Отчет

Прогноз угроз McAfee® Labs на 2014 год

Содержание

1. В 2014 году главным фактором роста общего «рынка» вредоносных программ как с точки зрения технических инноваций, так и с точки зрения объема атак, станут вредоносные программы для мобильных устройств.

В 2013 году новые вредоносные программы для мобильных устройств, нацеленные почти исключительно на платформу Android, появлялись намного чаще, чем новые вредоносные программы, нацеленные на ПК. За последние два отчетных квартала рост количества новых вредоносных программ для ПК был довольно стабильным, в то время как новые образцы для Android стали появляться на 33 % чаще.

Хотя эта тенденция, согласно прогнозам McAfee Labs, сохранится и в 2014 году, наше внимание в новом году привлечет не только количество новых атак на мобильные устройства. Мы ожидаем также увидеть совершенно новые типы атак на Android. Вполне вероятно, что мы станем свидетелями первых реальных атак на мобильные устройства с использованием программ-вымогателей, т. е. атак, в ходе которых будет производиться шифрование имеющихся на устройстве важных данных и удержание их «в заложниках» с целью получения выкупа. Преступники будут выпускать захваченную информацию «на свободу» только в том случае, если жертва выплатит выкуп — либо обычными деньгами, либо виртуальными электронными деньгами (например, Bitcoin). Кроме того, мы считаем, что в сфере мобильных устройств будут также использоваться такие новые тактики, как атаки на уязвимости функций беспроводной связи ближнего радиуса действия, имеющихся уже на многих устройствах, и атаки в виде внесения изменений в проверенные приложения с целью незаметной кражи данных.

Атакам на мобильные устройства будет также подвергаться корпоративная инфраструктура. Эти атаки станут возможными благодаря теперь уже повсеместно распространенному феномену BYOD (Bring Your Own Device — «принеси свое собственное устройство»), когда сотрудники компаний используют на рабочем месте свои личные устройства, а также благодаря относительной незрелости технологий защиты мобильных устройств. Пользователи, невольно загружающие вредоносные программы, предназначенные для кражи конфиденциальных данных, в свою очередь распространяют эти программы внутри корпоративного периметра. Практика BYOD никуда не исчезнет, поэтому, чтобы не стать жертвами подобных атак, фирмам и предприятиям необходимо брать на вооружение комплексные политики и решения по управлению устройствами.

2. Виртуальные деньги станут стимулом для проведения по всему миру все большего количества атак с использованием программ-вымогателей.

Атаки с использованием программ-вымогателей, шифрующих данные на устройствах, появились уже довольно давно. Однако раньше успеху таких атак угрожали действия правоохранительных органов, направленные против используемых преступниками платежных систем.

Диалоговое окно CryptoLocker

С одной стороны, более активное использование виртуальных денег положительно сказывается на экономической деятельности. Но с другой стороны, виртуальные деньги дают злоумышленникам нерегулируемую и анонимную платежную инфраструктуру, идеально подходящую для сбора денег с объектов их атак. Мы считаем, что число таких атак, как CryptoLocker, будет увеличиваться до тех пор, пока их проведение не перестанет быть (очень) выгодным делом. Также мы прогнозируем появление новых атак на фирмы и предприятия, в ходе которых программы-вымогатели будут пытаться шифровать важные корпоративные данные.

Однако отчаиваться ни простым пользователям, ни предприятиям не стоит: несмотря на то, что код программ-вымогателей является уникальным, механизмы их распространения (спам, попутные загрузки и зараженные приложения) уникальными не являются. Потребители и корпоративные клиенты, вовремя обновляющие свои системы для защиты конечных точек и сетей от вредоносных программ, будут относительно защищены от данной угрозы. Изолировать пользователей от большей части негативных последствий контакта с программами-вымогателями поможет также наличие эффективной системы резервного копирования данных. Это касается как домашних, так и корпоративных пользователей.

3. В шпионском мире киберпреступных и кибервоенных действий преступные группировки и государственные структуры будут развертывать новые скрытые атаки, выявлять и пресекать которые станет сложнее, чем когда-либо прежде.

С развитием решений для обеспечения информационной безопасности все изощреннее становятся попытки киберпреступников обойти эти средства защиты. Атаки с использованием сложных методов обхода защиты представляют собой новейший фронт борьбы в войне за безопасность корпоративных данных. Популярным методом обхода защиты, который получит широкое распространение среди киберпреступников в 2014 году, является метод обнаружения «песочницы», позволяющий проводить полное развертывание атаки только тогда, когда есть уверенность в том, что вредоносный код запущен непосредственно на незащищенном устройстве, а не в «песочнице».

К другим популярным технологиям атаки, которые будут дальше разрабатываться и использоваться в 2014 году, относятся методы обратно-ориентированного программирования, которые заставляют обычные приложения вести себя вредоносным образом, самоудаляющиеся вредоносные программы, скрывающие свои следы после проведения атаки, и сложные методы проведения атак на специализированные промышленные системы управления, способные нанести ущерб объектам государственной и частной инфраструктуры.

По-прежнему будет расти число политически мотивированных атак, особенно во время зимних Олимпийских игр в Сочи (февраль) и чемпионата мира по футболу в Бразилии (июнь-июль). Воспользоваться этими событиями для продвижения своих идей не преминут и хактивисты.

Корпоративным ИТ-организациям нужно будет научиться реагировать на этот новый набор тактик и сделать так, чтобы используемые ими средства защиты не были основаны только на тех мерах безопасности, которые могут быть легко преодолены международными киберпреступными группировками.

4. «Социальные атаки» получат повсеместное распространение к концу 2014 года.

Атаки на социальные платформы — это атаки, для проведения которых используются огромные пользовательские базы Facebook, Twitter, LinkedIn, Instagram и т. д. Во многих из этих атак будет имитироваться тактика таких давно известных вредоносных программ, как Koobface, когда социальные платформы используются просто в качестве механизма доставки кода. По нашим прогнозам, однако, в 2014 году мы станем также свидетелями атак, в которых уникальные особенности социальных платформ используются для получения данных о контактах, местонахождении и деловой активности пользователей. С помощью таких данных киберпреступники могут целенаправленно размещать рекламу и совершать разного рода преступления в виртуальном и реальном мире.

Одна из самых распространенных атак на социальные платформы заключается просто в краже аутентификационных данных пользователей, которые затем используются для получения персональной информации от ничего не подозревающих «френдов» и коллег. Бот-сеть Pony[1], укравшая более двух миллионов паролей пользователей Facebook, Google, Yahoo и др., является, скорее всего, лишь верхушкой айсберга. По оценкам самого Facebook 50–100 млн учетных записей «ежемесячно активных пользователей» (Monthly Active User — MAU) являются дубликатами, а 14 млн зарегистрированных MAU можно считать «нежелательными». По данным недавнего исследования, проведенного компанией Stratecast, 22 % пользователей социальных медиа хотя бы раз столкнулись с инцидентом безопасности.[2]

Государственные и частные предприятия тоже будут использовать социальные платформы для проведения «разведывательных атак» на своих конкурентов и соперников, либо напрямую, либо через третьих лиц. В 2013 году объектами таких атак стал ряд ведущих компаний государственного и частного секторов. Есть основания полагать, что в 2014 году такие атаки станут более частыми и более масштабными.

Еще одним видом социальных атак, которые, как мы ожидаем, будут распространены в 2014 году, станут атаки «под чужим флагом», проводимые для того, чтобы обманным путем заставить пользователей раскрыть свою персональную информацию или аутентификационные данные. Одной из самых популярных атак станет «срочный» запрос на сброс пароля пользователя. Целью такой атаки является кража имени пользователя и пароля, чтобы затем использовать учетную запись ничего не подозревающего пользователя для сбора персональной информации о нем и его контактах.

Для предотвращения атак на социальные платформы и атак «под чужим флагом» потребуется повышение уровня бдительности как со стороны сотрудников, так и со стороны корпоративных политик и решений. Только в таком случае использование социальных сетей сотрудниками не будет приводить к существенным нарушениям безопасности данных.

5. Новые атаки на персональные компьютеры и серверы будут нацелены на уязвимости, расположенные на уровнях выше и ниже операционной системы.

Хотя многие киберпреступные синдикаты переключат свое внимание на мобильные устройства, остальные будут по-прежнему нацелены на персональные компьютеры и серверные платформы. Однако новые атаки, которые мы будем наблюдать в 2014 году, будут не просто атаками на операционную систему: они будут также нацелены на уязвимости, расположенные на уровнях выше и ниже ОС.

В 2014 году во многих новых атаках на персональные компьютеры будут использоваться уязвимости стандарта HTML5, который, с одной стороны, могут «оживить» веб-сайты, предоставляя программистам богатые возможности для создания интерактивных и персонализированных веб-сайтов, но, с другой стороны, обнажает ряд новых поверхностей атаки. Исследователи уже показали, как с помощью HTML5 осуществлять мониторинг посещаемых пользователем веб-страниц, чтобы более целенаправленно отображать рекламу. Поскольку многие приложения, созданные на базе HTML5, предназначены для мобильных устройств, мы прогнозируем появление атак, которые смогут выходить за пределы «песочницы» веб-обозревателя и давать злоумышленникам прямой доступ к устройству и его службам. Кроме того, многие фирмы и предприятия будут создавать корпоративные приложения на основе HTML5. Для предотвращения утечек данных, используемых этими приложениями, в эти новые системы необходимо будет с самого первого дня встроить соответствующие средства защиты.

Киберпреступники будут все чаще пытаться использовать уязвимости, находящиеся ниже операционной системы в стеке хранилища и даже в BIOS. В корпоративной среде для снижения риска таких низкоуровневых атак потребуется провести развертывание средств защиты с аппаратной поддержкой, тоже работающих ниже уровня операционной системы.

6. Эволюционирующий ландшафт угроз и требования, предъявляемые к качеству обнаружения угроз и уровню быстродействия систем, будут диктовать необходимость анализа больших объемов данных.

Так сложилось, что в основе большинства прежних решений для обеспечения информационной безопасности лежит либо выявление вредоносного кода (технология черных списков), либо отслеживание известных, проверенных приложений (технология белых списков). Теперь же перед специалистами по информационной безопасности встала задача определения и соответствующей обработки «серого» кода. Это требует использования большого количества разных технологий безопасности в сочетании с надежными службами сбора информации о репутации.

Службы сбора информации о репутации угроз уже доказали свою эффективность при обнаружении вредоносных программ, вредоносных веб-сайтов, спама и сетевых атак. В 2014 году производители средств защиты выпустят новые службы сбора информации о репутации угроз и аналитические инструменты, которые дадут им и их пользователям возможность выявлять скрытые и постоянные угрозы повышенной сложности быстрее и точнее, чем это возможно на сегодняшний день. Средства анализа больших объемов данных позволят специалистам по безопасности обнаруживать сложные, изощренные методы обхода защиты и постоянные угрозы повышенной сложности, способные нарушить ход выполнения критически важных бизнес-процессов.

7. Развертывание облачных корпоративных приложений создаст новые поверхности атаки, которые будут использоваться злоумышленниками.

Вилли Саттону (Willie Sutton), который, как говорят, в начале XX века ограбил 100 банков, приписывают слова о том, что он грабил банки, «потому что там находятся деньги».[3] Киберпреступные группировки XXI века будут атаковать облачные приложения и хранилища данных, потому что там находятся или довольно скоро будут находиться данные. Инструментом их атак могут стать бизнес-приложения, не прошедшие проверку в службе ИТ на соответствие корпоративным политикам безопасности. Согласно недавно опубликованному отчету, более 80 % бизнес-пользователей используют облачные приложения без ведома и поддержки корпоративной службы ИТ.[4]

У облачных приложений без сомнения есть убедительные функциональные и экономические преимущества, но при этом они дают злоумышленникам возможность использовать совершенно новое семейство поверхностей атаки: это и повсеместно распространенные гипервизоры, имеющиеся во всех центрах обработки данных, и инфраструктура многопользовательской связи, являющаяся неотъемлемой частью облачных служб, и инфраструктура управления, используемая для запуска и мониторинга крупномасштабных облачных служб. Проблема, стоящая перед специалистами по корпоративной безопасности, заключается в том, что при миграции корпоративного приложения в «облако» организация теряет возможность собирать информацию о профиле защиты и осуществлять контроль над ним.

Потеря прямого контроля над защитным периметром компании заставляет руководителей и администраторов подразделений безопасности делать все возможное для того, чтобы пользовательское соглашение с поставщиком облачной службы и порядок ее эксплуатации гарантировали наличие и постоянное обновление мер защиты в соответствии с постоянно эволюционирующим ландшафтом угроз. У крупных компаний может оказаться достаточно рычагов влияния для того, чтобы потребовать у поставщиков облачных служб принятия мер безопасности, отвечающих действующим в этих компаниях стандартам безопасности. У менее крупных пользователей облачных служб, однако, таких рычагов влияния не будет, поэтому им нужно будет внимательно изучать (зачастую неоднозначное) пользовательское соглашение поставщика в той его части, где речь идет о безопасности и правах владения данными. Кроме того, у новых облачных служб могут обнаружиться новые поверхности атаки, которые будут открыты до тех пор, пока эти службы не достигнут некоторого уровня зрелости, подразумевающего наличие инструментов и мер противодействия, необходимых для обеспечения безопасности тех данных, которые они должны защищать.

Об авторах

В подготовке и написании данного отчета принимали участие: Кристоф Альме (Christoph Alme), Рамнат Венугопалан (Ramnath Venugopalan), Адам Восотовски (Adam Wosotowsky) , Паула Греве (Paula Greve), Торальв Дирро (Toralv Dirro), Адитья Капур (Aditya Kapoor), Седрик Кошен (Cedric Cochin), Бенджамин Круз (Benjamin Cruz), Джеффри Купер (Geoffrey Cooper), Клаус Маевски (Klaus Majewski), Дуг МакЛин (Doug McLean), Игорь Муттик (Igor Muttik), Юкихиро Окутоми (Yukihiro Okutomi), Франсуа Паже (François Paget), Рик Саймон (Rick Simon), Дэн Соммер (Dan Sommer), Бин Сунь (Bing Sun), Чун Сюй (Chong Xu)., Джимми Ша (Jimmy Shah), Райан Шерстобитофф (Ryan Sherstobitoff) и Крейг Шмугар (Craig Schmugar).

О лаборатории McAfee Labs

McAfee Labs занимает лидирующее положение в мире как источник аналитической информации об угрозах, данных об угрозах, а также передовых идей в области кибербезопасности. Штат McAfee Labs насчитывает 500 аналитиков. Они собирают данные с миллионов датчиков, расположенных по всем ключевым векторам угроз (файлы, веб-трафик, электронная почта и сети), а затем проводят межвекторный сопоставительный анализ собранных данных и посредством облачной службы McAfee Global Threat Intelligence в режиме реального времени снабжают информацией об угрозах тесно интегрированные между собой продукты McAfee для защиты конечных точек и сетей. Кроме того, McAfee Labs занимается разработкой ключевых технологий обнаружения угроз (DeepSAFE, создание профилей приложений, управление серыми списками и др.), встроенных в самый обширный из имеющихся в отрасли наборов защитных продуктов.

О компании McAfee

McAfee, стопроцентная дочерняя компания Intel Corporation (NASDAQ: INTC), позволяет предприятиям, организациям государственного сектора и домашним пользователям безопасно и эффективно применять Интернет-технологии. Компания поставляет проверенные упреждающие решения защиты для систем, сетей и мобильных устройств по всему миру. Благодаря своей стратегии Security Connected, новаторскому подходу к решениям безопасности, усиленным средствами аппаратного обеспечения, а также благодаря уникальной сети сбора информации об угрозах Global Threat Intelligence, компания McAfee непрерывно и целеустремленно ищет новые пути защиты своих клиентов. www.mcafee.com/ru

[1] http://blogs.mcafee.com/consumer/pony-botnet-steals-2-million-passwords

[2] Stratecast, «*The Hidden Truth Behind Shadow IT*» (Скрытая правда теневой ИТ-отрасли). Ноябрь 2013 г., http://www.mcafee.com/ru/resources/reports/rp-six-trends-security.pdf

[3] По утверждению самого Саттона, он никогда не говорил этой приписываемой ему знаменитой фразы. По его словам, он грабил банки, потому что «ему это нравилось».

[4] Stratecast, «*The Hidden Truth Behind Shadow IT*» (Скрытая правда теневой ИТ-отрасли). Ноябрь 2013 г., http://www.mcafee.com/ru/resources/reports/rp-six-trends-security.pdf

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.McAfee.ru

60756rpt_threats-predictions_1213_fnl_ETMG