КИБЕРБЕЗОПАСНОСТЬ 2016-2017:
ОТ ИТОГОВ К ПРОГНОЗАМ

POSITIVE TECHNOLOGIES

Содержание

Введение

Минувший год оказался богат на события в области информационной безопасности. В 2016 году помимо традиционных пентестов и анализа уязвимостей эксперты компании Positive Technologies приняли участие в расследовании ряда инцидентов, включая крупные атаки на банки, а также проанализировали общую картину атак, благодаря данным собственного центра мониторинга (SOC) и данным, полученным в ходе пилотных проектов и внедрению продуктов компании в различных организациях. Собранная информация позволяет предложить экспертную оценку ИБ-трендов года, а также сделать определенные прогнозы относительно того, что ждет индустрию в будущем, 2017 году. Вот, чем, по нашему мнению, запомнится 2016 год:

Потеря данных не лучше, чем потеря денег. Результатом большинства компьютерных атак 2016 года стали утечки конфиденциальной и приватной информации.

Целевые атаки: через человека — в корпорацию. Большинство кибератак года являются целевыми. Главный метод проникновения — хорошо таргетированный фишинг.

Рост атак на все финансовые системы. Злоумышленники используют простые методы и легальное ПО для маскировки, а сами атаки готовятся более тщательно.

Выкуп на высшем уровне. Крупные компании подвергаются вымогательству с помощью троянов-шифровальщиков, DDoS-атак и уязвимостей веб-сайтов.

Под ударом энергетика. Среди промышленных систем управления, доступных через Интернет, лидируют системы автоматизации зданий и управления электроэнергией.

Между АСУ и Интернетом вещей. Автоматизация управления стала доступна массовым пользователям без необходимых мер безопасности.

Государственные сайты — самая частая цель веб-атак. Наиболее популярны атаки «Внедрение операторов SQL» и «Выход за пределы назначенной директории (Path Traversal)».

Не верьте спутниковой навигации. Реализация атак с подменой GPS-сигнала стала доступной всем желающим.

Вами управляет Android. Вредоносное ПО для мобильных устройств получает права суперпользователя и обходит системы защиты.

Атаки через уязвимости аппаратных платформ. Легальные аппаратные возможности, предусмотренные самими производителями, могут быть использованы не по назначению.

Общие тренды

Потеря данных не лучше, чем потеря денег. Результатом большинства компьютерных атак 2016 года (по нашим данным, 46%) стала компрометация данных. Самый яркий пример — «переписка Клинтон», публикация которой, как предполагается аналитиками и СМИ, могла повлиять на исход выборов в США. Не обошли вниманием и простых пользователей: утекло множество учетных данных Yahoo, «ВКонтакте» и других массовых сервисов.

Целевые атаки: через человека — в корпорацию. Более половины кибератак, совершенных в 2016 году, являются целевыми (62%), причем большинство из них направлены на корпоративные активы. В последние годы такие атаки стали более скрытными: среднее время присутствия атакующих в системе увеличилось до 3 лет (максимальное — 8 лет). При этом лишь 10% атак выявляются самими жертвами: в 90% случаев они узнают о том, что были атакованы, из внешних источников.

Популярным способом проникновения является социальная инженерия, чаще всего — таргетированный фишинг в виде делового письма. Атаки с использованием социальной инженерии используются во всех сферах, уровень осведомленности большинства компаний очень низок. Потери от одного фишингового письма могут превышать 50 млн евро (атака на австрийскую аэрокосмическую компанию FACC, атака на бельгийский банк Crelan). Именно с фишинговых писем начались и многие успешные атаки на финансовый сектор России, стран СНГ и Восточной Европы, включая атаку Cobalt.

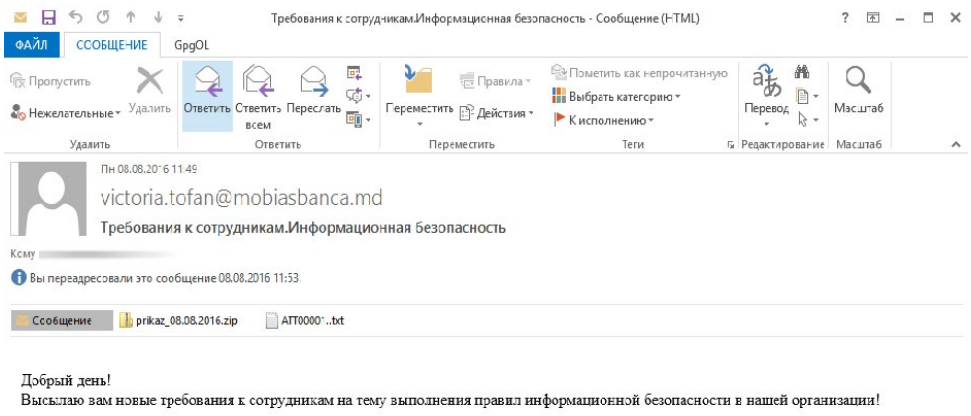

Рис. 1. Пример фишингового письма, использованного при атаке Cobalt

В России атаки на финансовые структуры стали лидирующими (30%). Только по открытым источникам, более 2 млрд рублей похищены в 2016 году в ходе атак на российские финансовые сервисы.

Выкуп на высшем уровне. В прошлые годы ransomware, то есть программы, требующие выкупа за прекращение вредоносных действий, в основном ассоциировались с трояны-шифровальщиками, которые терроризировали отдельных пользователей, шифруя файлы на их компьютерах. В 2016 году, не в последнюю очередь благодаря удобству и анонимности использования криптовалюты Bitcoin, атакам с требованием выкупа активно подвергались и крупные организации. Иногда это делают те же трояны-шифровальщики, которые атакуют всех без разбора — как в случае бухгалтерии казанского МВД, метро Сан-Франциско и целого множества американских клиник. Однако есть и ряд прицельных бизнес-схем.

В частности, продолжает развиваться техника DDoS for Ransom: демонстрация DDoS-атаки с обещанием продолжить ее, если не будет выплачен выкуп. Эта бизнес-модель объясняет некоторые DDoS-атаки, которые со стороны кажутся бессмысленными рекордами: злоумышленники демонстрируют свои возможности на популярных площадках, чтобы пугать потенциальных жертв. В некоторых случаях жертвы платят, даже не дожидаясь какой-либо атаки на их собственные ресурсы.

Другой способ вымогательства — bug poaching: хакеры требуют выкуп за информацию об уязвимостях, найденных в веб-приложениях компаний. Хотя такое бывало и раньше, специалисты считают, что именно в этом году такая техника стала массовой: пострадали более 30 организаций за год. Мы полагаем, что перечисленные техники вымогательства будут развиваться и в 2017 году.

Промышленные системы управления

Под ударом энергетика. Согласно нашему прошлогоднему исследованию «Безопасность АСУ ТП в цифрах», количество уязвимых компонентов промышленных систем управления из года в год не снижается.

Практически половина уязвимостей, найденных уже в 2016 году, имеет высокую степень риска.

Так, наши специалисты выявили уязвимость в системе Siemens SICAM PAS для управления энергосистемами. Уязвимость имеет оценку 9,8 по 10-балльной шкале CVSSv3, что соответствует высокому уровню опасности. Данное ПО используется на подстанциях различных классов напряжения в России и многих других странах. Производитель уже подтвердил наличие брешей и выпустил рекомендации по их устранению, но это редкое исключение: лишь 14% уязвимостей АСУ ТП прошлого года устранены в течение трех месяцев. 34% устранялись более трех месяцев, а оставшиеся 52% ошибок — либо вовсе не исправлены, либо производитель не сообщает о времени устранения.

В целом, среди найденных в сети Интернет компонентов АСУ ТП только две трети можно условно назвать защищенными. При этом самыми распространенными компонентами, доступными через Интернет (как правило, с несложным словарным паролем) являются системы для автоматизации зданий (Tridium / Honeywell), а также системы мониторинга и управления электроэнергией, в том числе на основе солнечных батарей (SMA Solar Technology).

Такая ситуация приводит к атакам: в декабре 2015 и декабре 2016 года были взломаны электросети Украины, электричества были лишены тысячи людей. То же самое ПО для систем управления используется и в других странах, поэтому некоторые уже предпринимают новые меры безопасности — опубликована стратегия США и Канады по защите энергосетей, а также черновик руководства по кибербезопасности АЭС от МАГАТЭ.

Между АСУ и Интернетом вещей. По итогам 2015 года мы отмечали, что различные системы автоматизации с дистанционным управлением все активнее входят в повседневную жизнь людей — например, взлом «умного дома» может повлиять на работу вентиляции, отопления и других систем жизнеобеспечения. Но если в случае АСУ, применяемых на производстве, уже есть целый ряд средств и политик безопасности, то пользователи Интернета вещей лишены такой защиты. Как правило, даже нет интерфейсов, позволяющих понять, что устройство скомпрометировано, или обновить его прошивку, или поставить на нем антивирус.

Поэтому неудивительно появление Mirai и других ботнетов из миллионов зараженных веб-камер, о которых эксперты Positive Technologies предупреждали еще в 2013 году:

даже известная уязвимость в Интернете вещей остается незакрытой годами. Следующим по популярности (для хакеров) умным устройством обещает стать Smart TV. Правда, бизнес-модель здесь другая: телевизор обладает большим экраном, где можно разместить требование выкупа.

Не исключено, что ситуация в сфере Интернета вещей может потребовать регулирования минимального уровня защищенности устройств — если производители сами не проявят сознательность в этом вопросе, то подключится государство, которое займется вопросами сертификации и стандартизации подобной продукции.

Среди мер противодействия стоит отметить разработку рекомендаций The Industrial Internet Security Framework. Документ, подготовленный экспертами крупных IT- и ИБ-компаний, интересен тем, что связывает ICS и IoT общими практиками безопасности. Однако это лишь рекомендации: не факт, что производители IoT-устройств будут их применять.

Финансы

Рост атак на все финансовые системы (SWIFT, межбанковские переводы, процессинг, ДБО, АБС, банкоматы, платежные терминалы, мобильные платежные системы). По оценкам наших экспертов, количество атак будет продолжать расти как минимум на 30% за год.

Основные причины такой ситуации — банки используют старые реактивные подходы к ИБ и защиту «из коробки» (которая не работает), отказываются от регулярного анализа защищенности. В то же время хакеры, увидев «легкие деньги», начинают тиражировать успешные атаки.

При этом, если в западных странах доминируют атаки на клиентов (60%), то в России активнее атакуют банки: персональные платежи наличными здесь по-прежнему популярнее электронных, и это ограничивает возможности кибер-кражи.

Нарушители все реже прибегают к атакам с эксплуатацией уязвимостей нулевого дня, переходя на более простые методы проникновения (например, фишинг). При этом сами атаки становятся более проработанными, что включает длительное исследование целей и хорошую маскировку. В частности, злоумышленники чаще применяют легитимные коммерческие инструменты, а также встроенные функции ОС, что позволяет им скрывать свою вредоносную активность в инфраструктуре.

Ярким примером могут служить атаки на банки России и Восточной Европы, осуществленные группой Cobalt. Как выяснили наши эксперты в ходе расследования этих инцидентов, злоумышленники взяли на вооружение коммерческое ПО для проведения легальных тестов на проникновение, а для загрузки на серверы и рабочие станции необходимых утилит они применяли легитимные веб-ресурсы (в частности, github.com). Для удаленного управления банкоматами использовалась программа RAdmin, которую активно применяли администраторы атакованного банка, потому ее запуск не вызвал подозрений у отдела безопасности.

Банкоматы по-прежнему под угрозой. Появляются довольно изощренные схемы грабежа, которые включают предварительную атаку инфраструктуры банка для последующего выведения денег из банкоматов — это и уже упомянутая операция Cobalt, а также атаки на Тайване (34 банкомата, $2,2 млн.) и в Японии (1400 банкоматов, $13 млн.).

Также остаются популярны атаки на банкоматы с использованием физического доступа к «железу» или к сетевому соединению. Значительное количество уязвимостей

находится и в ПО банкоматов, включая уязвимости OS (и старой Windows XP, и новой Windows 7) и уязвимости систем защиты.

К примеру, в 2014 году был обнаружен троян для банкоматов Tyupkin, который отличался тем, что умел отключать защитную систему Solidcore (McAfee), чтобы скрыть свою вредоносную активность. Благодаря этому преступники смогли похитить сотни тысяч долларов из банкоматов Восточной Европы без привлечения внимания. Спустя два года, в 2016 году, в ходе анализа защищенности банкоматов одного из банков эксперты Positive Technologies обнаружили, что система Solidcore по-прежнему уязвима — и позволяет выполнять внедрение вредоносного кода в любые системные процессы, не вызывая подозрения и записей в логах.

Веб-приложения

Веб-ресурсы являются самым популярным объектом для современных кибератак. В 2016 году был проведен ряд пилотных проектов по внедрению защитного экрана Positive Technologies Application Firewall (PT AF) в различных организациях, что позволило нам проанализировать общую картину веб-атак 2016 года. Вот некоторые выводы:

Атаки на государственные сайты — самые частые (более 3 тыс. в день). Интернет-магазины занимают вторую строчку в этом рейтинге: в день регистрировалось около 2200 атак. В финансовой сфере PT AF регистрировал около 1400 атак в день. Интересный факт — в 2016 году был активно атакован информационно-аналитический центр, в функции которого входит обработка результатов государственных экзаменов.

Лидируют простые атаки. Наиболее популярные атаки года — «Внедрение операторов SQL», «Выполнение команд ОС», «Выход за пределы назначенной директории (Path Traversal)» и «Межсайтовое выполнение сценариев». Они не требуют лишних затрат и дополнительных условий, а необходимые для этих атак уязвимости встречаются на сайтах по-прежнему часто.

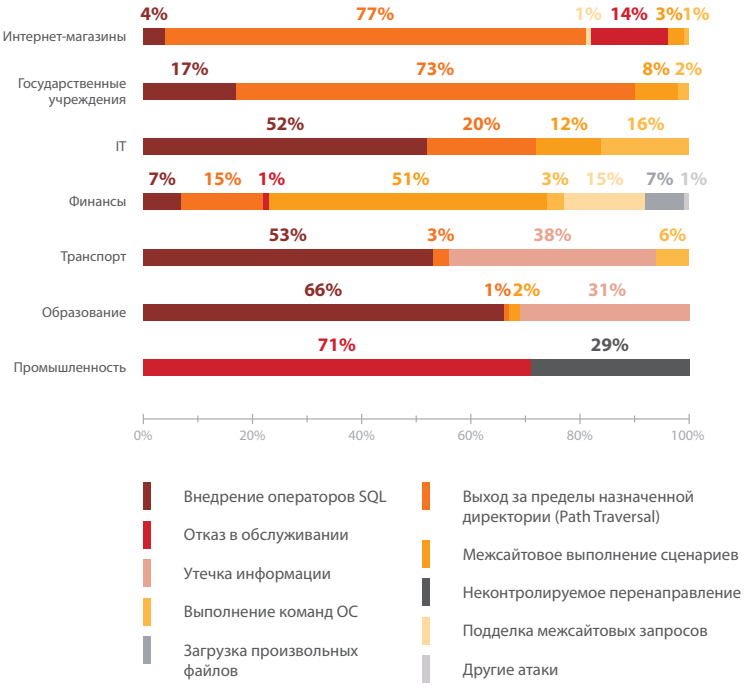

Рис. 2. Соотношение типов атак, выполняемых вручную

Высокая автоматизация. Большая часть веб-атак выполняется при помощи специализированного ПО для поиска уязвимостей. В случае сайтов промышленных компаний, количество автоматизированных атак достигает 98%. А вот в случае государственных учреждений и интернет-магазинов картина иная: там преобладают ручные атаки.

Телекоммуникации

Не верьте спутниковой навигации. Проблема стала достаточно наглядной в 2016 году на таком примере, как подмена GPS-сигнала вокруг московского Кремля. Для реализации подобных атак не нужно быть спецслужбой — они уже доступны любому.

Атаки через SS7 и Diameter. Ряд скандалов со взломом аккаунтов в мобильных мессенджерах типа Telegram или WhatsApp продемонстрировали, что угроза атак через древний протокол SS7 и его более молодого преемника, протокол Diameter, по-прежнему актуальна, хотя операторы начали предпринимать меры для улучшения ситуации.

Слишком много беспроводного. Мода на Интернет вещей сопровождается активным использованием известных протоколов с известными уязвимостями (GSM, Wi-Fi, Zigbee, Bluetooth). В частности, наш конкурс на PHDays VI показал возможности перехвата квадрокоптеров даже без особой подготовки.

Тем временем в России активно внедряется беспроводная система «Стриж» для учета потребления воды и электроэнергии. Считается, что у проекта большое будущее, поскольку он одобрен президентом. Но исследования безопасности «Стрижа» нам пока неизвестны.

Телеком-оператор как «доверенный провайдер». С одной стороны, новые устройства с беспроводным доступом позволяют оператору значительно увеличить абонентскую базу, то есть являются новыми желанными клиентами. С другой стороны, это ведет к ответственности за проблемы безопасности. Интересен случай Deutsche Telekom — после того, как почти миллион домашних роутеров пострадали из-за хакерской атаки (попытка включения в Mirai-ботнет), немецкий оператор решил пересмотреть отношения с производителем уязвимых роутеров. Уже известны примеры, когда операторы проводят дополнительное тестирование защищенности новых устройств, прежде чем предлагать пользователям эти устройства в рамках своих сервисов.

Гаджеты

Вами управляет Android. Поскольку смартфоны становятся основным «пультом управления» современной жизни, внимание злоумышленников к устройствам на базе OS Android не ослабевает. Вредоносное ПО, которое получает на Android-устройствах права суперпользователя и обходит новые системы защиты (Gugi, Hummer, Gooligan), стало обычным делом для 2016 года, а количество пострадавших уже исчисляется миллионами.

Большую угрозу представляют легитимные приложения с повышенными привилегиями, которые сами не выполняют вредоносных действий, но содержат уязвимости, позволяющие вредоносным приложениям проводить атаки практически незаметно. Такие уязвимости могут содержаться даже в приложениях, написанных опытными разработчиками. Известны случаи, когда из-за невнимательного отношения к настройке используемых SDK, добавление обычной библиотеки для удобного встраивания рекламы разрешало любому приложению на устройстве выполнять звонки на платные номера. Грядущие атаки на доверенную среду исполнения в мобильных устройствах могут привести к более серьезным последствиям, чем получение root-прав на телефоне.

При этом «сфера влияния» мобильных приложений расширяется: приложения для управления бытовыми приборами или для игр с дополненной реальностью (Pokemon Go) дают злоумышленникам новые возможности вмешательства в жизнь своих жертв. А после случаев возгорания Samsung Galaxy Note 7 довольно пугающей представляется идея программного контроля батарей мобильных устройств.

Утерянные или украденные смартфоны могут стать причиной масштабной утечки ввиду недостаточной защиты данных из-за некорректной реализации приложений. Мобильные устройства также оказываются весьма эффективными для атак на корпоративные сети изнутри, в обход защиты сетевого периметра: пользователи сами подключают зараженные устройства к рабочему Wi-Fi, а вредоносные приложения сканируют и атакуют ЛВС, заражая роутеры и рабочие станции пользователей. Помимо этого, мобильные устройства открывают широкий спектр возможностей для промышленного шпионажа через микрофоны и другие сенсоры.

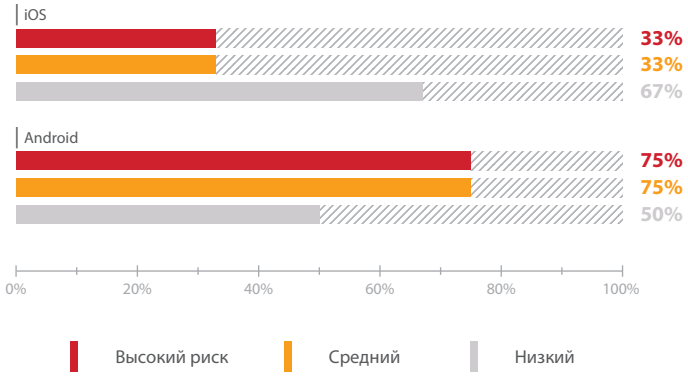

Рис. 3. Доли мобильных банковских клиентов, подверженных уязвимостям различной степени риска

Атаки через уязвимости аппаратных платформ. В прошлом выпуске Positive Research мы прогнозировали появление устройств, в которых легальные аппаратные возможности, предусмотренные самими производителями, могут быть использованы не по назначению. И если проблемам небезопасного ПО разработчики уделяют внимание уже давно, то вопросы уязвимостей самой аппаратуры еще только поднимаются. А ведь именно аппаратные атаки страшны тем, что зачастую они не зависят от ОС и не могут быть оперативно предотвращены.

Так, например, осенью 2016 года международная группа исследователей разработала атаку для root-доступа к большому количеству Android-устройств. Для этого они применили технику Rowhammer, позволяющую осуществлять манипуляции с данными, хранящимися в соседних ячейках оперативной памяти смартфона.

На конференции PHDays VI был представлен доклад о способах отключения Intel Management Engine (ME) — одного из элементов современных x86-платформ. Подсистема Intel ME представляет собой дополнительный «скрытый» процессор, который присутствует во всех устройствах на базе чипсетов Intel. Она работает даже при выключенном компьютере, имеет широкий доступ к памяти и устройствам, поэтому многие рассматривают ее как потенциальный вектор атаки.

Другая аппаратная возможность архитектуры в процессорах Intel описана экспертами Positive Technologies в декабре на конференции CCC в Гамбурге. Это низкоуровневый отладочный интерфейс, доступ к которому можно получить через USB 3.0. Этот функционал позволяет осуществлять аппаратную отладку гипервизоров, ядра ОС и драйверов.

Однако этот же механизм может использоваться и для атак, позволяя взломщику закрепиться в системе и совершить нападение в любой момент времени. При этом такая атака не требует особых финансовых затрат и не будет отслежена никакими системами безопасности.

Не исключено, что в 2017 году атаки через функциональность и уязвимости аппаратных платформ станут новым трендом.

Прогнозы и рекомендации

Ожидающийся рост атак на финансовые системы, государственные сайты и корпоративные инфраструктуры с использованием несложных технологий (фишинг, легальное ПО) говорит о необходимости использования более современных средств мониторинга событий и расследования инцидентов (SIEM), систем обнаружения атак на основе машинного обучения (WAF), а также требует значительного повышения осведомленности сотрудников.

Слабая защищенность промышленных систем управления (АСУ ТП), в сочетании с ухудшением геополитической обстановки, может привести в 2017 году к увеличению числа кибератак на промышленные объекты, особенно в энергетической сфере. При этом даже такие простые меры безопасности, как использование сложных паролей и отключение компонентов АСУ ТП от Интернета, могут значительно уменьшить риски. Более серьезные меры включают регулярные аудиты безопасности, своевременное обновление уязвимого ПО и использование средств защиты, «заточенных» на специфику конкретных АСУ ТП.

Пользователям мобильных устройств рекомендуется уделять повышенное внимание безопасности приложений — в частности, скачивать их только из официальных магазинов, и даже в случае легитимных приложений использовать настройки для ограничения прав доступа к персональной информации и потенциально опасным действиям. Актуальными остаются все советы по безопасности авторизации, включая двухфакторную авторизацию и сложные пароли. Использование сервисов на основе систем спутникового позиционирования желательно дублировать альтернативными методами навигации.

В то же время атаки на Интернет вещей показали, что пользователи зачастую лишены возможности самостоятельно контролировать безопасность новых устройств. В данном случае для уменьшения рисков необходимо, чтобы сами вендоры или провайдеры услуг Интернета вещей проводили дополнительные тестирования защищенности устройств перед их выпуском на рынок. Обязать их к такому тестированию могут либо дополнительные правила государственных регуляторов, либо саморегуляция на основе угрозы потери репутации после крупных атак (Mirai).

О компании

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована ФСТЭК России и в системе добровольной сертификации «Газпромсерт». Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

POSITIVE TECHNOLOGIES

ptsecurity.ru
pt@ptsecurity.com

facebook.com/PositiveTechnologies

facebook.com/PHDays