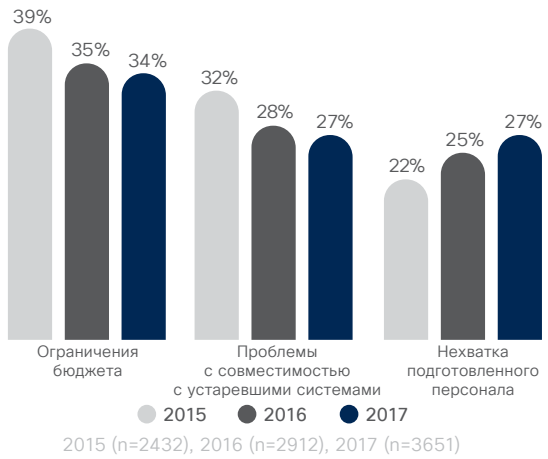


Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Основными ограничениями при управлении безопасностью специалисты называют бюджет, несовместимость и нехватку квалифицированных сотрудников (рис. 42). Отсутствие обученного персонала также ведет к сложностям при внедрении передовых процессов и технологий безопасности. В 2017 году 27% организаций назвали одним из основных препятствий отсутствие талантливых специалистов, по сравнению с 25% в 2016 году и 22% в 2015 году.

Рис. 42 Самое серьезное препятствие обеспечению безопасности: ограничения бюджета



Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Отсутствие талантливых специалистов считается основной проблемой во всех отраслях и во всех регионах. «Если бы я мог по волшебству получить на 10% больше специалистов, чтобы снять часть нагрузки с перегруженных сотрудников, я был бы очень счастлив», – сказал директор по безопасности крупной компании, занимающейся оказанием профессиональных услуг.

Хотя нехватка квалифицированных специалистов остается постоянной проблемой, организации говорят, что они все равно ищут и нанимают дополнительных сотрудников в свои отделы безопасности. В 2017 году в организациях в среднем работало 40 специалистов по безопасности, что значительно выше среднего показателя 2016 года в 33 сотрудника (рис. 43).

Рис. 43 Организации нанимают больше специалистов по безопасности

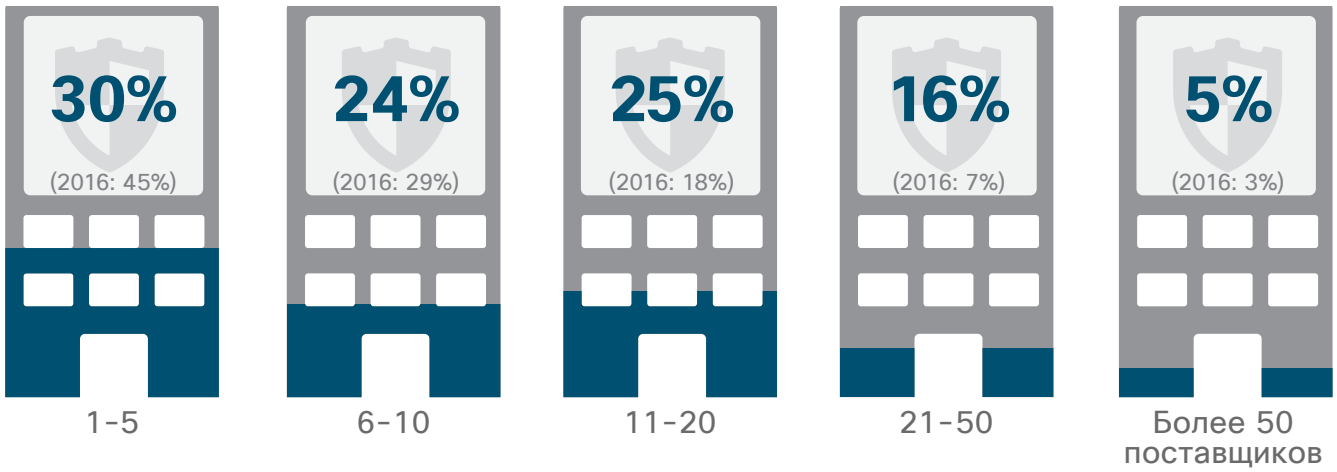
Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Сложности организации работы решений разных поставщиков

Защитники внедряют сложный комплекс решений безопасности различных поставщиков, но эти разнородные инструменты усложняют систему безопасности, а не делают ее более прозрачной. Эти сложности значительно ухудшают способность организаций защищаться от атак, в частности увеличивают риск потерь.

В 2017 году 25% специалистов по безопасности использовали продукты 11–20 поставщиков, в то время как в 2016 году такое количество продуктов безопасности от разных поставщиков использовало лишь 18% таких специалистов. Также в 2017 году 16% специалистов по безопасности использовали продукты 21–50 поставщиков, по сравнению с 7% в 2016 году (рис. 44).

Рис. 44 В 2017 г. организации использовали больше поставщиков решений безопасности



Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

По мере увеличения количества поставщиков повышается сложность управления оповещениями от большого числа разных решений. Как показано на рис. 45, 54% специалистов по безопасности сказали, что управление оповещениями решений разных поставщиков создает некоторые сложности, а 20% назвали эти сложности серьезными.

Рис. 45 Проблема с управлением оповещениями

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

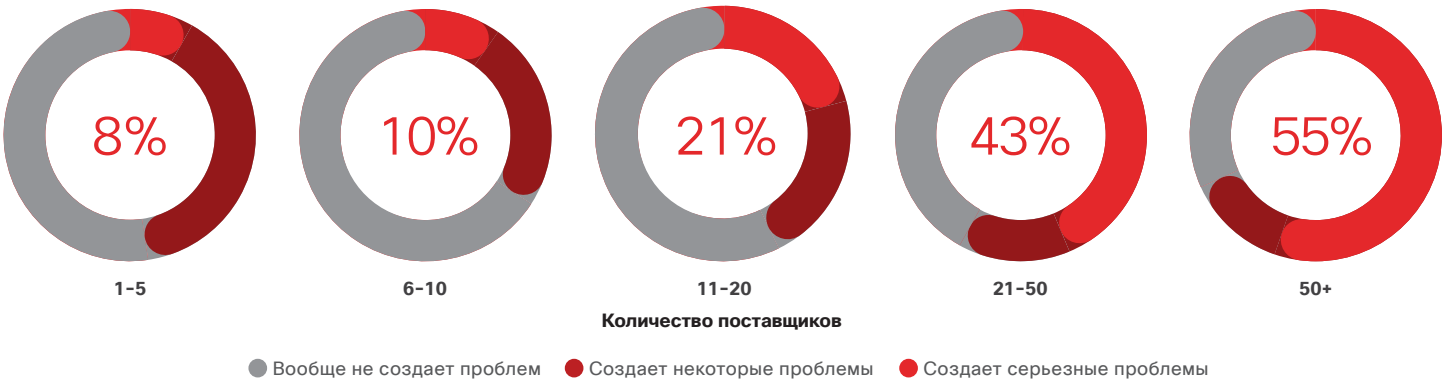
Отделы безопасности сталкиваются со сложностями в управлении оповещениями, получаемыми от решений разных поставщиков

Как видно из рис. 46, среди организаций, использующих решения 1–5 поставщиков, лишь 8% специалистов упомянули серьезные сложности с управлением оповещениями.

Среди организаций, использующих более 50 поставщиков, 55% назвали управление оповещениями очень сложным.

Если организации не могут управлять получаемыми оповещениями и понимать их, через бреши в защите могут просочиться серьезные угрозы.

Рис. 46 По мере увеличения количества поставщиков повышается сложность управления оповещениями безопасности



	Образование	Финансовые услуги	Государственные учреждения	Здравоохранение	Производство	Фармацевтика	Розничная торговля	Телекоммуникации	Транспорт	Коммунальные предприятия/энергетика
Создает серьезные проблемы	17%	24%	16%	42%	14%	25%	19%	14%	12%	27%

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

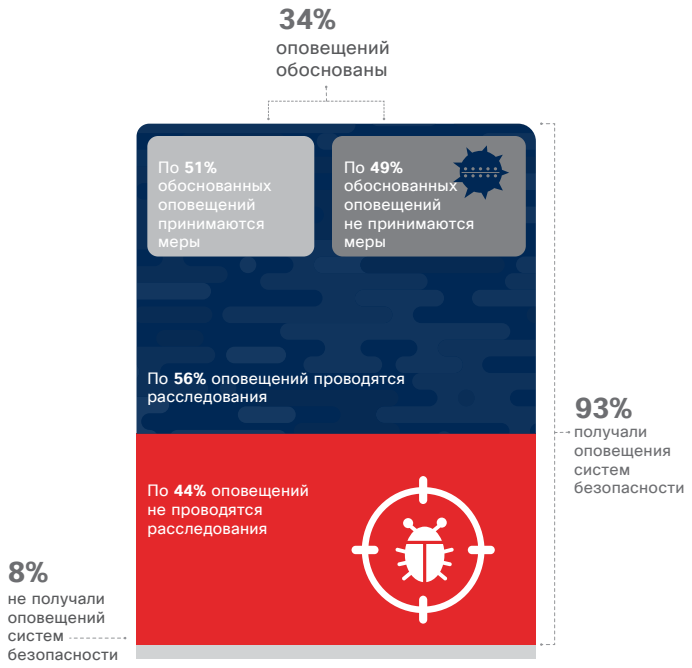
Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

По данным респондентов, существуют разрывы между генерируемыми оповещениями, оповещениями, по которым проводится расследование, и оповещениями, на основе которых устанавливаются исправления. Как показано на рис. 47:

- Среди организаций, получающих ежедневные оповещения по безопасности, в среднем 44% оповещений остаются без расследования.
- Из тех оповещений, по которым проводится расследование, 34% признаются обоснованными.
- По 51% обоснованных оповещений принимаются меры.
- Почти по половине (49%) обоснованных оповещений меры не принимаются.

В результате многие обоснованные оповещения остаются без внимания. Одна из причин этого – нехватка квалифицированных сотрудников, которые могли бы обеспечить расследование всех оповещений.

Рис. 47 Многие оповещения об угрозах не расследуются, или по ним не принимаются никакие меры

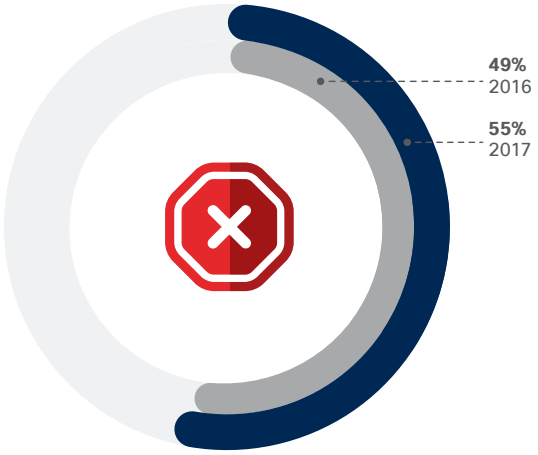


Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Последствия. Внимание общественности в результате нарушений, более высокий риск потерь

«Существует два вида компаний: те, которых взломали, и те, которые не знают, что их взломали», – сказал один из респондентов исследования. (Этот ответ повторяет известное высказывание бывшего генерального директора Cisco Джона Чемберса: «Существует два вида компаний: те, которых взломали хакеры, и те, которые еще не знают, что их взломали».) Хотя организации пытаются ответить на будущие вызовы безопасности и адекватно подготовиться к ним, специалисты по безопасности ожидают, что они падут жертвами взлома, который получит огласку. Пятьдесят пять процентов респондентов сказали, что на протяжении прошлого года их организациям пришлось столкнуться с публичными расследованиями в результате взлома (рис. 48).

Рис. 48 Пятидесяти пяти процентам организаций пришлось столкнуться с публичными расследованиями в результате взлома



2016 (n=2824), 2017 (n=3548)

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

> *«Практически каждая компания из списка Fortune 500 подвергалась взлому в течение последних 24 месяцев. Вы должны быть готовы к этому, особенно с точки зрения маркетинга и связей с общественностью»,*
>
> *– участник исследования.*

Организации сообщили о значительном увеличении количества взломов, повлиявших более чем на 50% систем (рис. 49), по сравнению с предыдущим годом. В 2017 году 32% специалистов по безопасности сообщили о взломах, повлиявших более чем на половину систем, в то время как в 2016 году доля таких взломов составила 15%. Взломы обычно влияют на производство, финансовые операции, интеллектуальную собственность и репутацию бренда (рис. 50).

В средах со сложными системами безопасности взломы происходят чаще. Среди организаций, использующих решения от 1 до 5 поставщиков, 28% утверждают, что им пришлось проводить публичные проверки после взлома; а среди организаций, использующих решения более 50 поставщиков, эта цифра составила 80% (рис. 51). Это может быть связано с более высокой степенью мониторинга угроз за счет большего количества решений.

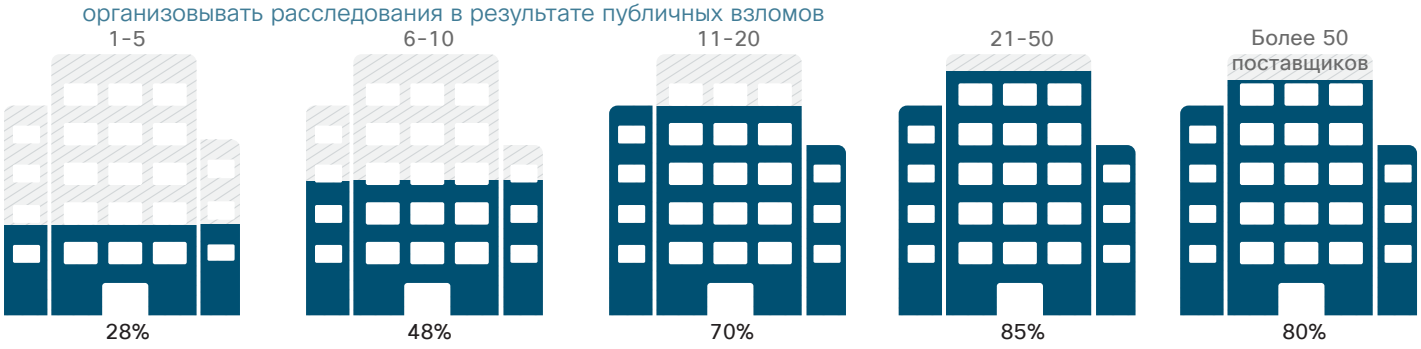
Рис. 49 Значительный рост количества взломов, влияющих на более 50% систем

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Рис. 50 Взломы системы безопасности с наибольшей вероятностью влияют на производственную деятельность и финансы

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Рис. 51 Восемьдесят процентов организаций, использующих решения более 50 поставщиков, были вынуждены организовывать расследования в результате публичных взломов



Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Ценность интегрированной структуры

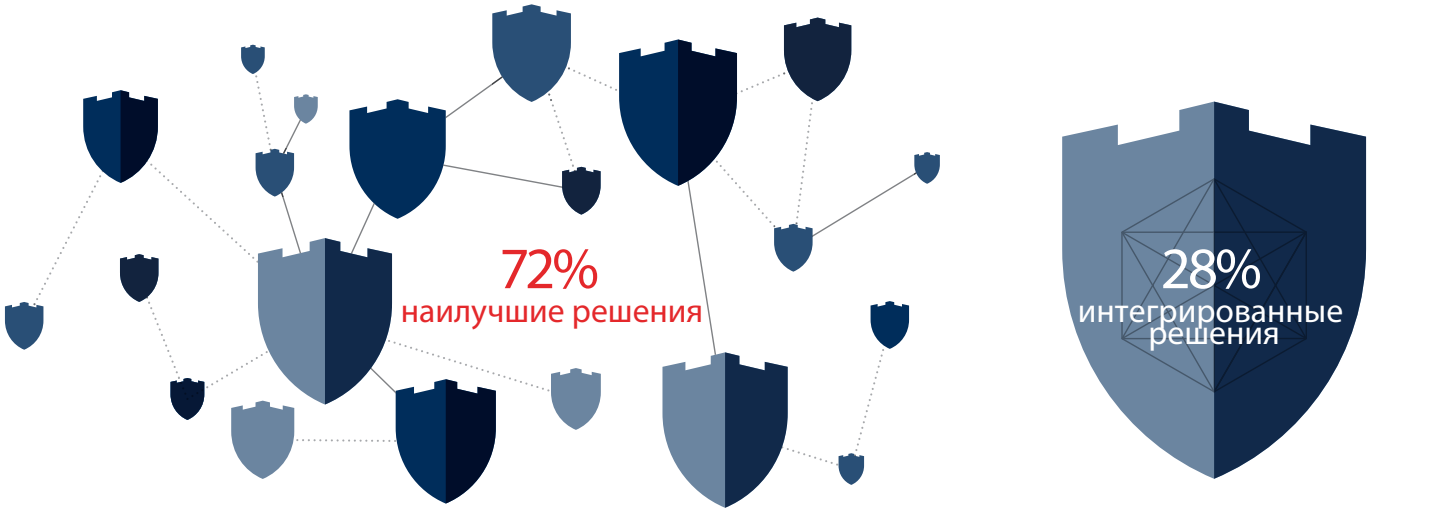
Зачем использовать множество продуктов разных поставщиков, если получающейся средой сложно управлять? Одной из основных причин является подход, основанный на использовании наилучших решений, когда отделы безопасности выбирают наилучшее решение для каждой конкретной задачи. Согласно исследованию, специалисты по безопасности, использующие такой подход, считают его наиболее эффективным с экономической точки зрения.

При сравнении наилучших решений и интегрированных решений, 72% специалистов по безопасности сказали, что приобретают наилучшие точечные решения для конкретных задач, а 28% приобретают продукты, разработанные для работы в качестве интегрированного решения (см. рис. 52). Из организаций, применяющих подход, основанный на использовании наилучших решений, 57% называют в качестве преимущества экономическую эффективность, а 39% говорят, что такой подход проще реализовать.

Интересно, что организации, использующие интегрированные решения, называют примерно такие же причины своего выбора. Пятьдесят шесть процентов говорят, что использование интегрированных решений более эффективно с экономической точки зрения. Сорок семь процентов говорят, что такой подход проще реализовать.

Удобство внедрения все чаще называется в качестве важного фактора при выборе подхода на основе интегрированной архитектуры: в 2016 году простоту внедрения в качестве причины выбора интегрированного подхода назвали 33% организаций, а в 2017 году – 47%. Хотя решения одного поставщика могут быть недостаточно практичными для всех организаций, покупатели решений безопасности должны убедиться в совместимости решений, чтобы снизить риски и повысить эффективность работы.

Рис. 52 Семьдесят два процента организаций приобретают лучшие в своем классе решения, потому что эти решения соответствуют конкретным требованиям



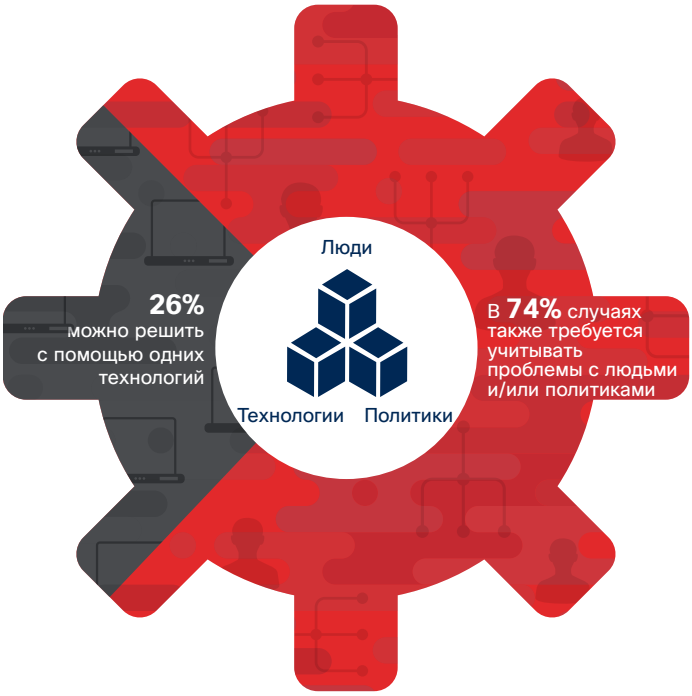
Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Услуги. Работа с людьми, политиками и технологиями

В условиях вероятности потерь и отрицательного воздействия на системы организациям нужно полагаться для защиты не только на технологии. Это означает, что им следует изучить другие возможности повышения безопасности, такие как применение политик и обучение пользователей. Такой комплексный подход к обеспечению безопасности можно увидеть в проблемах, выявленных в исследовании интеллектуальной безопасности Red Team, проведенном консультативной группой по безопасности Cisco Advanced Services.

При изучении рекомендаций на основе нескольких исследований Red Team, проведенных в 2017 году, члены группы услуг определили три ключевых аспекта защиты: люди, политики и технологии. Если организация будет использовать только технологии для устранения уязвимостей безопасности, это позволит решить лишь 26% проблем, выявленных во время симуляций атак Red Team. Таким образом, 74% проблем останутся без решения (см. рис. 53). Если организации будут использовать только политики для решения проблем безопасности, это позволит устранить лишь 10% проблем; а если они будут использовать только обучение пользователей – лишь 4%. Поэтому необходимо контролировать все три аспекта безопасности в совокупности.

Рис. 53 Лишь 26% проблем безопасности можно предотвратить исключительно с помощью программных продуктов



Источник: Исследование Cisco в области безопасности.

На рис. 54 показаны примеры проблем разных категорий, обнаруженных при моделировании атак. Некоторые проблемы, такие как слабые пароли, распространяются на все три категории. Для укрепления паролей может потребоваться обучение пользователей, улучшение продуктов (настройка серверов для использования более сложных паролей) и усиление политик (установка более строгих требований к паролям).

Рис. 54 Типы проблем, обнаруженных при моделировании атак, распределенные по категориям требований к восстановлению

Источник: Исследование Cisco в области безопасности.

Организации могут повысить вероятность успешного управления всеми тремя областями, если обеспечат интеграцию безопасности на всех уровнях организации, а не фрагментарную интеграцию. Также им не следует полагаться исключительно на продукты или технические средства для обеспечения безопасности. Чтобы использование продуктов было успешным, организации должны понимать и применять важные политики и процессы, относящиеся к технологии.

Ожидания. Инвестиции в технологии и обучение

Специалисты в области безопасности ожидают, что организации продолжат сталкиваться со сложными и серьезными угрозами. Они считают, что злоумышленники будут разрабатывать более сложные и разрушительные способы взлома сетей. Также они знают, что на современных рабочих местах возникают благоприятные условия для злоумышленников: Мобильность работников и внедрение IoT-устройств открывают перед злоумышленниками новые возможности. Наряду с ростом угроз, многие специалисты по безопасности ожидают дополнительного внимания со стороны регуляторов, руководства, заинтересованных сторон, партнеров и клиентов.

Чтобы снизить риски и вероятность потерь, защитники должны определить, куда следует инвестировать ограниченные ресурсы. В основном специалисты по безопасности говорят, что бюджеты остаются относительно стабильными, пока серьезный взлом, становящийся достоянием общественности, не приводит к переосмыслению технологий и процессов и соответствующим расходам. Пятьдесят один процент респондентов заявили, что расходы на безопасность основываются на бюджетах предыдущих лет, и примерно столько же назвали в качестве основного фактора при определении бюджета достижение результатов (рис. 55). Большинство руководителей отделов безопасности назвали расходы своих компаний на безопасность адекватными.

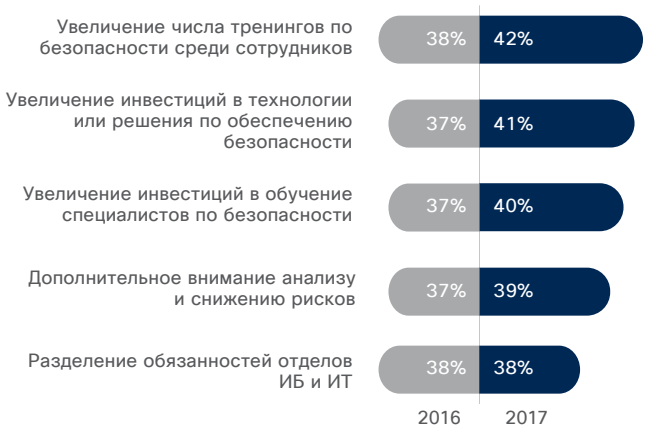
Рис. 55 Пятьдесят один процент респондентов заявили, что размер расходов на безопасность зависит от бюджетов предыдущих лет

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

При планировании бюджета многие компании систематически работают со списками пожеланий, составляемыми в рамках комплексных планов безопасности, и делают приоритетные инвестиции по мере появления ресурсов. Приоритеты могут измениться при обнаружении новых уязвимостей в результате внутренних инцидентов, подвергнувшихся огласке взломов и рутинных оценок риска, проводимых третьими сторонами.

Взломы – это наиболее важные факторы, способствующие будущим инвестициям и соответствующим улучшениям технологий и процессов. В 2017 году 41% специалистов по безопасности назвали взломы систем безопасности движущим фактором увеличения инвестиций в технологии и решения безопасности, в то время как в 2016 году таких специалистов было 37% (рис. 56). Сорок процентов назвали взломы движущим фактором инвестиций в обучение специалистов по безопасности по сравнению с 37% в 2016 году.

Рис. 56 Взломы системы безопасности способствуют инвестициям в технологии и обучение



2016 (n=1375), 2017 (n=1933)

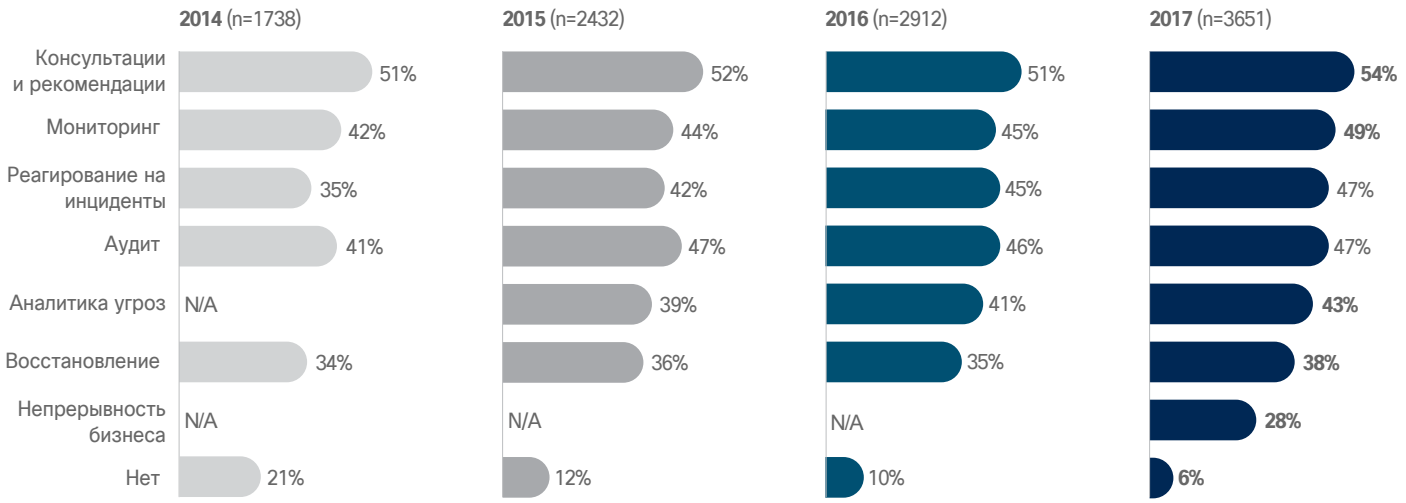
Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Специалисты по безопасности предполагают расходовать больше средств на инструменты, использующие искусственный интеллект и машинное обучение в стремлении укрепить защиту и защитить важные рабочие задачи. Кроме того, они планируют инвестиции в инструменты для защиты критически важных систем, в частности в критически важные инфраструктурные сервисы.

Чтобы более эффективно использовать ресурсы и укрепить защиту, организации начинают больше полагаться на аутсорсинг. 49% специалистов по безопасности сообщили, что использовали аутсорсинг услуг мониторинга в 2017 году, по сравнению с 44% в 2015 году; 47% использовали аутсорсинг реагирования на инциденты в 2017 году, по сравнению с 42% в 2015 году (рис. 57).

Рис. 57 Использование аутсорсинга для мониторинга и реагирования на инциденты растет с каждым годом



Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Дополнительные результаты Сравнительного исследования в области безопасности, проведенного Cisco в 2018 году, приведены в Приложении на **стр. 64**.

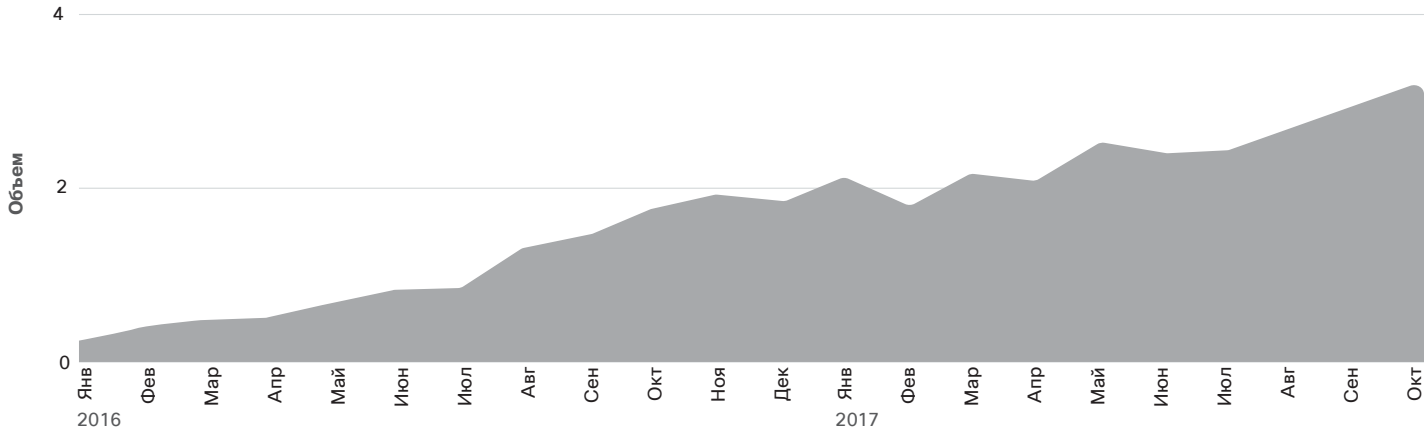
Заключение

Заключение

В современных условиях злоумышленники хорошо умеют избегать обнаружения. Они используют более эффективные инструменты, такие как шифрование, а также более передовую и продвинутую тактику, в том числе злонамеренное использование легитимных интернет-сервисов, чтобы скрывать свою деятельность и подрывать работу традиционных технологий безопасности. Они постоянно развивают свою тактику, чтобы их вредоносное ПО оставалось свежим и эффективным. Идентификация даже тех угроз, которые известны сообществу специалистов по безопасности, может занять длительное время.

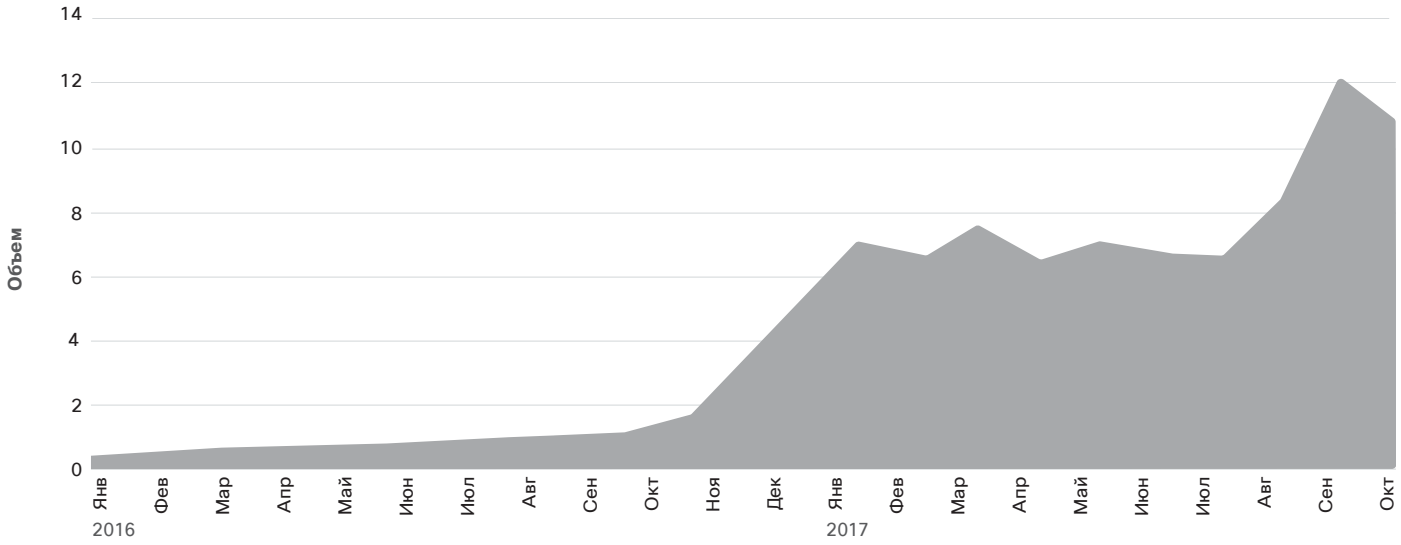
Одна из причин, по которой защитники стремятся подняться над хаосом войны со злоумышленниками и видеть и понимать ситуацию в области угроз, – это огромный объем потенциально вредоносного трафика. Наше исследование показывает, что общий объем событий, наблюдаемый в облачных продуктах Cisco по обеспечению безопасности оконечных устройств, за период с января 2016 года по октябрь 2017 года вырос в четыре раза (см. рис. 58). «Общее количество событий» – это количество всех нормальных и вредоносных событий, обнаруженных нашими облачными продуктами по защите оконечных устройств в течение периода наблюдения.

Рис. 58 Общее количество событий



Источник: Исследование Cisco в области безопасности.

Рис. 59 Общий объем вредоносного ПО



Источник: Исследование Cisco в области безопасности.

За тот же период наши продукты по безопасности зафиксировали одиннадцатикратное увеличение общего объема вредоносного ПО, как показано на рис. 59.

Тенденции роста объемов вредоносного ПО влияют на время обнаружения атак защитниками, что очень важно для любой организации, чтобы определить, как хорошо ее системы защиты работают под давлением постоянного потока вредоносных атак со стороны злоумышленников.

Определенный Cisco средний показатель времени обнаружения в 4,6 часа в период с ноября 2016 года по октябрь 2017 года показывает сложность текущей задачи быстрого определения угроз в хаотичных условиях. Тем не менее, эта цифра значительно меньше среднего времени обнаружения угрозы в 39 часов, которое наблюдалось в ноябре 2015 года, когда мы только начали отслеживать этот показатель, и среднего времени обнаружения угрозы в 14 часов, отмеченного в *Отчете Cisco по информационной безопасности за 2017 год* за период с ноября 2015 года по октябрь 2016 года[20].

Использование облачных технологий безопасности всегда было ключевым фактором, помогавшим Cisco сохранять среднее время обнаружения угрозы на относительно низком уровне. Облачные решения помогают масштабировать инфраструктуру и сохранить производительность в условиях роста общего числа событий и количества оконечных устройств, уязвимых для атак вредоносного ПО. Локальным решениям безопасности сложно обеспечить такую же гибкость. Разработка масштабного решения, способного обработать более чем 10-кратный объем вредоносных событий за двухлетний период с сохранением и увеличением времени реагирования, представляет собой очень сложную и дорогостоящую задачу для любой организации.

Cisco определяет «время обнаружения» как промежуток времени между взломом и идентификацией угрозы. Мы определяем такой промежуток времени, используя телеметрические данные, которые поступают от продуктов обеспечения безопасности Cisco, разворачиваемых по всему миру. Используя наш глобальный мониторинг и модель непрерывного анализа, мы можем проводить измерения с момента загрузки вредоносного файла на оконечное устройство и до момента, когда он определяется как угроза, которая не была классифицирована при ее появлении.

«Среднее время обнаружения» – среднее значение среднемесячных показателей за период наблюдения.

20 *Годовой отчет Cisco по информационной безопасности за 2017 год:* cisco.com/c/m/en_au/products/security/offers/annual-cybersecurity-report-2017.html.

О компании Cisco

О компании Cisco

Компания Cisco создает интеллектуальные системы кибербезопасности для реального мира. Предлагаемый ею комплекс решений является одним из наиболее полных в отрасли и защищает от широкого спектра угроз. Наш подход к информационной безопасности, ориентированный на нейтрализацию угроз и восстановление работоспособности, упрощает систему безопасности, делает ее более цельной, предоставляет возможности детального мониторинга, согласованного управления и усовершенствованной защиты от угроз до, во время и после атаки.

Аналитики угроз из экосистемы коллективной информационной безопасности (CSI) объединяют наиболее полную в отрасли аналитику угроз, данные телеметрии от огромного количества устройств и сенсоров, информацию из общедоступных и частных веб-каналов по уязвимостям, а также от сообщества разработчиков открытого ПО. Ежедневный объем этой информации составляют миллиарды веб-запросов, миллионы сообщений электронной почты, образцов вредоносного ПО и данных о сетевых вторжениях.

Эти данные обрабатываются в развитой инфраструктуре, которая позволяет аналитикам и самообучающимся системам отслеживать угрозы в различных сетях, центрах обработки данных, оконечных и мобильных устройствах, виртуальных системах, веб-сайтах, электронной почте и облачных системах с целью определения основных причин и масштабов распространения угроз. Итоговые данные анализа немедленно распространяются по всему миру среди клиентов Cisco и используются для защиты наших продуктов и сервисов в режиме реального времени.

Дополнительную информацию о нашем ориентированном на предотвращение угроз подходе к обеспечению безопасности можно найти на сайте cisco.com/go/security.

УЧАСТНИКИ ИССЛЕДОВАНИЯ ДЛЯ ГОДОВОГО ОТЧЕТА CISCO ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗА 2018 ГОД

Мы хотим поблагодарить нашу команду исследователей угроз и других экспертов Cisco по этой теме, а также наших технологических партнеров, которые внесли свой вклад в создание **Отчета Cisco по информационной безопасности за 2018 год.** *Их исследования и прогнозы важны для Cisco, чтобы предоставить сообществам специалистов в области безопасности, предприятиям и пользователям информацию о сложности и широте современного глобального ландшафта киберугроз и познакомить их с передовыми методиками для улучшения защиты.*

Наши партнеры по технологиям также играют жизненно важную роль в оказании помощи нашей компании в разработке простой, открытой и автоматизированной системы обеспечения безопасности, которая позволяет организациям интегрировать решения, необходимые для обеспечения безопасности их сред.

Решение Cisco Advanced Malware Protection (AMP) для оконечных устройств

Система защиты Cisco AMP для оконечных устройств сочетает в одном решении автоматизированные функции профилактики и обнаружения угроз и реагирования на угрозы. Она обеспечивает непрерывный мониторинг и анализ признаков вредоносной деятельности для обнаружения атак, проникающих через первую линию обороны и представляющих наибольшую угрозу для организаций. Для быстрого обнаружения и устранения угроз в ней используются разнообразные методики обнаружения, в том числе изолированные системы, профилактика уязвимостей, а также машинное обучение. Cisco AMP для оконечных устройств – единственное решение ретроспективной защиты, позволяющее быстро реагировать на угрозы и определять масштаб угрозы, точку происхождения и способ сдерживания угрозы для защиты организации.

Cisco CloudLock

Cisco Cloudlock предлагает решения брокера безопасности доступа к облачной среде (CASB), помогающие организациям использовать облако безопасным образом. Обеспечивает наглядность и контроль пользователей, данных и приложений для сред «программное обеспечение как услуга» (SaaS), «платформа как услуга» (PaaS) и «инфраструктура как услуга» (IaaS). Также компания обеспечивает полезный анализ кибербезопасности благодаря собственному центру CyberLab со специалистами, а также анализу безопасности по принципу краудсорсинга.

Служба когнитивного анализа угроз Cisco

Служба когнитивного анализа угроз Cisco (Cognitive Threat Analytics, CTA) – это облачная служба, обнаруживающая нарушения безопасности, вредоносное ПО, работающее внутри защищенных сетей, и другие угрозы безопасности путем статистического анализа данных сетевого трафика. Она борется с пробелами в защите периметра, определяя симптомы заражения вредоносным ПО или утечки данных путем поведенческого анализа и выявления аномалий. Когнитивный анализ угроз использует расширенное статистическое моделирование, а также машинное обучение для независимого определения новых угроз, обучаясь и адаптируясь с течением времени.

Группа Cisco по реагированию на проблемы с безопасностью продуктов (PSIRT)

Группа Cisco по реагированию на проблемы с безопасностью продуктов (PSIRT) – специализированная международная группа, занимающаяся сбором, исследованием и публичным распространением информации об уязвимостях и проблемах безопасности, связанных с продуктами и сетями Cisco. Группа PSIRT получает отчеты от независимых исследователей, отраслевых организаций, поставщиков, клиентов и из других источников, обеспокоенных безопасностью продуктов или сетей.

Услуги Cisco по реагированию на инциденты компьютерной безопасности (CSIRS)

Группа Cisco по услугам реагирования на инциденты компьютерной безопасности (CSIRS) состоит из лучших специалистов в этой области, чьей задачей является помогать клиентам Cisco до, во время и после инцидента. CSIRS использует лучший персонал, корпоративные решения безопасности, новейшие методы реагирования и опыт, накопленный за годы борьбы со злоумышленниками, чтобы гарантировать способность наших клиентов предупреждать, а также быстро реагировать и устранять последствия любых атак.

Cisco Talos Intelligence Group

Группа Cisco Talos Intelligence Group – одна из крупнейших в мире групп аналитики коммерческих угроз, в которую входят исследователи, аналитики и инженеры мирового уровня. В их работе им помогают непревзойденные системы телеметрии и комплексного анализа, позволяющие быстро получать точные и полезные аналитические данные об угрозах для клиентов, продуктов и услуг Cisco. Talos Group защищает заказчиков Cisco от известных и новых угроз, находит новые уязвимости в распространенном программном обеспечении и сдерживает угрозы до того, как они могут нанести ущерб глобальному Интернету. Аналитические данные Talos лежат в основе продуктов Cisco, помогая обнаруживать известные и новые угрозы, анализировать их и защищать от них данные. Talos придерживается официальных наборов правил Snort.org, ClamAV и SpamCop, а также выпускает множество средств для исследований и анализа с открытым исходным кодом.

Cisco Threat Grid

Cisco Threat Grid – платформа анализа вредоносного ПО и аналитики угроз. Threat Grid выполняет статический и динамический анализ подозрительных образцов вредоносного ПО, получаемых от заказчиков и из интегрированных продуктов со всего мира. Через пользовательский интерфейс облачного портала Threat Grid или через Threat Grid API в облако Threat Grid ежедневно поступают сотни тысяч образцов самых разнообразных типов. Также возможно развертывание Threat Grid в качестве локального решения.

Cisco Umbrella

Защищенный интернет-шлюз Cisco Umbrella служит первой линией обороны от интернет-угроз независимо от местонахождения пользователей. За счет интеграции с фундаментальными структурами Интернета Umbrella обеспечивает полную прозрачность действий в Интернете всех пользователей на всех устройствах в любой точке и блокирует угрозы еще до того, как они проникнут в сеть или на оконечные устройства. Анализируя шаблоны интернет-трафика и получая полезные данные, Umbrella автоматически выявляет инфраструктуру злоумышленников, подготовленную для активных и планируемых атак, и заранее блокирует запросы к вредоносным узлам до установления соединения.

Исследования и обеспечение безопасности (SR&O)

Группа SR&O отвечает за управление угрозами и уязвимостями всех продуктов и служб Cisco и включает в себя лучшую в отрасли группу реагирования на уязвимости технических решений (Cisco PSIRT). SR&O помогает заказчикам изучить меняющуюся среду угроз на таких мероприятиях, как Cisco Live и Black Hat, а также в процессе совместной работы с коллегами в Cisco и отрасли в целом. Кроме того, SR&O разрабатывает новые службы, например специальную службу анализа угроз (Custom Threat Intelligence, CTI) Cisco, позволяющую определить индикаторы компрометации, которые не были обнаружены или обработаны текущими инфраструктурами безопасности.

Организация информационной безопасности и доверия

Организация информационной безопасности и доверия Cisco подчеркивает наше стремление решить две наиболее критичные проблемы многих советов директоров и мировых лидеров. Основные цели организации – защита публичных и частных заказчиков Cisco, реализация и поддержка безопасного жизненного цикла разработки и благонадежных систем Cisco для всего портфеля продуктов и услуг Cisco, а также защита инфраструктуры Cisco от постоянно развивающихся киберугроз. Cisco применяет всесторонний подход к комплексному обеспечению информационной безопасности и доверия, который объединяет людей, процессы, технологии и политики. Формирование системы информационной безопасности и доверия предназначено для оптимизации информационной безопасности, инжиниринга с учетом безопасности, защиты и конфиденциальности данных, безопасности облачной среды, прозрачности и проверки, расширенных функций безопасности и управления. Дополнительную информацию можно найти на сайте trust.cisco.com.

Отчет Cisco по информационной безопасности за 2018 год. Партнеры по технологиям

ANOMALI®

Набор решений для анализа угроз Anomali позволяет организациям обнаруживать и исследовать активные угрозы кибербезопасности и реагировать на них. Признанная платформа анализа угроз ThreatStream собирает и оптимизирует миллионы индикаторов угроз, составляя «черный список». Anomali интегрируется с внутренней инфраструктурой для выявления новых атак, анализа за прошлый год для обнаружения уже совершенных атак, а также позволяет специалистам в области обеспечения безопасности быстро разобраться в угрозах и сдерживать их. Anomali также предлагает бесплатный инструмент STAXX для сбора и обмена результатами анализа угроз, а также предоставляет бесплатную готовую к использованию ленту аналитики Anomali Limo. Для получения дополнительной информации посетите веб-сайт anomali.com, а также следите за нами в Twitter: @anomali.

LUMETA
DETECT WITH A HIGHER SENSE

Lumeta позволяет группам обеспечения безопасности и управления сетью выявлять киберугрозы и предотвращать вторжения. Lumeta предлагает беспрецедентную возможность находить известные, неизвестные, теневые и подставные элементы сетевой инфраструктуры, превосходящую возможности других существующих решений. Также Lumeta позволяет выполнять мониторинг сети и оконечных устройств в режиме реального времени для обнаружения несанкционированных изменений, предотвращения утечек, правильной сегментации сетей и обнаружения подозрительного поведения для динамических сетей, оконечных устройств, виртуальных машин и облачной инфраструктуры. Дополнительные сведения см. на веб-сайте lumeta.com.

Qualys, Inc. (NASDAQ: QLYS) является пионером и ведущим поставщиком облачных решений обеспечения безопасности и соответствия нормативным требованиям, обслуживая свыше 9300 клиентов более чем в 100 странах, большая часть которых входит в списки Forbes Global 100 и Fortune 100. Облачная платформа Qualys и интегрированный набор решений помогают организациям упростить обеспечение безопасности и снизить затраты на соответствие нормативным требованиям, предоставляя необходимый анализ критически важной инфраструктуры безопасности и автоматизируя все операции аудита, обеспечения соответствия и защиты для ИТ-систем и веб-приложений. Созданная в 1999 году компания Qualys установила стратегические партнерские отношения с ведущими поставщиками административных услуг и консалтинговыми организациями по всему миру. Дополнительные сведения можно найти на сайте qualys.com.

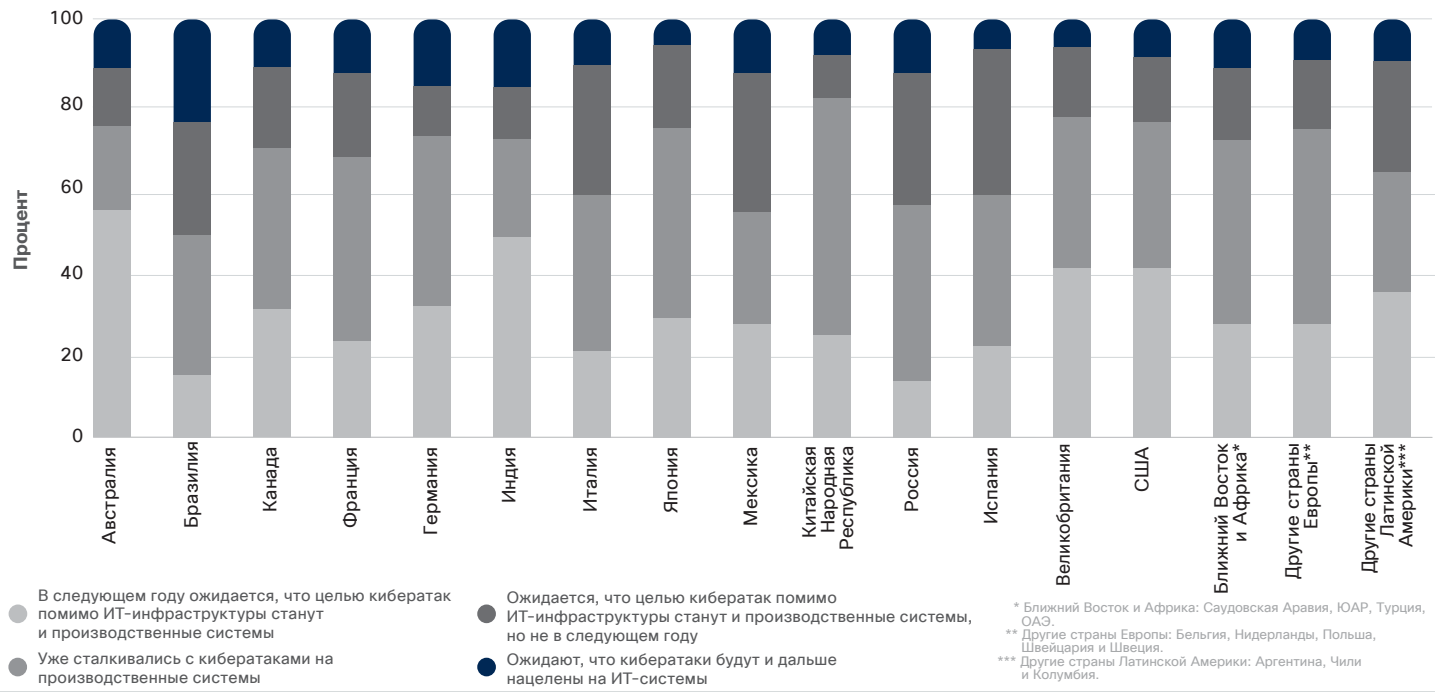
Radware (NASDAQ: RDWR) является глобальным лидером на рынке приложений и решений кибербезопасности для виртуальных, облачных и программно-определяемых центров обработки данных. Ее признанные решения защищают более 10 000 организаций и операторов связи по всему миру. Дополнительные ресурсы и информацию можно найти в онлайн-центре безопасности Radware, содержащем всесторонний анализ инструментов DDoS-атак, тенденций и угроз: security.radware.com.

Корпорация SAINT, лидер в области интегрированных решений управления уязвимостями следующего поколения, помогает компаниям и госучреждениям определять и снижать подверженность рискам на всех уровнях организации. Благодаря SAINT доступ, безопасность и конфиденциальность мирно сосуществуют к выгоде всех заинтересованных сторон. SAINT позволяет клиентам усиливать средства защиты информационной безопасности и при этом снизить совокупную стоимость владения. Для получения дополнительной информации посетите веб-сайт saintcorporation.com.

TrapX Security предлагает автоматизированную защитную сеть для автоматической маскировки и защиты, позволяющую пресекать угрозы в режиме реального времени, одновременно предоставляя имеющую практическую ценность аналитику для блокировки злоумышленников. TrapX DeceptionGrid™ позволяет компаниям обнаруживать, перехватывать и анализировать вредоносное ПО нулевого дня, используемое лучшими в мире группами, осуществляющими APT-атаки. Компании используют TrapX для усиления своей ИТ-экосистемы и снижения рисков приносящих убытки и подрывающих репутацию компрометаций, утечек данных и нарушения нормативных требований. Средства защиты TrapX встраиваются в самое сердце сети и критически важной инфраструктуры, не требуя наличия агентов или настройки. Новейшие методы обнаружения вредоносного ПО, анализа угроз и криминалистической экспертизы в рамках единой платформы помогают снижать сложность и уровень затрат. Дополнительную информацию можно найти на сайте trapx.com.

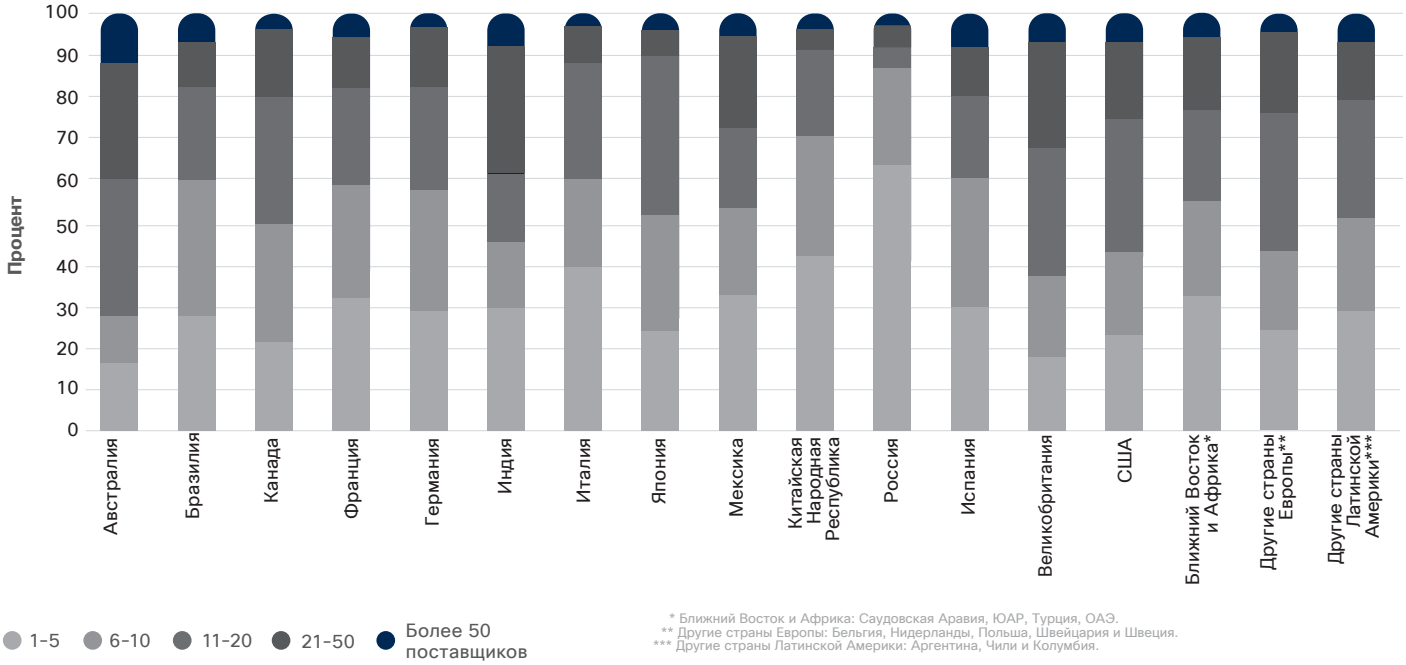
Приложение

Рис. 60 Ожидаемые кибератаки на производственную инфраструктуру и ИТ-инфраструктуру, по странам и регионам



Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

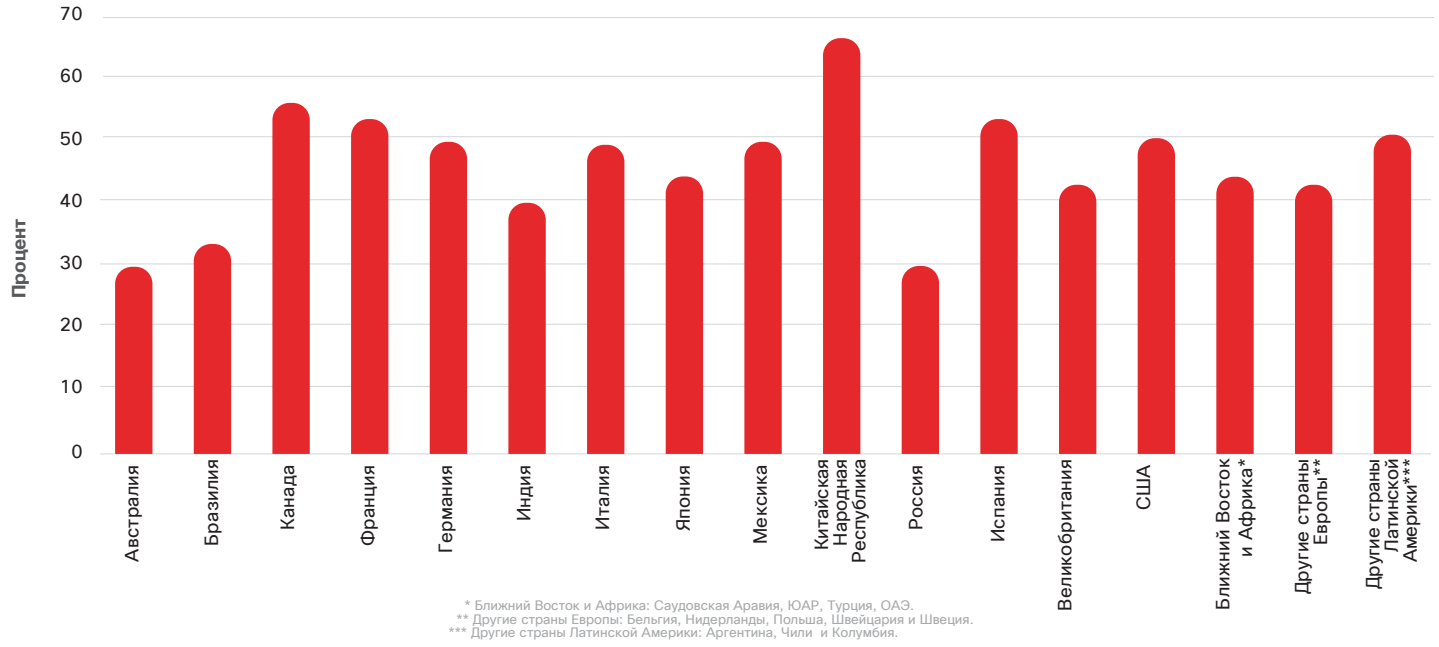
Рис. 61 Количество поставщиков решений безопасности для инфраструктуры, по странам и регионам



Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Рис. 62 Процент оповещений, по которым не проводится расследование, по странам и регионам



* Ближний Восток и Африка: Саудовская Аравия, ЮАР, Турция, ОАЭ.
** Другие страны Европы: Бельгия, Нидерланды, Польша, Швейцария и Швеция.
*** Другие страны Латинской Америки: Аргентина, Чили и Колумбия.

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Рис. 63 Препятствия на пути внедрения современных процессов и технологий обеспечения безопасности, по странам и регионам

Which of the following do you consider the biggest obstacles to adopting advanced security processes and technology?

	Австралия	Бразилия	Канада	Франция	Германия	Индия	Италия	Япония	Мексика	Китайская Народная Республика	Россия	Испания	Великобритания	США	Ближний Восток и Африка*	Другие страны Европы**	Другие страны Латинской Америки***
Ограничения бюджета	23%	35%	29%	33%	25%	36%	38%	31%	31%	38%	60%	33%	27%	34%	36%	37%	35%
Конкурирующие приоритеты	28%	11%	29%	27%	28%	26%	24%	27%	16%	27%	20%	18%	32%	32%	25%	18%	24%
Нехватка подготовленного персонала	25%	28%	19%	22%	24%	31%	24%	28%	30%	25%	35%	33%	31%	26%	25%	23%	26%
Отсутствие знаний о передовых процессах и технологиях безопасности	26%	26%	24%	21%	22%	24%	21%	26%	23%	29%	18%	21%	27%	22%	22%	17%	21%
Проблемы с совместимостью с устаревшими системами	27%	19%	30%	27%	30%	30%	22%	23%	32%	40%	25%	25%	24%	28%	30%	25%	28%
Требования сертификации	33%	27%	29%	29%	24%	27%	27%	22%	27%	23%	22%	27%	27%	30%	24%	33%	21%
Организационная культура и отношение к безопасности	30%	23%	25%	20%	16%	26%	17%	21%	26%	17%	19%	24%	28%	25%	20%	20%	27%
Нежелание совершать покупку до проверки на рынке	19%	20%	23%	26%	25%	29%	20%	28%	15%	16%	17%	20%	21%	22%	22%	21%	25%
Слишком высокая рабочая нагрузка для выполнения новых обязанностей	22%	16%	28%	18%	28%	28%	26%	27%	23%	21%	15%	28%	22%	22%	20%	17%	19%
Организация не является привлекательной целью для атак	25%	18%	21%	22%	24%	17%	14%	20%	12%	16%	11%	13%	21%	21%	21%	20%	16%
Безопасность не является приоритетом для руководства	22%	10%	17%	17%	20%	13%	13%	23%	15%	18%	11%	11%	19%	19%	17%	19%	21%

* Ближний Восток и Африка: Саудовская Аравия, ЮАР, Турция, ОАЭ.
** Другие страны Европы: Бельгия, Нидерланды, Польша, Швейцария и Швеция.
*** Другие страны Латинской Америки: Аргентина, Чили и Колумбия.

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Рис. 64 Закупка решений безопасности, по странам и регионам

Что лучше всего описывает подход вашей организации к приобретению решений для защиты от угроз?

Страна	N=	Обычно приобретаем лучшие решения для конкретных целей	Обычно приобретаем продукты, которые хорошо будут работать вместе
Австралия	203	86	14
Бразилия	197	72	28
Канада	185	67	33
Франция	191	59	41
Германия	195	69	31
Индия	199	78	22
Италия	201	71	29
Япония	223	72	28
Мексика	198	77	23
Китайская Народная Республика	205	63	37
Россия	196	58	42
Испания	148	70	30
Великобритания	194	76	24
США	393	81	19
Ближний Восток и Африка*	249	69	31
Другие страны Европы**	199	73	27
Другие страны Латинской Америки***	196	71	29

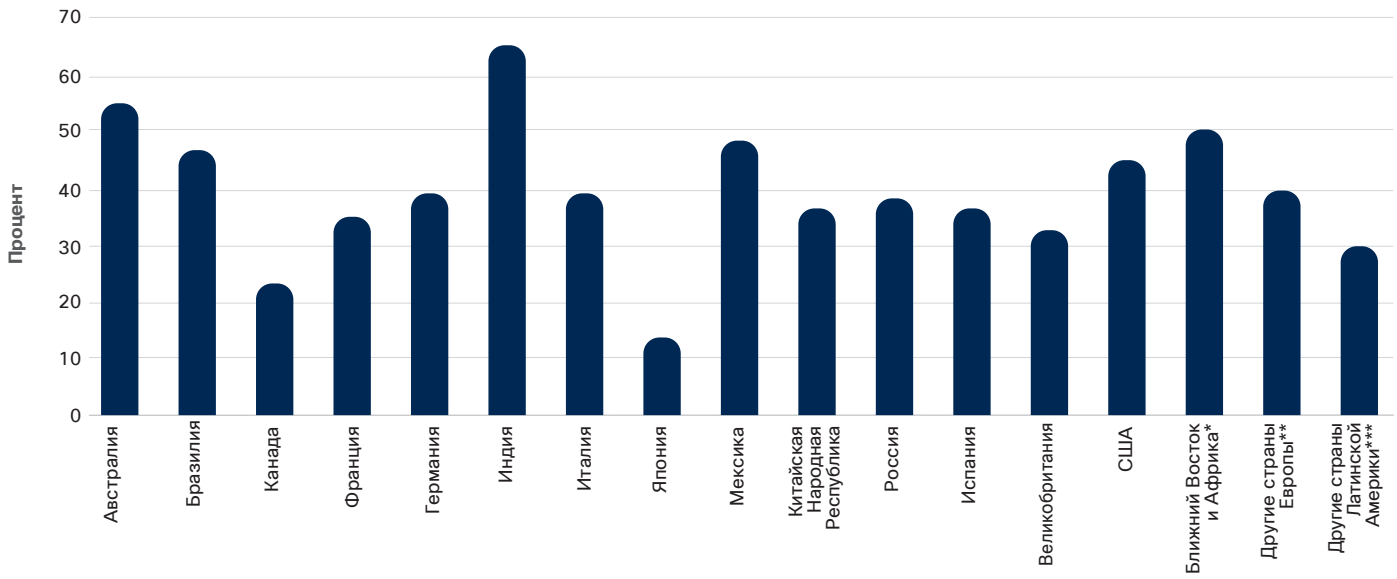
* Ближний Восток и Африка: Саудовская Аравия, ЮАР, Турция, ОАЭ.

** Другие страны Европы: Бельгия, Нидерланды, Польша, Швейцария и Швеция.

*** Другие страны Латинской Америки: Аргентина, Чили и Колумбия.

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Рис. 65 Процент организаций, считающих, что они очень хорошо следуют стандартным практикам информационной безопасности, по странам и регионам



* Ближний Восток и Африка: Саудовская Аравия, ЮАР, Турция, ОАЭ.

** Другие страны Европы: Бельгия, Нидерланды, Польша, Швейцария и Швеция.

*** Другие страны Латинской Америки: Аргентина, Чили и Колумбия.

Источник: Сравнительное исследование Cisco в области безопасности за 2018 г.

Загрузить графики за 2018 г.: cisco.com/go/acr2018graphics

Загрузка иллюстраций

Все иллюстрации к данному отчету можно загрузить на странице: cisco.com/go/mcr2018graphics.

Исправления и обновления

Обновления и исправления информации, приведенной в данном проекте, см. по адресу cisco.com/go/errata.

Головной офис в США
Cisco Systems, Inc.
г. Сан-Хосе, Калифорния

Центральное представительство в Азиатско-Тихоокеанском регионе
Cisco Systems (USA) Pte. Ltd.
Сингапур

Центральное представительство в Европе
Cisco Systems International BV Амстердам, Нидерланды

Компания Cisco имеет более 200 офисов по всему миру. Адреса, номера телефонов и факсов приведены на сайте Cisco по адресу www.cisco.com/go/offices.

Опубликовано в феврале 2018 г.