Отчет McAfee Labs об угрозах

Ноябрь 2014 г.

intel Security

О лаборатории McAfee Labs

McAfee Labs занимает одно из ведущих мест в мире как источник аналитической информации об угрозах, данных об угрозах, а также передовых идей в области кибербезопасности. Получая данные с миллионов датчиков, расположенных по ключевым векторам угроз (файлы, веб-трафик, электронная почта и сети), McAfee Labs в режиме реального времени предоставляет информацию об угрозах, проводит анализ их критичности и дает экспертную оценку, позволяющую повысить уровень защиты и сократить риски. McAfee теперь входит в состав Intel Security.

www.mcafee.com/ru/mcafee-labs.aspx

Подпишитесь на McAfee Labs

Введение

Приближается период праздников, и злоумышленники, как всегда, готовят новые сюрпризы. Недавно McAfee опубликовала список ***«12 видов мошенничества в праздники»*** (12 Scams of the Holidays), включающий наиболее распространенные трюки. Рекомендуем ознакомиться с этим занятным чтением. Мы уже видим, что начинают сбываться прогнозы на 2015 год в самых разных областях — от тенденций в глобальной экономике до наиболее ярких звезд Голливуда.

В последние годы McAfee Labs также представляет прогнозы в своей области компетенции. Многие из наших прогнозов, высказанных **в прошлогоднем отчете**, сбылись с поразительной точностью. К примеру, мы точно предсказали бурный рост числа программ-вымогателей (включая таковые для мобильных платформ!), увеличение количества атак по политическим мотивам, а также то, что предприятия начнут активно внедрять средства сбора и анализа информации об угрозах для выявления всё более скрытых угроз. Однако никто не идеален, поэтому, конечно же, некоторые прогнозы не сбылись. Такова суть прогнозов.

В этом году мы решили ускорить публикацию прогноза угроз на 2015 год и включили его в данный отчет. Это даст нашим клиентам возможность заранее подумать о том, что может их ожидать в 2015 году, и заблаговременно подготовиться к наиболее серьезным угрозам. Конечно, мы не забыли и о традиционных разделах «Главные темы» и «Статистика угроз», входящих в каждый квартальный отчет.

В этот раз главной темой отчета стала уязвимость BERserk — уязвимость в механизме проверки цифровых подписей RSA, которая может быть использована киберпреступниками множеством способов и повлечь за собой серьезные последствия. Обнародованная компанией McAfee новость об обнаружении уязвимости BERserk прошла незамеченной на фоне обсуждений уязвимости **Shellshock**, однако BERserk также может нанести существенный вред. Более подробные сведения об уязвимости BERserk приведены **здесь**. В отдельной статье отчета рассматриваются различные способы злоупотребления доверием, к которым прибегают киберпреступники. Мы еще раз напоминаем, что основные средства противодействия такого рода угрозам — это осведомленность и личные навыки.

В этом отчете мы изменили привычное представление некоторых диаграмм в разделе статистики угроз и добавили новые сведения. Это было сделано в ответ на пожелания читателей видеть больше нужной им статистики. Кроме того, мы начали получать более качественные отчеты из своих собственных систем, что позволило повысить точность некоторых диаграмм. Надеемся, вам понравятся наши нововведения.

Благодарим всех, кто ответил на вопросы, опубликованные в ***августовском отчете об угрозах***. Усовершенствованное представление статистических данных в этом отчете свидетельствует о том, что мы прислушиваемся к пожеланиям наших читателей. Если вы хотите поделиться с нами своими соображениями в отношении данного *отчета об угрозах*, щелкните **здесь** и уделите несколько минут ответам на вопросы.

Примите наши поздравления с приближающимися праздниками! Желаем всего наилучшего вам и вашим близким!

Винсент Уифер (Vincent Weafer), старший вице-президент McAfee Labs

Поделитесь своим мнением

Содержание

Отчет McAfee Labs об угрозах
Ноябрь 2014 г.

В подготовке и написании этого отчета принимали участие:

Рамнат Венугопалан (Ramnath Venugopalan)
Адам Восотовски (Adam Wosotowsky)
Мишель Деннеди (Michelle Dennedy)
Стенли Жу (Stanley Zhu)
Адитья Капур (Aditya Kapoor)
Седрик Кошен (Cedric Cochin)
Бенджамин Крус (Benjamin Cruz)
Дэн Ларсон (Dan Larson)
Хайфей Ли (Haifei Li)
Крис Миллер (Chris Miller)
Игорь Муттик (Igor Muttik)
Франсуа Паже (François Paget)
Эрик Петерсон (Eric Peterson)
Рик Саймон (Rick Simon)
Мэри Сальваджио (Mary Salvaggio)
Дэн Соммер (Dan Sommer)
Бин Сунь (Bing Sun)
Вино Томас (Vinoo Thomas)
Джеймс Уолтер (James Walter)
Райан Шерстобитофф (Ryan Sherstobitoff)
Крейг Шмугар (Craig Schmugar)

Краткая сводка

Прогноз угроз McAfee Labs на 2015 год

В этом *отчете об угрозах* рассматриваются угрозы, которые мы ожидаем увидеть в 2015 году. Наши прогнозы охватывают широкий спектр вопросов, включая концепцию «Интернета вещей», кибершпионаж, мобильные устройства, конфиденциальность персональных данных, программы-вымогатели и многое другое.

Уязвимость BERserk основана на ошибке в программном обеспечении проверки цифровых подписей RSA, в результате чего злоумышленникам предоставляется возможность реализации незаметных для пользователя атак типа «незаконный посредник».

Уязвимость BERserk: безопасность соединений под сомнением

В сентябре компания **Intel Security опубликовала подробности** о чреватой серьезными последствиями уязвимости, получившей имя BERserk — с намеком на механизм, лежащий в ее основе. На момент написания данной статьи все последствия уязвимости BERserk еще неизвестны, однако уже ясно, что она очень опасна. Уязвимость BERserk основана на ошибке в программном обеспечении проверки цифровых подписей RSA, в результате чего злоумышленникам предоставляется возможность реализации незаметных для пользователя атак типа «незаконный посредник». Установление доверительных отношений при подключении к веб-сайту, как правило, начинается с указания протокола «https» в начале URL-адреса. Дополнительным свидетельством безопасности служит отображаемый в браузере значок замка́. Уязвимость BERserk ставит такое соединение под угрозу, позволяя злоумышленникам отслеживать и как угодно использовать данные, передаваемые между пользователем и веб-сайтом.

Специалисты McAfee Labs считают, что доверие к различным формам взаимодействия в Интернете проходит путь, который уже преодолела в свое время электронная почта — сегодня уже мало кто слепо верит в подлинность сообщений.

Злоупотребление доверием: использование слабых звеньев в системах сетевой безопасности

Пользователи — это самые слабые звенья во всех системах безопасности. Мы доверяем бóльшую часть своих данных различным устройствам и полагаем, что они предоставляют точные сведения безопасным способом. Одновременно с этим злоумышленники, как правило, сосредоточены на доверии, проявляемом нами по отношению к устройствам, и используют это доверие с целью хищения данных. В этой статье рассматривается проблема злоупотребления доверием и приводятся новые примеры того, как злоумышленники используют доверие пользователей в своих интересах. Специалисты McAfee Labs считают, что доверие к различным формам взаимодействия в Интернете проходит путь, который уже преодолела в свое время электронная почта — сегодня уже мало кто слепо верит в подлинность сообщений.

Прогноз угроз McAfee Labs на 2015 год

Кибершпионаж

Интернет вещей

Конфиденциальность

Программы-вымогатели

Мобильные устройства

Торговые терминалы

Вредоносные программы не только для Windows

Уязвимости

Выход из «песочницы»

Поделитесь своим мнением

Кибершпионаж

Частота кибершпионских атак продолжит свой рост. Опытные кибершпионы будут всё более незаметно собирать информацию, в то время как начинающие будут искать способы похищать деньги и подрывать деятельность своих противников.

Малые страны и иностранные террористические группировки выйдут в киберпространство для ведения военных действий против своих противников. От них можно ожидать разрушающих атак типа «распределенный отказ в обслуживании» или использования вредоносных программ, удаляющих загрузочную запись с целью уничтожить сети противников. В то же время опытные кибершпионы будут применять усовершенствованные методы для того, чтобы оставаться незаметными в сети жертвы. Более сложные и эффективные технологии обеспечения скрытности и другие методы позволят им действовать вне зоны видимости, ниже уровня операционной системы.

В частности, McAfee Labs наблюдает переход восточноевропейских киберпреступников от быстрых прямых атак, направленных на завладение учетными данными клиентов финансовых учреждений (с целью кражи денег), к более изощренным средствам, подразумевающим использование сложных постоянных угроз (APT) для сбора информации, которую можно продать или использовать позже. Таким образом, преступники начинают действовать подобно государственным кибершпионам, которые в охоте за информацией взяли на вооружение выжидательную тактику.

Аналогичный подход стал просматриваться и в секторе розничной торговли. Многие торговые организации теперь создают подробные профили своих клиентов — содержащие, среди прочего, информацию о покупательских привычках клиента, сведения об интересующих его товарах, его кредитную историю, историю перемещений, а также контактные данные. Помимо этого, успешные стратегические, операционные и финансовые планы торговых организаций могут представлять большую ценность для определенных покупателей. Некоторые киберпреступники, по всей видимости, используют кибершпионский подход, основанный на использовании сложных постоянных угроз для проникновения в системы торговых организаций, где они незаметно собирают информацию, не ограничивающуюся лишь данными кредитных карт, для продажи покупателю, предложившему самую высокую цену.

Райан Шерстобитофф (Ryan Sherstobitoff)

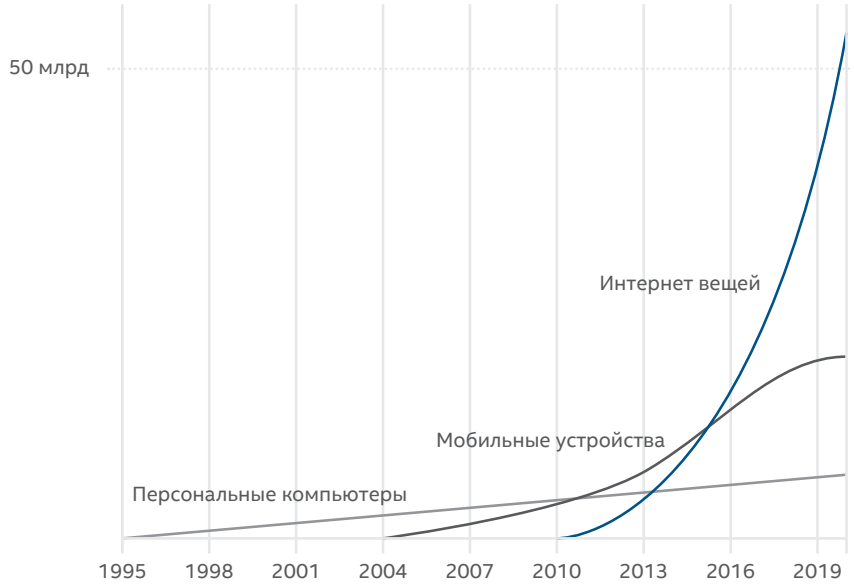
Интернет вещей

Частота атак на устройства «Интернета вещей» будет быстро расти в связи с огромным количеством подключаемых объектов, низкой культурой безопасности и высокой ценностью данных, содержащихся на этих устройствах.

Число и разнообразие устройств, относящихся к «Интернету вещей», растет в геометрической прогрессии. В потребительской сфере такие устройства можно встретить в бытовой технике, автомобилях, системах «умного дома» и даже в лампочках. В сфере коммерческих продуктов для технологий «Интернета вещей» имеется множество применений, в том числе в сельском хозяйстве, промышленности и здравоохранении. Устройства «Интернета вещей» создаются на основе постоянно расширяющегося спектра программных и аппаратных компонентов, что приводит к высокой сложности и отрицательно сказывается на безопасности.

При проектировании этих компонентов и, таким образом, самих устройств безопасность, как правило, не ставится во главу угла. Всё более широкое внедрение устройств «Интернета вещей» на фоне отсутствия надежной защиты представляет собой растущую угрозу конфиденциальности и безопасности как частных лиц, так и компаний.

Количество подключенных к Интернету устройств в мире



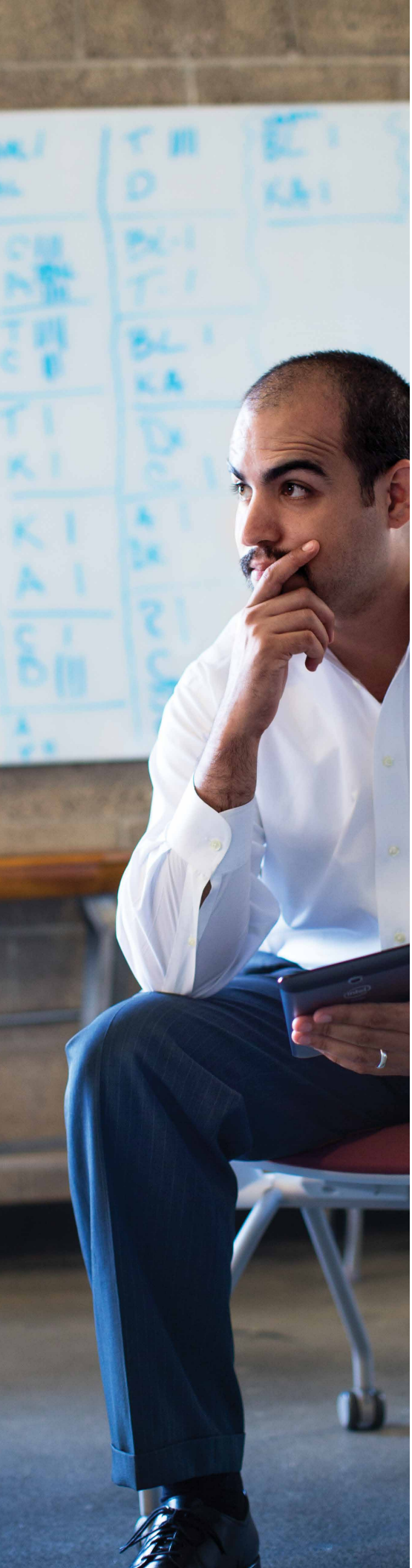
Источники: McAfee, на основании исследований компаний BI Intelligence, IDC и Intel

Уже сейчас широко распространены атаки, направленные на устройства «Интернета вещей», начиная от слабо защищенных IP-камер и интеллектуальных счетчиков с элементарными ошибками шифрования до устройств SCADA, используемых в критически важных инфраструктурах по всему миру. Например, подключенные к Интернету электрические счетчики, установленные в миллионах домов в Испании, содержат уязвимости, потенциально позволяющие злоумышленникам выставлять мошеннические счета или даже отключать электроэнергию. На прошлогодней конференции «белых» хакеров исследователи продемонстрировали, как легко преодолеть защиту некоторых подключаемых к Интернету камер наблюдения. Уязвимости этих камер позволяют злоумышленникам получить не только видеосигнал, но и доступ в сеть видеокамер.

Особую тревогу вызывает один из видов угроз. Учитывая всё более широкое распространение устройств «Интернета вещей» в сфере здравоохранения и активное использование их в больницах всё более вероятной становится угроза потери информации, содержащейся на этих устройствах. **Согласно данным агентства Рейтер**, медицинские данные представляют еще большую ценность, чем данные кредитных карт, потому что за каждую учетную запись, украденную из медицинских систем, платят до 10 долларов — примерно в 10–20 раз больше, чем за номер американской кредитной карты.

То, что раньше было под силу лишь государственным организациям и крупным киберпреступным группировкам, может теперь оказаться доступным любому целеустремленному хакеру. Мы прогнозируем, что в 2015 году будет произведена крупная атака, непосредственно связанная с уязвимостями устройств «Интернета вещей».

Крис Миллер (Chris Miller) и Рамнат Венугопалан (Ramnath Venugopalan)



Конфиденциальность

Пока правительства и компании пытаются определить, что же является честным и авторизованным доступом к не вполне дефинированному понятию «персональная информация», под угрозой остается конфиденциальность данных.

Конфиденциальность данных определяется как честный и авторизованный доступ к информации, соотносимой с конкретной личностью. Хотя метод и проблему обеспечения конфиденциальности можно описать этим простым предложением, сложность и риск, связанные с ее нарушениями, в 2015 году будут по-прежнему расти в геометрической прогрессии.

Разберем определение более подробно. Понятие честности субъективно по отношению к пользователям системы, клиентам и сотрудникам компании или гражданам государства. Более подробное определение честности дает свод принципов честного использования информации, признанных еще в 1960-х годах многими странами мира. В частности, к этим принципам относятся прозрачность, осведомленность, возможность выбора, соразмерность сбора данных, обработка и передача данных через границу, безопасность, ограничение доступа к данным и возможность их удаления.

Другим слагаемым конфиденциальности данных является авторизация. Авторизация позволяет идентифицировать пользователя и определить его полномочия в области управления информационными активами. Она дает возможность установить личность клиента, сотрудника или гражданина в мировой экономике, приобретающей всё более отчетливый цифровой и обезличенный характер. В 2015 году устаревшие системы доступа на базе ролей и схемы авторизации на основе паролей окажутся несостоятельными и будут взламываться злоумышленниками или нарушаться в результате простой неосмотрительности. Биометрические и идентификационные данные с учетом контекста служат, вероятно, лучшими индикаторами присутствия и намерений. В этой области будет сосредоточено множество инноваций. Мы полагаем, что проблемы сбора контекстной информации станут одновременно и фактором инновационного развития и фактором увеличения риска использования уязвимостей.

Последним элементом в определении конфиденциальности является информация, соотносимая с конкретной личностью. В 2015 году нас ожидает еще больше дискуссий и еще меньше ясности относительно того, какая именно информация считается «персональной» и какая ее часть может на законных основаниях рассматриваться государственными или частными организациями. Во многих странах принято юридическое определение, согласно которому персональной информацией считаются либо данные, идентифицирующие личность непосредственно, либо данные, которые в сочетании с другими данными могут идентифицировать личность с большой вероятностью. Хотя специалисты по статистике и экономисты всегда использовали большие наборы отдельных случаев для создания «данных», среди технических специалистов принято говорить об использовании больших объемов информации как о «больших данных». Чем больше объем этих данных, тем меньше вероятность того, что мы сможем сохранять анонимность. Таким образом, начиная с 2015 года будет наблюдаться тенденция ко всё более широкому применению правил и норм конфиденциальности данных — со всеми сопутствующими требованиями к безопасности и защите от утечек — в отношении ранее анонимных наборов данных.

Мы ожидаем, что к концу 2015 года Европейский союз заменит свою **Директиву о защите данных 1995** года новым Регламентом о защите данных 2016 года, который вступит в действие во всех странах-членах ЕС и будет принят во всех международных организациях. Этот шаг со стороны ЕС будет, вероятно, самой заметной инициативой, касающейся норм защиты данных, при этом страны Латинской Америки, а также Австралия, Япония, Южная Корея, Канада и многие другие государства будут использовать всё более агрессивный и национально-ограниченный подход в законодательстве и регулировании применительно к конфиденциальности и защите данных.

Мишель Деннеди (Michelle Dennedy)

Программы-вымогатели

Методы распространения, шифрования и выбора целей в программах-вымогателях будут совершенствоваться. Атакам подвергнется большее число мобильных устройств.

Мы прогнозируем, что варианты программ-вымогателей, способные обойти установленные защитные программы, будут выбирать своей целью те конечные точки, на которых используются облачные хранилища данных, такие как Dropbox, Google Drive и OneDrive. После заражения этих конечных точек программы-вымогатели попытаются использовать учетные данные пользователя, зарегистрированного в облачном хранилище, чтобы заразить также и резервные копии данных в «облаке».

Обнаружив, что данные на конечной точке зашифрованы, жертвы программ-вымогателей будут совершенно ошеломлены при попытке восстановить данные из облачного хранилища — ведь резервные копии тоже будут зашифрованы.

Хотя файлы, зашифрованные программой-вымогателем, не могут самостоятельно распространяться и заражать другие устройства, можно представить себе такое развитие тактики, при котором каждый зашифрованный файл станет переносчиком программы-вымогателя. Для этого понадобится преобразовать файл жертвы в исполняемый файл, содержащий исходные данные в теле программы-вымогателя. Такой метод давно применяется вирусами, заражающими невредоносные исполняемые файлы для использования их в качестве переносчиков. Авторы программ-вымогателей могут вновь применить ту же модель для шифрования файлов.

Как и в прошлом году, мы снова ожидаем увеличения числа программ-вымогателей, нацеленных на мобильные устройства. Телефоны и планшетные компьютеры представляют большой интерес для авторов программ-вымогателей, потому что они содержат ценные фотографии и персональные данные. Мы также ожидаем, что программы-вымогатели, заражающие резервные копии данных в «облаке», распространятся и в мобильном пространстве. Мобильные платформы поддерживают огромное количество нерегламентированных способов оплаты, так что злоумышленники найдут множество путей для получения от жертв выкупа за расшифровку зашифрованных данных.

Вино Томас (Vinoo Thomas)

Мобильные устройства

Число атак на мобильные устройства продолжает быстро расти, в то время как новые мобильные технологии увеличивают поверхность атаки и мало что делается для пресечения злоупотреблений в магазинах приложений.

Число вредоносных программ для ПК исторически росло вслед за крупными событиями, такими как появление пакетов для генерирования вредоносных программ (при помощи которых создание угроз не требовало знаний в области программирования), публикация исходного кода вредоносных программ (что позволило злоумышленникам с минимальным опытом программирования создавать новые разновидности угроз), а также злоупотребление уязвимостями популярных функций, приложений и механизмов сценариев. В 2015 году мы увидим аналогичную картину на мобильных платформах. Число коммерческих и общедоступных вредоносных программ для мобильных устройств растет, и результаты этого роста, вероятно, проявят себя в скором будущем. Появление пакетов для генерирования мобильных вредоносных программ, снижающих входной барьер для потенциальных преступников, — лишь вопрос времени.

Apple iPhone 6 со специальной микросхемой беспроводной связи ближнего радиуса действия (near field communication — NFC) и встроенным электронным кошельком узаконит использование NFC для электронных платежей. В 2015 году другие производители мобильных устройств быстро внедрят эти технологии, и пользователи начнут совершать денежные операции с их помощью. Поскольку эти операции совершаются с торговыми терминалами, столь любимыми киберворами, они станут важной целью для злоумышленников. В 2015 году исследователи, скорее всего, обнаружат уязвимости в оборудовании NFC и программном обеспечении электронных кошельков, а киберворы попытаются эти уязвимости использовать.

Способ установки вредоносных программ для мобильных устройств практически не изменится. Надежным магазинам приложений, таким как Apple App Store и Google Play, как правило, удается не допускать вредоносные приложения на свои страницы, однако иногда это всё же случается. Кроме того, существует множество ненадежных магазинов приложений и сайтов с прямой загрузкой приложений, и приложения, полученные из этих источников, часто содержат вредоносный код. Во многих случаях пользователи попадают на такие злоумышленные сайты из-за вредоносной рекламы, количество которой на мобильных платформах быстро увеличивается. В 2015 году мы будем по-прежнему наблюдать быстрый рост количества вредоносной рекламы, направленной на мобильных пользователей, а также дальнейший рост числа вредоносных программ для мобильных устройств.

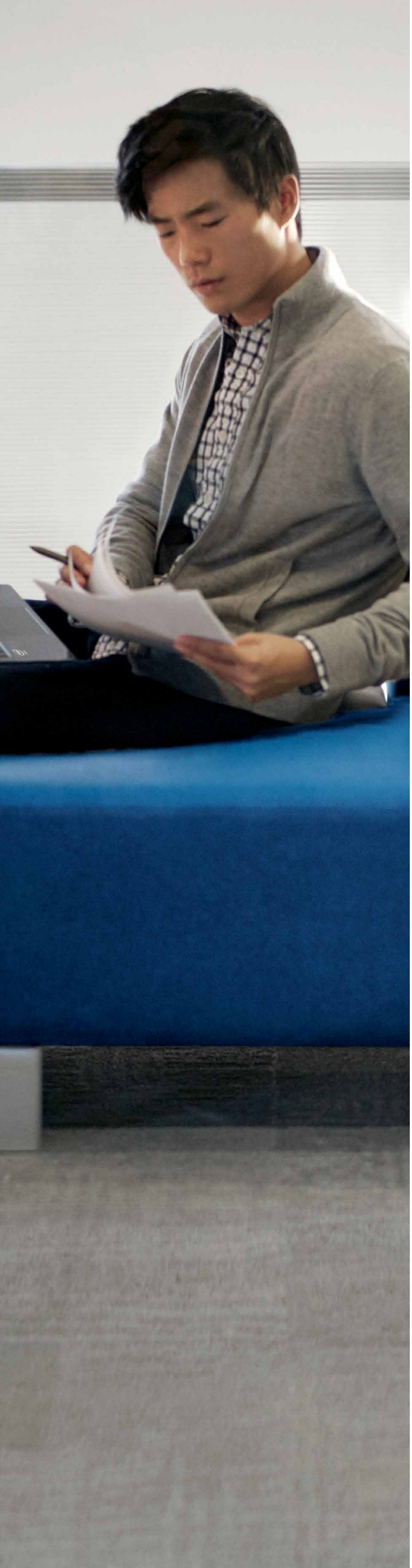
Кроме того, злоумышленники будут стремиться перенести эффективные методы вымогательства из мира ПК на мобильные платформы, в связи с чем мы ожидаем увеличения числа мобильных программ-вымогателей. После того, как эти программы будут доведены до совершенства на мобильных платформах, они станут для киберворов еще более выгодны, чем программы для ПК, потому что пользователи в значительной мере рассчитывают на возможность использования своих устройств для мгновенного доступа к важной информации, такой как контакты, расписания и маршруты. Положив так много яиц в одну мобильную корзину, пользователи готовы будут сделать всё, что угодно, чтобы восстановить доступ — в том числе и заплатить выкуп.

Крейг Шмугар (Craig Schmugar) и Бин Сунь (Bing Sun)

Торговые терминалы

Атаки на торговые терминалы (Point of sale — POS) будут по-прежнему выгодны. Значительно более широкое распространение электронных платежных систем на мобильных платформах создаст новые поверхности атаки, которыми киберпреступники непременно воспользуются.

По данным одной **статьи в Forbes**, в 2013 году объем розничных сделок составил 15 трлн долларов США. Поэтому платежные системы для совершения таких сделок представляют собой заманчивую цель для киберпреступников. В 2014 году мы наблюдали значительное увеличение числа атак на подобные системы, в том числе крупномасштабное нарушение безопасности в компании Home Depot. Всё это время пользователям досаждали скиммеры — устройства, незаконно считывающие информацию с кредитных карт. Скиммеры также получили еще большее распространение в этом году. Они устанавливались на самые разные устройства, включая считыватели карт в ресторанах, банкоматы и бензоколонки. Атаки на платежные терминалы происходят так часто, что в сфере розничной торговли борьба с ними стала частью повседневной деятельности. Несмотря на это, существенных усовершенствований в области безопасности терминалов не произошло, так что мы ожидаем, что число нарушений безопасности платежных терминалов будет расти и в 2015 году. Однако в США в конце 2015 года ситуация может измениться к лучшему, потому что розничные организации начнут внедрять смарт-карты, требующие ввода PIN-кода, и соответствующие устройства чтения.



В следующем году мы прогнозируем значительно более широкое использование электронных платежных систем. В обновленном iPhone компании Apple реализована технология NFC. Она позволяет использовать новую функцию iWallet, которая передает данные кредитной карты в платежную систему беспроводным способом, без контактного считывания с карты. Некоторые устройства на платформе Android также поддерживают NFC, и для проведения мобильных платежей они используют процесс под названием Host Card Emulation (эмуляция карт хост-процессором). Эта технология была внедрена в системах Visa и MasterCard, и теперь мобильные платежные приложения могут работать с устройствами, поддерживающими NFC. Наличие инфраструктуры позволяет нам ожидать широкого распространения новой технологии среди потребителей. Как следствие, мы также ожидаем успешных атак на платежные системы.

Электронные платежные системы неуязвимы для скиммеров, но они подвержены своим собственным рискам. Первостепенными среди этих рисков являются уязвимости лежащей в их основе технологии NFC. Некоторые из этих уязвимостей были освещены на конференции DEF CON 2013 и отслеживаются в рамках проекта **NFC Awareness Project**. Основная проблема заключается в том, что конфиденциальная информация теперь передается посредством беспроводного соединения, и существует возможность незаконного использования этого соединения злоумышленниками. Атаки такого рода имеют долгую историю, включающую такие эпизоды, как создание «снайперской винтовки Bluetooth» в 2005 году и дистанционное клонирование RFID-паспортов в 2009 году. Аналогичные атаки, нацеленные на NFC-устройства, вполне вероятны: **документированные уязвимости** уже существуют. В условиях, когда потребители передают платежную информацию по протоколу с известными уязвимостями, можно с высокой вероятностью предполагать, что в 2015 году начнутся атаки на эту инфраструктуру.

Дэн Ларсон (Dan Larson)

Вредоносные программы не только для Windows

Вредоносные программы для операционных систем, отличных от Windows, ожидает взрывной рост, которому способствует уязвимость Shellshock.

Во второй половине 2014 года мы узнали об **уязвимости Shellshock** — слабом месте Bash, командной оболочки операционных систем Unix, Linux и OS X. Эта уязвимость позволяет злоумышленникам выполнять произвольные команды на машине жертвы и, таким образом, относится к самой опасной категории — 10 из 10 баллов по шкале серьезности в **Национальной базе данных уязвимостей США**.

Отголоски этой недавно обнаруженной уязвимости будут ощущаться еще много лет. Огромное множество устройств работает под управлением той или иной разновидности Unix или Linux. К таким устройствам относятся маршрутизаторы, телевизоры, промышленные контроллеры, системы управления полетом и объекты критически важной инфраструктуры. Мы пока только начинаем осознавать масштабы этой уязвимости.

Такой вектор атаки даст злоумышленникам доступ к различным инфраструктурам — от бытовых приборов до предприятий, в значительной мере полагающихся на системы, отличные от Windows. В результате в 2015 году ожидается значительный рост числа вредоносных программ для этих систем. Злоумышленники попытаются нажиться на утечках данных, требованиях выкупа, внедрении спам-ботов и других видах преступной деятельности. Shellshock будет оставаться предметом заголовков, в то время как злоумышленники будут пользоваться пробелами в защите новых и старых уязвимых устройств для осуществления своих атак.

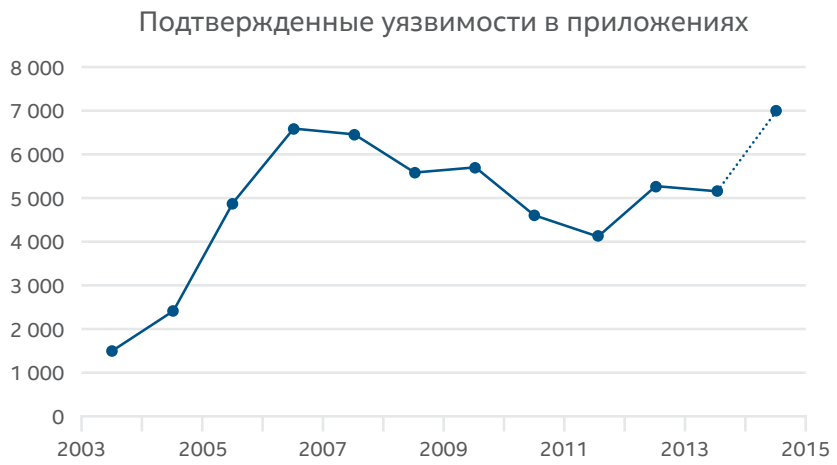
Крейг Шмугар (Craig Schmugar)

Уязвимости

Число уязвимостей растет вместе с числом ошибок в популярном программном обеспечении.

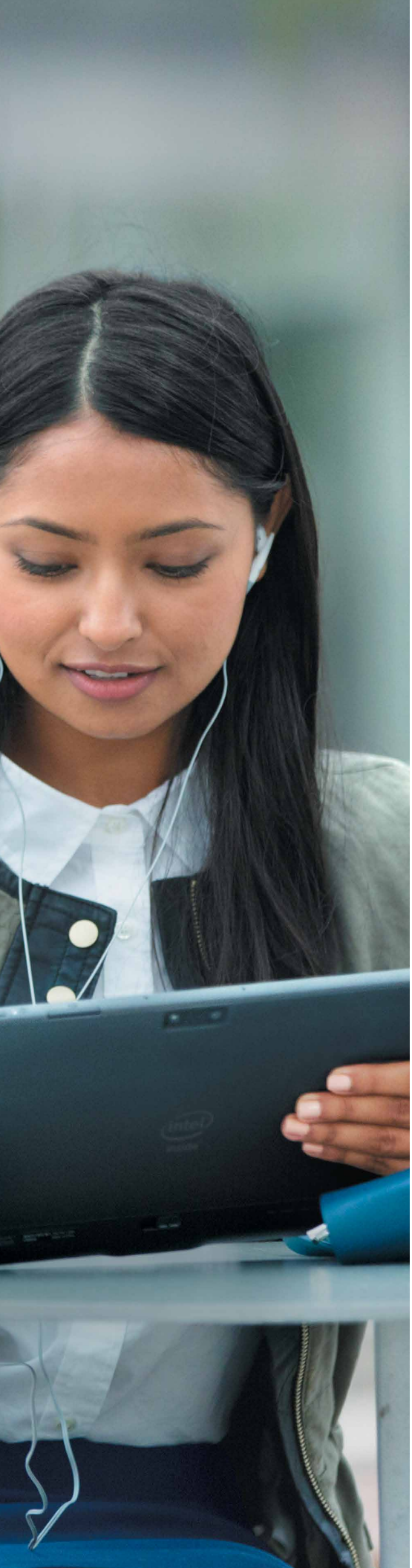
Данные из Национальной базы данных уязвимостей правительства США показывают, что число уязвимостей за последние три года увеличилось. Исходя из приблизительно 5 200 записей, внесенных в базу по состоянию на 30 сентября, общее число уязвимостей, зарегистрированных в 2014 году, может побить рекорд, установленный в 2006 году.

Одно только количество уязвимостей не позволяет в точности оценить уровень риска, потому что он зависит от множества взаимосвязанных факторов — это и быстрота появления и объем исправлений, и серьезность каждой отдельной уязвимости, и продолжительность подверженности, и многое другое. Эти числа, тем не менее, позволяют оценить состояние экосистемы в целом.



Источник: Национальный институт стандартов и технологий (США) — Национальная база данных уязвимостей

В период с 2006 по 2011 год мы наблюдали снижение темпов появления новых уязвимостей, но с тех пор ситуация изменилась. Снижение темпов могло быть связано с контролем стека в компиляторах, предотвращением выполнения данных и рандомизацией распределения адресного пространства в 64-разрядном программном обеспечении. Современная тенденция роста отражает новые методы использования уязвимостей, такие как переключение стека, а также программирование с использованием операторов возврата и безусловного перехода в сочетании с более глубоким пониманием 64-разрядного программного обеспечения «черными» и «белыми» хакерами, ищущими уязвимости.



Источник: McAfee Labs

Специалисты McAfee Labs проанализировали свой «зоопарк» вредоносных программ, чтобы определить, как часто эти программы используют известные уязвимости. В зависимости от квартала, известные уязвимости используются в 1–6 % всех новых образцов вредоносных программ. Показатель за этот период составил около 2 %, то есть на использовании известных уязвимостей основана 821 000 новых образцов вредоносных программ. По мере роста абсолютного числа образцов, использующих уязвимости, растет и общее число вредоносных программ; поэтому доля основанных на уязвимостях образцов остается относительно неизменной.

Мы не ожидаем в 2015 году значительных изменений в отношении способов защиты от уязвимостей, доступных разработчикам приложений или операционных систем. Более того, скорость распространения новых и существующих передовых методов вряд ли увеличится. Таким образом, мы ожидаем, что число новых уязвимостей продолжит расти — а следовательно, расти будет и число вредоносных программ, их использующих.

Игорь Муттик (Igor Muttik) и Франсуа Паже (François Paget)

Выход из «песочницы»

Выход из «песочницы» станет значительной проблемой в области ИТ-безопасности.

Многие критически важные и популярные приложения, в том числе Microsoft Internet Explorer, Adobe Reader и Google Chrome, располагают собственными технологиями «песочницы», позволяющими изолировать вредоносное поведение. Поскольку эти программные «песочницы» эффективно останавливают многие виды атак, создатели вредоносных программ ищут способы обхода этого защитного механизма.

Рассмотрим для примера Internet Explorer. Вредоносные программы, не способные обойти его «песочницу», не представляют угрозы для пользователя, потому что изменения, вносимые эксплойтом в систему, не сохраняются. Однако в Internet Explorer существуют две версии технологии «песочницы»: защищенный режим (PM) и расширенный защищенный режим (EPM). В настоящее время Internet Explorer версий 10 и 11 по умолчанию работает в режиме PM, и наши исследования показали, что обойти режим PM относительно легко. Хотя на практике мы пока не видели эксплойтов, способных обойти режим PM или EPM, условия для этого существуют, так что в 2015 году мы с большой вероятностью увидим случаи выхода из «песочницы» Internet Explorer с последующими атаками «нулевого дня».

Уязвимости, способные привести к выходу программы из «песочницы», были обнаружены и раскрыты во многих популярных клиентских приложениях. Документированные уязвимости найдены в Adobe Reader и Flash, Chrome, Apple Safari, Oracle Java и Internet Explorer. Эти уязвимости послужили поводом для дальнейшего анализа со стороны как исследователей, так и злоумышленников. Например, на конференции BlackHat 2014 исследователи рассказали о четырех методах успешного обхода «песочницы», использовавшихся победителями конкурса хакеров Pwn2Own в этом году. Фактически, почти все «победы» на этом конкурсе включали в себя успешный выход из «песочницы» на последнем этапе взлома.

Мы уже видели методы, позволяющие использовать уязвимости и выходить из «песочницы». Через какое-то время эти методы будут предложены киберпреступникам на черном рынке. Мы полагаем, что это произойдет в 2015 году.

Еще один дополнительный прогноз. До настоящего времени киберпреступники в основном направляли свои усилия на выход из «песочницы». Однако всё более популярные автономные системы «песочниц», предлагаемые поставщиками программных средств обеспечения безопасности, ставят перед киберворами новый барьер. В свою очередь, киберпреступники начали искать способы создания вредоносных программ, способных выходить из таких «песочниц». Сегодня значительное число семейств вредоносных программ способно распознавать «песочницы» и избегать их. Тем не менее, пока что нам неизвестно о таком вредоносном ПО, которому на практике удалось бы успешно использовать уязвимости низкоуровневой оболочки для выхода из автономной «песочницы». Мы ожидаем, что в 2015 году эта ситуация изменится.

Хайфей Ли (Haifei Li), Рик Саймон (Rick Simon), Бин Сунь (Bing Sun) и Стенли Жу (Stanley Zhu)

Главные темы

Уязвимость BERserk: безопасность соединений под сомнением

Злоупотребление доверием: использование слабых звеньев в системах сетевой безопасности

Поделитесь своим мнением

Уязвимость BERserk: безопасность соединений под сомнением

Джеймс Уолтер (James Walter)

В статье **«Злоупотребление доверием: использование слабых звеньев в системах сетевой безопасности»** представлен обзор текущих проблем в контексте определения благонадежности сайтов в Интернете. В данной статье рассматривается конкретная уязвимость, значительно снижающая степень доверия к веб-сайту.

Отдел исследований сложных угроз компании Intel Security уделяет особое внимание нескольким ключевым факторам, влияющим на безопасность интернет-транзакций и процессов передачи данных. Одним из таких факторов является базовый уровень безопасности связи. Сюда входит глубокий анализ угроз и уязвимостей в протоколах SSL/TLS, TPM 2.0, побочных криптографических каналах и прочих областях, принимаемых как само собой разумеющееся при оценке модели доверия как «целостной».

В сентябре отдел исследований сложных угроз компании Intel Security опубликовал подробные сведения об уязвимости, получившей имя BERserk. Уязвимость названа так по состоянию, возникающему в результате синтаксической обработки определенных закодированных последовательностей, использующих базовые правила кодирования (Basic Encoding Rules — BER), в алгоритме проверки цифровой подписи RSA. Компания Intel Security и исследователь безопасности Антуан Делинья-Лаво (Antoine Delignat-Lavaud) сообщили об этой уязвимости компании Mozilla, предложив выпустить обновления для ряда продуктов, включая Firefox, Thunderbird, SeaMonkey и NSS. Компания Google также обновила свой браузер и операционную систему Chrome, поскольку в них используется криптографическая библиотека NSS.

Ошибка кроется в алгоритме проверки цифровых подписей RSA, в частности в некорректной синтаксической обработке при проверке последовательностей, закодированных по стандарту ASN.1. Эта уязвимость является вариантом обнаруженной ранее уязвимости Bleichenbacher PKCS#1 v1.5, описанной под номером **CVE-2006-4339**, которая позволяет злоумышленникам подделывать цифровые подписи RSA. В подверженных уязвимости системах выполняется поиск заполняющих байтов 0xFF в закодированных сообщениях до тех пор, пока не будет найден разделяющий байт 0x00. Затем система подтверждает соответствие данных DigestInfo и свертки сообщения ожидаемым значениям без проверки выравнивания их по правому краю в закодированном сообщении (EM), что гарантировало бы отсутствие лишних байтов после текста свертки. Без такой проверки возможно составить такое закодированное сообщение EM', которое будет содержать дополнительный мусор непосредственно после текста свертки, при этом удовлетворяя следующим условиям проверки цифровой подписи:

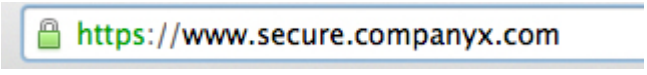
EM' = 00 01 FF FF FF FF FF FF FF FF 00 DigestInfo MessageDigest Garbage

Дополнительный мусор в закодированном сообщении дает злоумышленнику возможность генерировать цифровую подпись RSA, которая после возведения в куб модуля RSA дает то самое значение EM':

EM' = (s')^3 mod N

Злоумышленник может создавать цифровые подписи RSA, не зная закрытого ключа {p,q,d}, что позволяет ему успешно подделывать подписи RSA.

Таким образом, атакующий может подделывать сертификаты RSA, не зная соответствующих закрытых ключей RSA. Что это означает? Как это касается нас?



Уязвимость BERserk предоставляет злоумышленникам возможность установления интернет-сеансов с реализацией незаметных для пользователя атак типа «незаконный посредник». По уровню потенциальной опасности эта уязвимость сравнима с Shellshock.

Ответ прост. Мы, порядочные граждане и пользователи Интернета, уже привыкли к определенной модели доверия. Осуществляя определенные интернет-транзакции (банковские, медицинские и прочие операции, требующие передачи личных данных), мы знаем, как проверить, защищен ли сеанс. Нас учили, что URL-адрес должен начинаться с «https», а рядом должен отображаться «замóк». Так мы определяем, что веб-сайт безопасен и не передает какие-либо данные третьим сторонам, имеющим преступные намерения.

Уязвимость BERserk и аналогичные ей меняют правила игры. Мы больше не можем быть уверены в защищенности сеансов с использованием протоколов SSL/TLS. Благодаря возможности точной имитации цифровых подписей RSA злоумышленник может создать сеанс связи с «незаконным посредником» в самых разных сценариях.

Уязвимость BERserk могла повлечь за собой атаки типа «незаконный посредник»

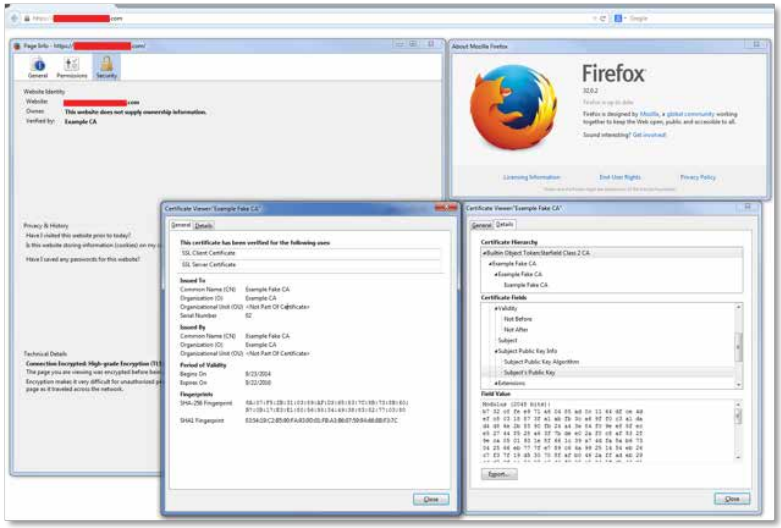
Например, под угрозой может оказаться конфиденциальность и целостность сеанса связи между клиентом и веб-сайтом банка. Пользователи с фальшивыми сертификатами могут посещать сайты и даже просматривать сами сертификаты, чтобы убедиться в их подлинности. Сертификаты будут неотличимы от настоящих. Аналогичным образом, пользователь может стать жертвой обмана, войдя на веб-сайт врача, чтобы посмотреть записи о себе. То же касается и уплаты налогов через Интернет. Подобных сценариев множество.

Угрозе подвержены не только веб-сайты и программные продукты. Криптографические библиотеки, используемые в аппаратных устройствах, например смартфонах, содержат конфиденциальные данные, доступ к которым предоставляется приложениям по требованию. Представим, что мобильный телефон или планшетный компьютер имеет защищенную память и среду выполнения для предоставления криптографических функций программному обеспечению устройства. На устройстве установлено микропрограммное обеспечение с цифровой подписью, предотвращающее внесение несанкционированных изменений вредоносным ПО или пользователем. Однако из-за уязвимости BERserk микропрограммное обеспечение попадает под угрозу, в результате чего под сомнение ставится целостность и конфиденциальность информации, защищаемой данным аппаратным компонентом.

Узнайте, как McAfee помогает защититься от этой угрозы.

В частности, такая модель широко используется для хранения информации о банковских счетах, используемой для осуществления платежей с применением специализированных торговых терминалов — например, в платежных системах на основе технологии NFC, где требуется хранение данных банковских карт в устройстве. В таких случаях злоумышленники могут манипулировать сеансами различными способами, включая перехват и модификацию ввода/вывода или простой сбор и хищение конфиденциальных данных.

В ходе исследований нам удалось подделать даже 1024- и 2048-разрядные сертификаты RSA. Эта возможность может быть на руку злоумышленникам. Злоумышленники могут создать поддельные сертификаты с помощью Mozilla NSS и цепочка этих сертификатов будет признана Mozilla NSS как достоверная.



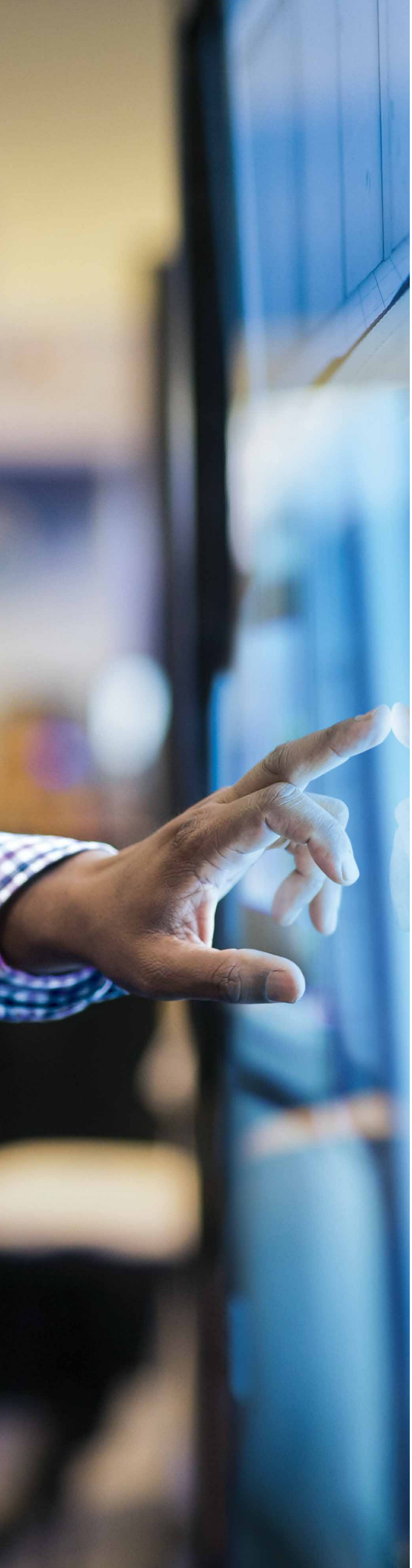
Поддельный сертификат в Firefox

Отдел исследований сложных угроз компании Intel Security продолжает изучение этих проблем и их влияния на сценарии, не предусматривающие использования браузера. В решении стоящих перед нами проблем мы также сотрудничаем с компьютерными группами быстрого реагирования (CERT) и поставщиками затронутых уязвимостью компонентов.

Поставщики затронутых криптографических библиотек продолжают выпускать обновления и публиковать соответствующие указания. Mozilla и Google уже обновили свои продукты. Затронутым уязвимостью пользователям необходимо следовать указаниям поставщиков ПО и поддерживать актуальность своих систем.

Дополнительные сведения об уязвимости BERserk можно найти в следующих публикациях.

- Отчет об уязвимости BERserk: **Part 1: RSA signature forgery attack due to incorrect parsing of ASN.1 encoded DigestInfo in PKCS#1 v1.5** (Часть 1. Атака с подделкой цифровых подписей RSA вследствие некорректной синтаксической обработки данных DigestInfo, закодированных по стандарту ASN.1, в PKCS#1 v1.5)
- Отчет об уязвимости BERserk: **Part 2: Certificate forgery in Mozilla NSS** (Часть 2. Подделка сертификатов в Mozilla NSS)
- Intelsecurity.com: **BERserk**
- Computer Emergency Response Team: **VU#772676**
- Национальная база данных уязвимостей (США): **CVE-2014-1568**



Злоупотребление доверием: использование слабых звеньев в системах сетевой безопасности

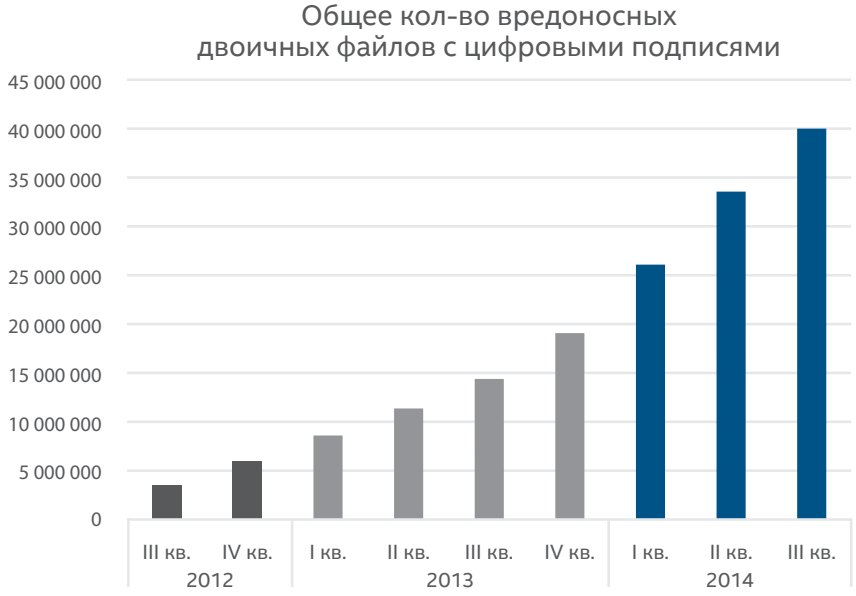
Седрик Кошен (Cedric Cochin) и Крейг Шмугар (Craig Schmugar)

Изо дня в день большинство людей в мире доверяют свою жизнь электронным устройствам — будь то персональный компьютер, мобильный телефон, телевизор или даже автомобиль. Мы привыкли доверять этим устройствам и в большинстве случаев уверены, что они предоставляют точную информацию.

Однако доверие необходимо заслужить и подкрепить делом, а это требует времени и средств. Компании ежегодно тратят миллионы долларов на укрепление позиций своих брендов, зная, что эти вложения окупаются сторицей. Они понимают, что потребителей легче склонить к действию, когда с товаром связано доброе имя.

Злоумышленники тоже знают об этом, однако им не всегда хватает времени, ресурсов и терпения, чтобы выстроить доверительные отношения с жертвой. Им остается искать способы использовать чужие инвестиции в доверие и чужую репутацию.

Ежедневно фиксируется множество фактов злоупотребления доверием, и тенденция неблагоприятна. Например, вредоносные двоичные файлы с цифровыми подписями, которые отслеживает McAfee Labs, являются одной из форм злоупотребления доверием, так как злоумышленники маскируют вредоносные программы, выдавая их за легитимные сертифицированные файлы. Число вредоносных двоичных файлов с цифровыми подписями постоянно растет с того момента, кода мы начали их отслеживать в 2007 году.

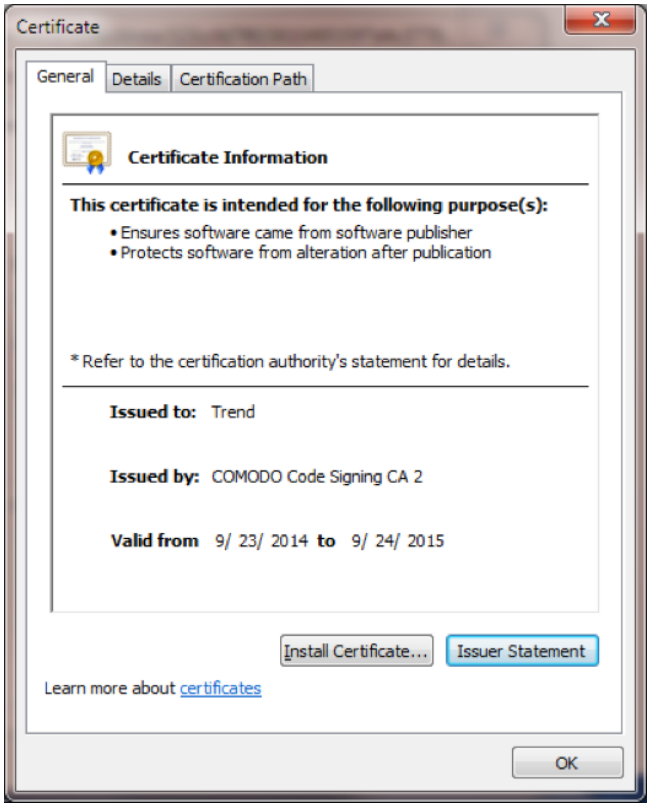


Авторы вредоносных программ используют цифровые подписи, злоупотребляя доверием пользователей и репутацией продуктов и операционных систем.
Источник: McAfee Labs

Наследование доверия позволяет злоупотреблять лояльностью пользователей по отношению к бренду. Веб-сайты часто смешивают репутацию благонадежных брендов с другими брендами, представленными на той же странице.

Наследование доверия

В течение многих лет для установления доверия в процессе транзакции достаточно было простого подтверждения бренда. Сегодня потребителю необходимо удостовериться еще и в том, что благонадежный бренд, в свою очередь, находится в доверительных отношениях с другими брендами, представленными на его веб-сайте. В сентябре была обнаружена **сеть вредоносной рекламы Kyle and Stan**, распространявшая вредоносное содержимое посредством рекламных объявлений на популярных веб-сайтах, таких как amazon.com, ads.yahoo.com и youtube.com, а также в **крупных рекламных сетях, таких как Double-Click и Zedo**. Сообщалось, что кампания в рекламной сети Zedo **принесла ущерб пользователям** ведущих веб-сайтов в рейтинге компании Alexa, внедрив в их компьютеры модификации «троянского коня» CryptoWall с цифровыми подписями. Использованная цифровая подпись была предоставлена на имя «Trend», что указывает на попытку имитации поставщика систем безопасности — компании Trend Micro. Первичная телеметрия показывает, что в наибольшей степени угрозе оказались подвержены пользователи из Северной Америки. К сожалению, пользователи склонны доверять предположительно безопасным брендам «по ассоциации», на что и рассчитывают злоумышленники.



Сертификат, использованный в цифровой подписи CryptoWall

Доверительные отношения между потребителем и брендом часто становятся объектом злоупотреблений. Примером могут служить приложения-подделки, в которых вирусы или «троянские кони» представляются как легитимные и зачастую популярные программы. В прошедшем квартале мошенники активно пытались продвигать подделку «FlashPlayer11» как подлинный продукт Adobe. По данным счетчиков загрузок Google Play и телеметрии McAfee Mobile Security, мошенникам удалось добиться некоторого успеха в обмане пользователей.

Одно из нескольких поддельных приложений «FlashPlayer11» в магазине Google Play

Экземпляры вредоносной программы «FlashPlayer11» (Android/Fladstep.B), обнаруженные программным обеспечением McAfee на мобильных устройствах

Рекомендовать отчет

Злоумышленники пользуются доверием пользователей к продуктам или операционной системе для реализации «боковой загрузки» DLL-файлов — распространенного метода внедрения вредоносного кода.

Доверие к продуктам и операционной системе

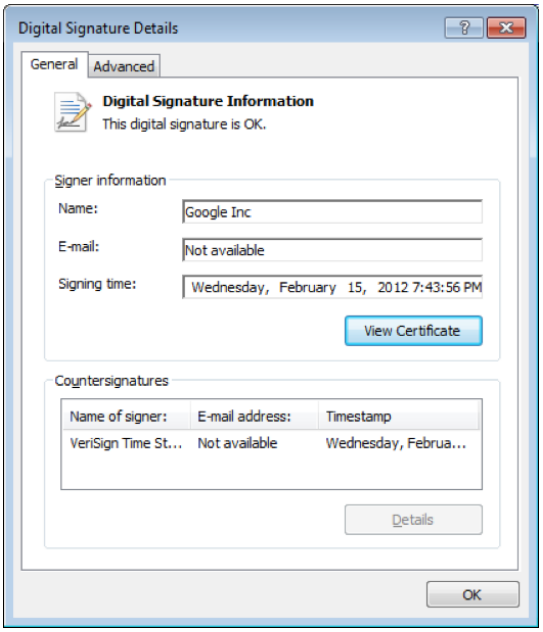
Современные продукты для обеспечения безопасности часто основаны на доверии. Для увеличения производительности и снижения числа ложных срабатываний проводится инвентаризация системы, в процессе которой определяются «безопасные» приложения, чье поведение уже не подвергается тщательному анализу. Злоумышленники знают, что если вредоносный код удается протащить под прикрытием доверенного приложения, то шансы на успех значительно возрастают. Вредоносные программы используют этот трюк уже много лет, реализуя так называемый механизм «боковой загрузки» DLL-файлов. Этот механизм предполагает выполнение легитимного приложения, которое, в свою очередь, выполняет код из внешней библиотеки. Злоумышленники создают вредоносное содержимое, имитирующее необходимый программе DLL-файл, заставляя таким образом заведомо «чистое» приложение выполнять вредоносный код.

Стандартный сценарий: благонадежный исполняемый файл загружает благонадежную библиотеку

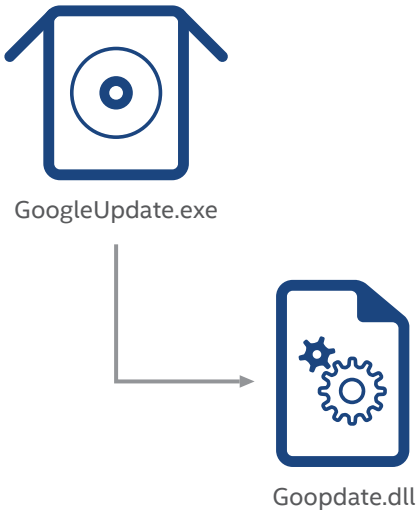
Вредоносный сценарий: благонадежный исполняемый файл загружает неизвестную вредоносную библиотеку

Рекомендовать отчет

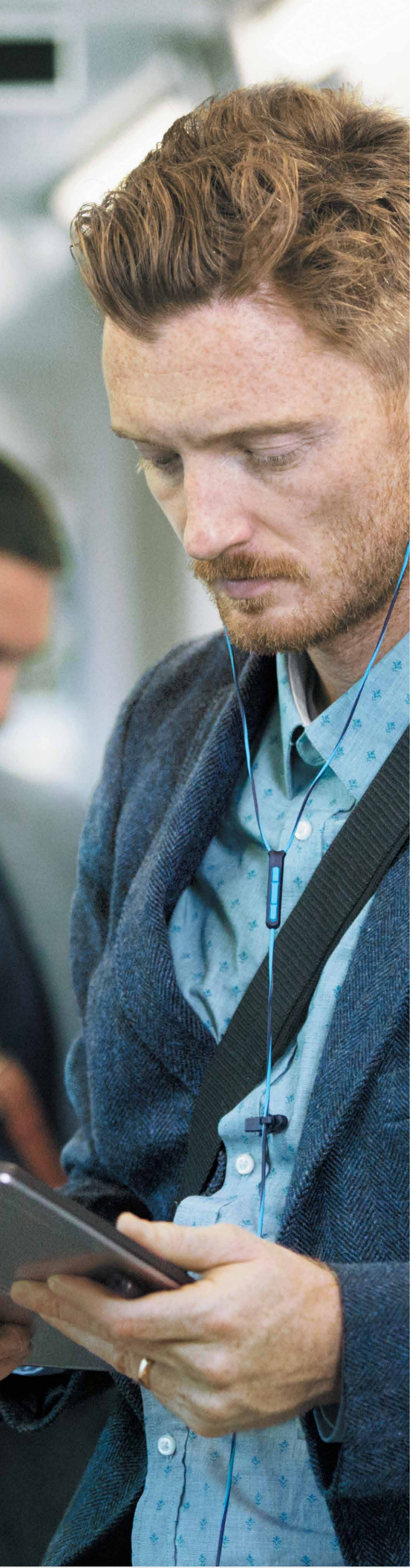
В третьем квартале специалисты McAfee Labs наблюдали атаки с использованием «боковой загрузки» DLL-файлов, направленные на относительно новую цель — приложение Google Updater с цифровой подписью. Новые модификации вредоносной программы PlugX выступают в роли импортируемого файла goopdate.dll, но в стремлении скрыть свои действия PlugX этим не ограничивается. Модуль goopdate.dll — это не более чем посредник, который считывает данные из зашифрованного файла goopdate.dll.map, расшифровывает их в память и передает управление выполнением полученному коду. Такой подход дает возможность замаскировать функции промежуточного DLL-файла. Каждый из трех участвующих в атаке компонентов сам по себе безвреден, и при анализе файлов по отдельности можно легко прийти к неверному заключению. Однако при рассмотрении файлов в комплексе вредоносные намерения становятся очевидными. Такой метод позволяет злоумышленникам использовать в своих интересах продукты, доверяющие файлам, подписанным легитимным сертификатом Google Inc.

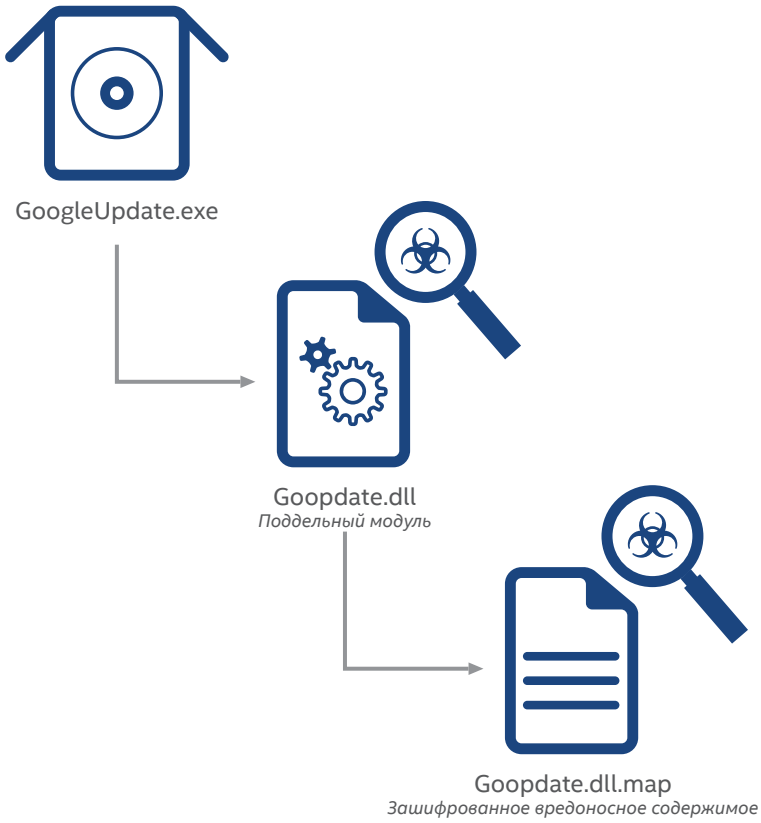


Легитимное приложение Google Updater с цифровой подписью

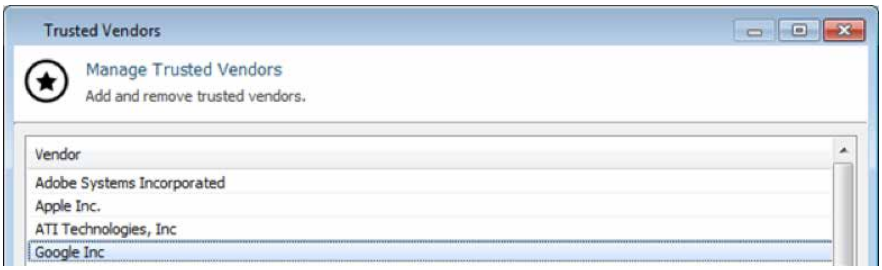


Легитимное приложение Google Updater загружает библиотеку Google

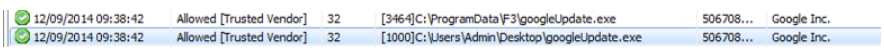




Легитимный исполняемый файл Google загружает вредоносный модуль, который затем загружает вредоносную программу; приложение Google Updater загружает библиотеку Google



Это приложение на основе «белых» списков по умолчанию доверяет приложениям Google

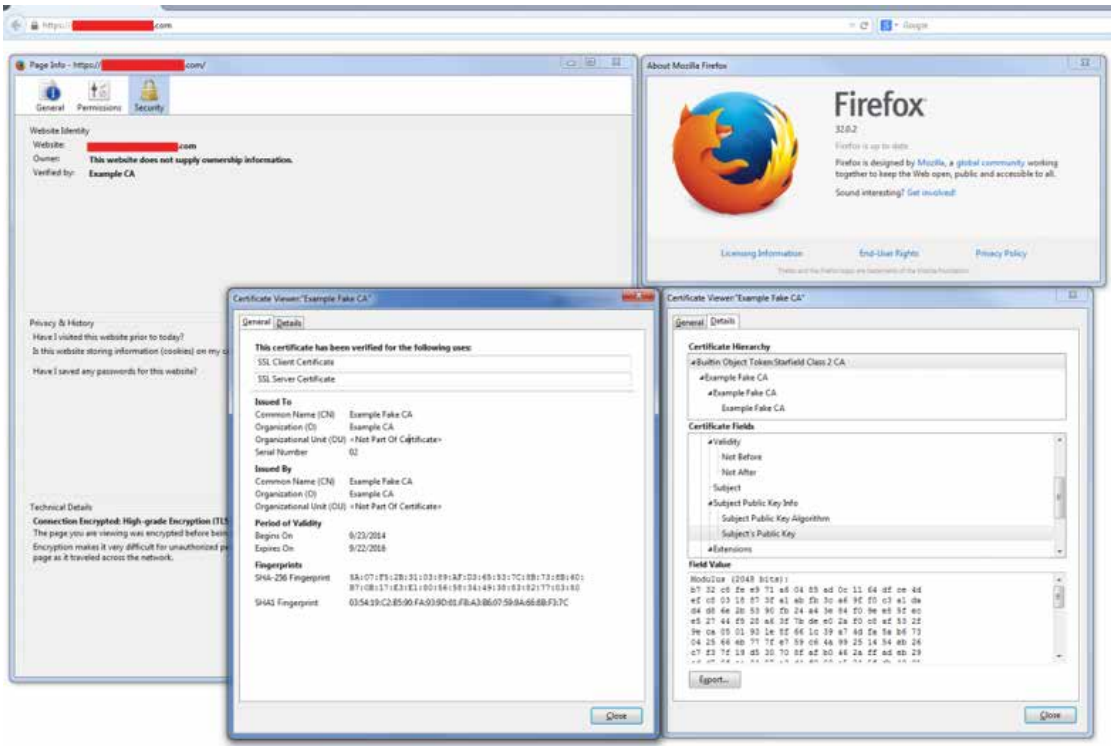


Приложение доверенного поставщика (Trusted Vendor) по умолчанию допускается в систему

В недавно обнаруженной **модификации комплекта для использования уязвимостей под названием Angler** применяется значительно более совершенный механизм злоупотребления доверием к приложениям. Новый механизм позволяет выполнять вредоносное содержимое без предварительной записи его на диск. Программный код запускается сразу же после доставки, не оставляя возможности разрешить или запретить его выполнение на основе «белых» списков. Это также позволяет обойти проверку файла на наличие вирусов, так как на момент атаки файла как такового не существует.

Другая форма злоупотребления доверием касается взаимодействия между операционной системой и средствами управления маршрутизацией в сети. Приложения полагаются на безопасность средств связи, предоставляемых операционной системой. Например, приложения рассчитывают на то, что их трафик будет маршрутизироваться корректно и безопасно, направляясь указанным получателям. Одним из хорошо известных семейств вредоносных программ являются программы, изменяющие систему DNS. Единственным назначением таких вредоносных программ является изменение конфигурации DNS с целью принудительного перенаправления всех DNS-запросов на DNS-сервер, контролируемый злоумышленником. Хоть браузер и ведет себя так, будто взаимодействует с благонадежным веб-сайтом банка, на самом деле обмен данными выполняется с подставным сайтом или невидимым вредоносным прокси-сервером, перехватывающим данные пользователя.

Выявить взаимодействие пользователя с подставным веб-сайтом не так легко, как кажется. Связанная со стандартом ASN.1 уязвимость BERserk, **о которой компания Intel сообщила 24 сентября** и которая подробно рассматривается в статье **«Уязвимость BERserk: безопасность соединений под сомнением»**, наглядно показывает, как легко заставить браузер поверить в то, что сеанс связи установлен с благонадежным веб-сайтом. Эта уязвимость позволяет злоумышленникам подделывать цифровые подписи RSA с целью обхода механизмов проверки подлинности на веб-сайтах, использующих протокол SSL/TLS. Поскольку сертификат можно подделать для любого домена, эта проблема вызывает серьезную озабоченность по поводу целостности и конфиденциальности данных при посещении веб-сайтов, которые мы заведомо считаем безопасными.



Пример использования уязвимости BERserk в реализации стандарта ASN.1

Узнайте, как McAfee помогает защититься от этой угрозы.

Злоупотребление алгоритмами разрешения имен также ставит под удар операционные системы. Указав системе вредоносный сервер обновлений и используя надежный сертификат не по прямому назначению, злоумышленникам удается развертывать в системе вредоносное ПО. Хорошо известным примером служит **вредоносная шпионская программа Flame**, обнаруженная в 2012 году. Код, который содержала эта программа, заражал компьютеры путем перехвата управления над механизмом обновления операционной системы Microsoft Windows, используемым для распространения исправлений системы безопасности.

Аналогичные атаки могут быть направлены на компоненты сети, например на домашние маршрутизаторы, что позволит злоумышленникам перехватывать трафик настольных и портативных компьютеров, а также телевизоров, игровых приставок и прочих подключенных к Интернету устройств. Подобная атака имела место в августе, когда пользователи сетевого хранилища данных Synology сообщили о заражении «троянской» программой-вымогателем SynoLocker, захватившей их данные.

Доверие — это еще один шанс для злоумышленника, поэтому число случаев злоупотребления доверием быстро растет. Пользователи должны быть постоянно настороже. Продукты для обеспечения безопасности должны давать пользователям возможность самостоятельно определять, чему доверять, а чему нет. Также необходимы гибкие средства управления, позволяющие наделять доверенные программы бóльшими полномочиями при одновременном ограничении полномочий других программ. Невнимание к этой проблеме может привести к росту недоверия ко многим технологиям, используемым для доступа к информации в Интернете, и, возможно, к общему снижению объемов пользования Интернетом.

Защита от злоупотребления доверием

Злоупотребление	Мера противодействия
Наследование доверия (вредоносная реклама), доверие к продуктам и операционной системе	Поддержание операционных систем, приложений и программных систем безопасности в актуальном состоянии.
Средства использования уязвимостей («попутные загрузки»)	Поддержание систем в актуальном состоянии, посещение заслуживающих доверия веб-сайтов, предварительная проверка гиперссылок путем наведения на них указателя мыши для просмотра адреса, отказ от перехода по подозрительным ссылкам, полученным по электронной почте или в социальных сетях.
Злоупотребление брендами (фальшивые электронные письма, поддельные приложения, подставные домены)	Бдительность и проверка, ввод адресов вручную, поиск приложений на благонадежных веб-сайтах, выбор веб-сайтов с подтвержденной репутацией (большое количество загрузок, положительные отзывы), внимательное изучение запросов на предоставление разрешений приложениям.
Злоупотребление устройствами	Поддержание микропрограмм устройств в актуальном состоянии.

Статистика угроз

Вредоносные программы для мобильных устройств

Вредоносные программы

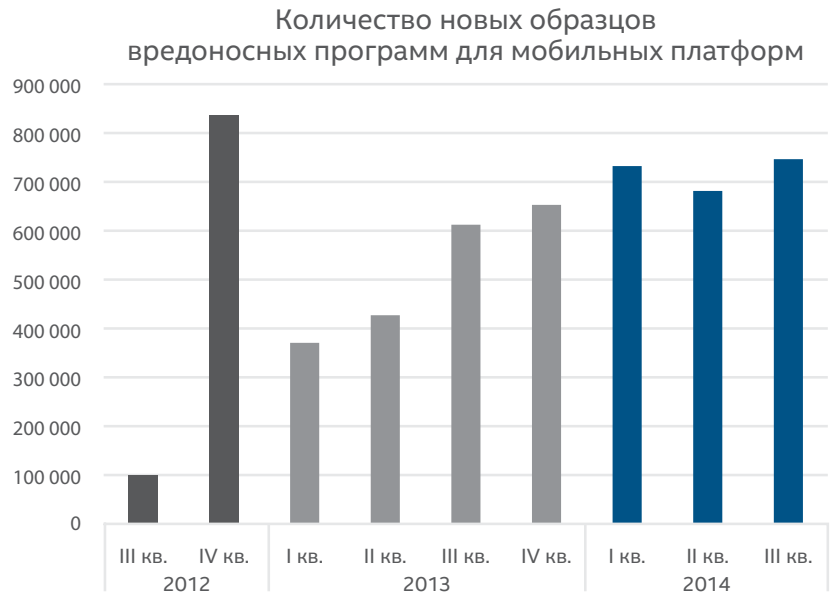
Веб-угрозы

Опасные сообщения

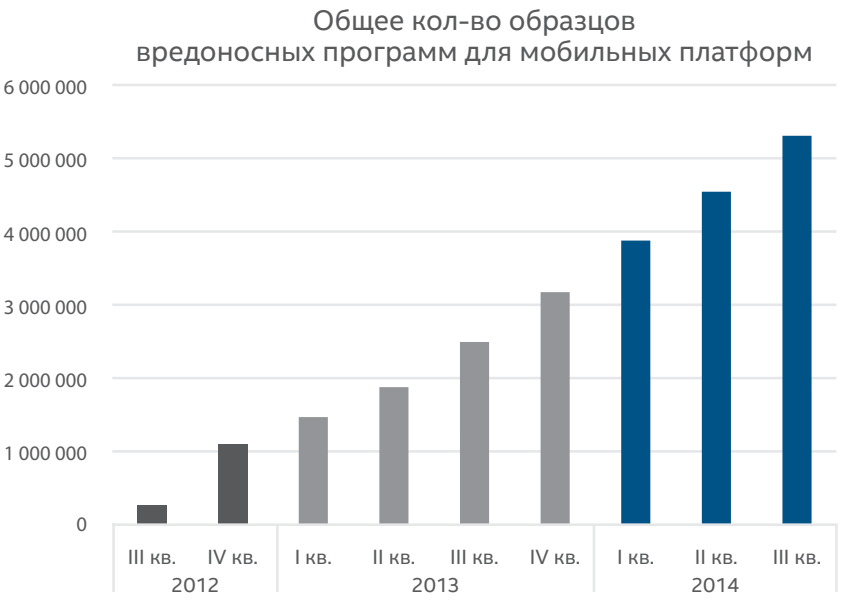
Сетевые угрозы

Поделитесь своим мнением

Вредоносные программы для мобильных устройств



Источник: McAfee Labs



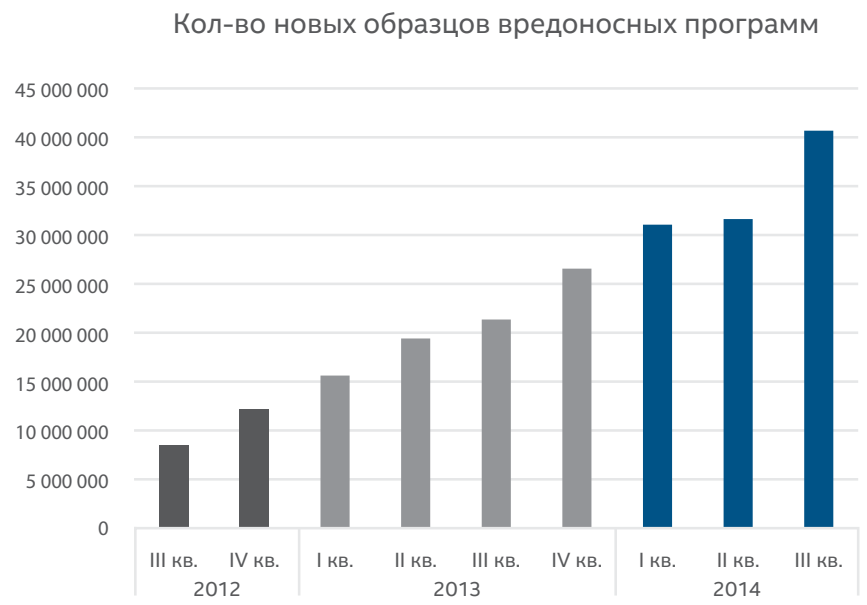
Источник: McAfee Labs

Общее число образцов вредоносных программ для мобильных устройств, зарегистрированных в третьем квартале 2014 года, превысило 5 миллионов. Это на 16 % больше, чем в предыдущем квартале, и на 112 % больше, чем в прошлом году.

Рекомендовать отчет

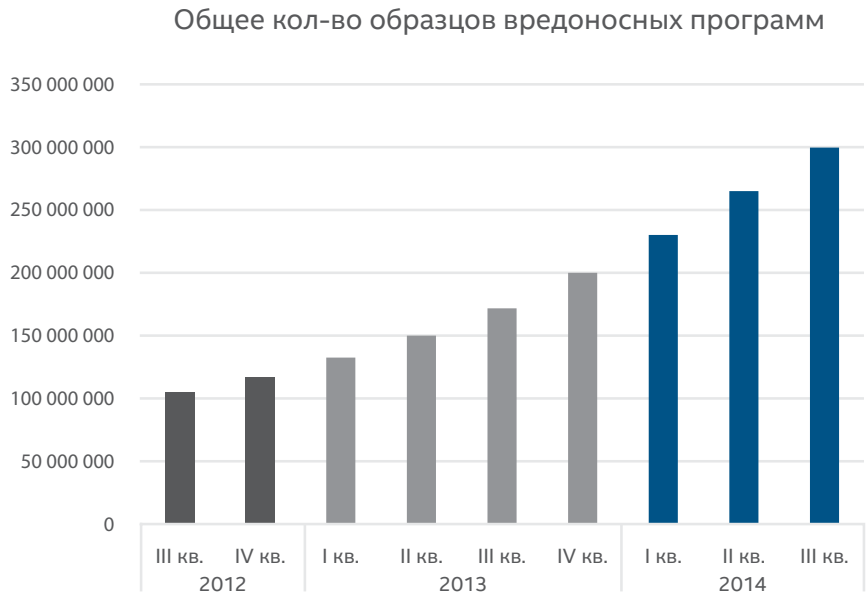
Вредоносные программы

Каждую минуту появляются 307 новых угроз, т. е. больше 5 угроз в секунду.



Источник: McAfee Labs

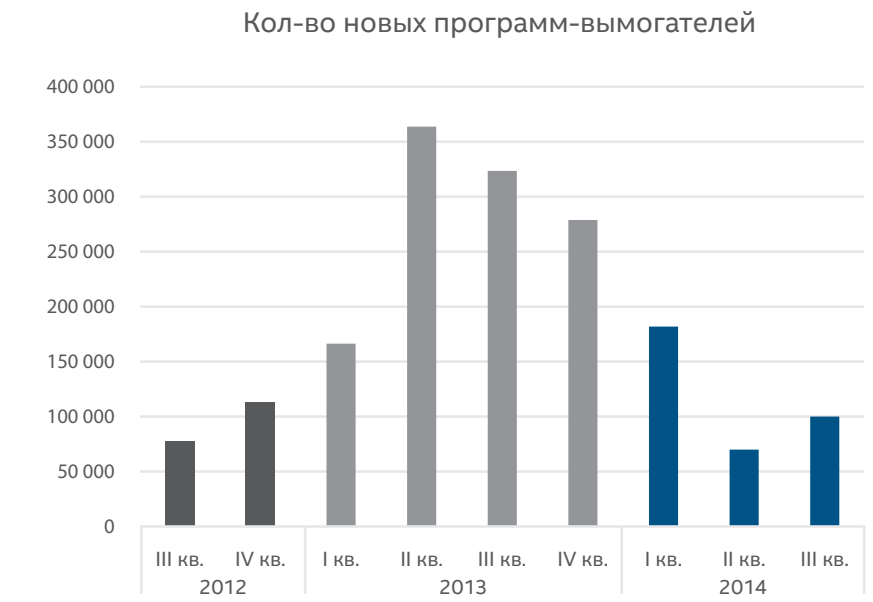
В третьем квартале 2014 года численность обитателей «зверинца» вредоносных программ McAfee Labs превысила 300 миллионов. Прирост по сравнению с прошлым годом составил 76 %.



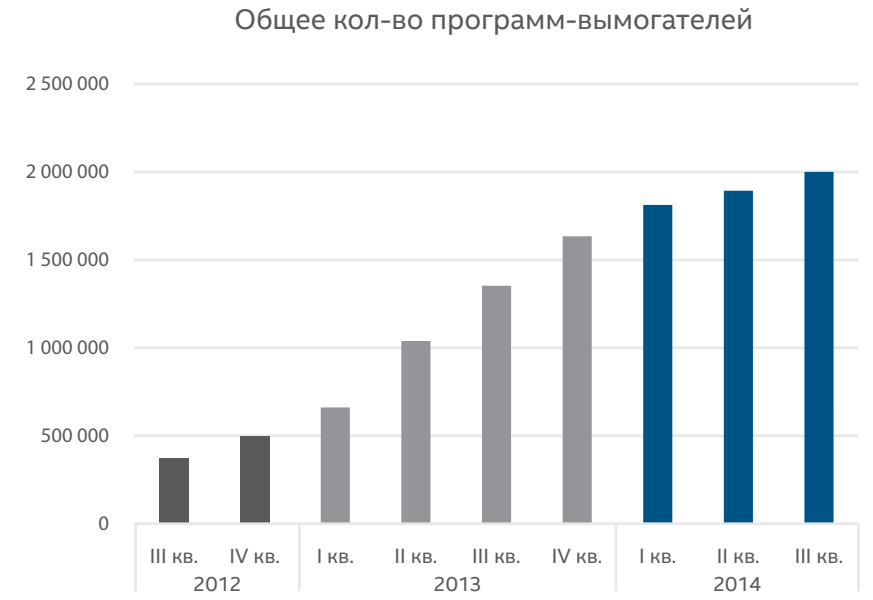
Источник: McAfee Labs

Рекомендовать отчет

Длившееся четыре квартала снижение числа новых образцов программ-вымогателей прекратилось. Мы были озадачены спадом, но нас не удивляет то, что их число снова растет.



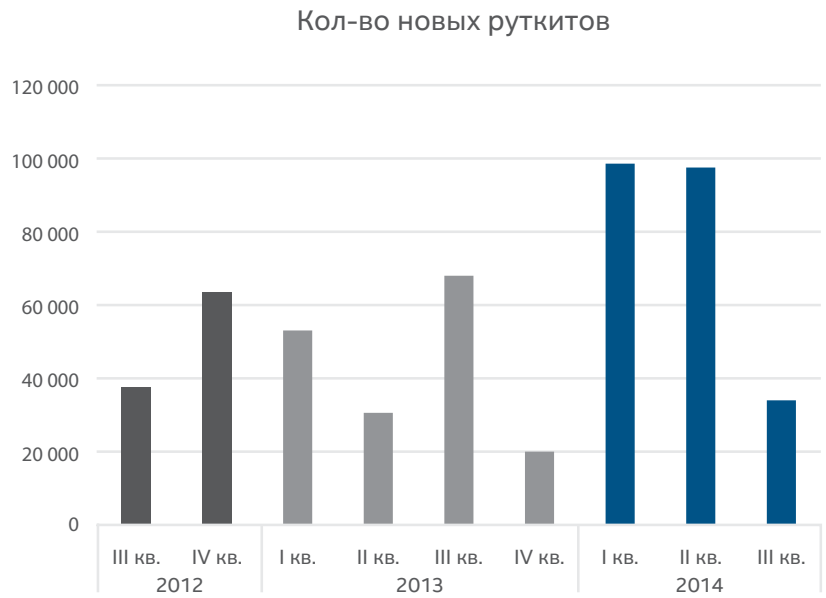
Источник: McAfee Labs



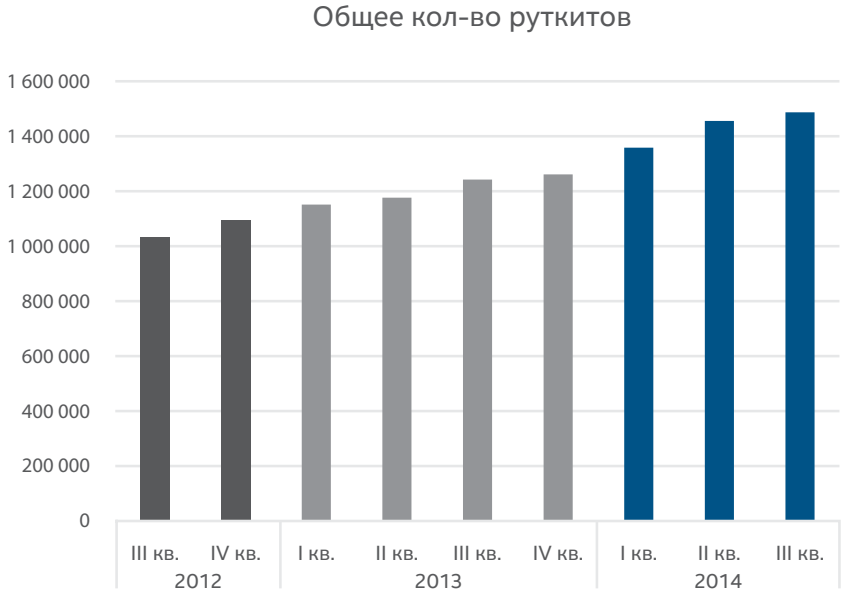
Источник: McAfee Labs

Рекомендовать отчет

Количество новых руткитов сократилось в третьем квартале на 65 %, что подчеркивает нестабильность вредоносных программ этого рода.



Источник: McAfee Labs

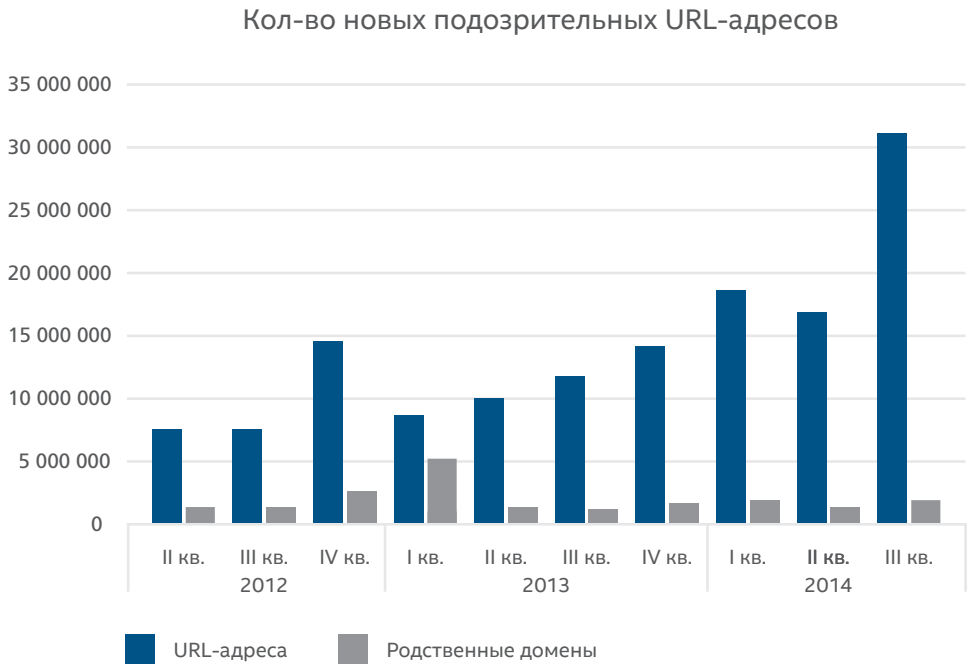


Источник: McAfee Labs

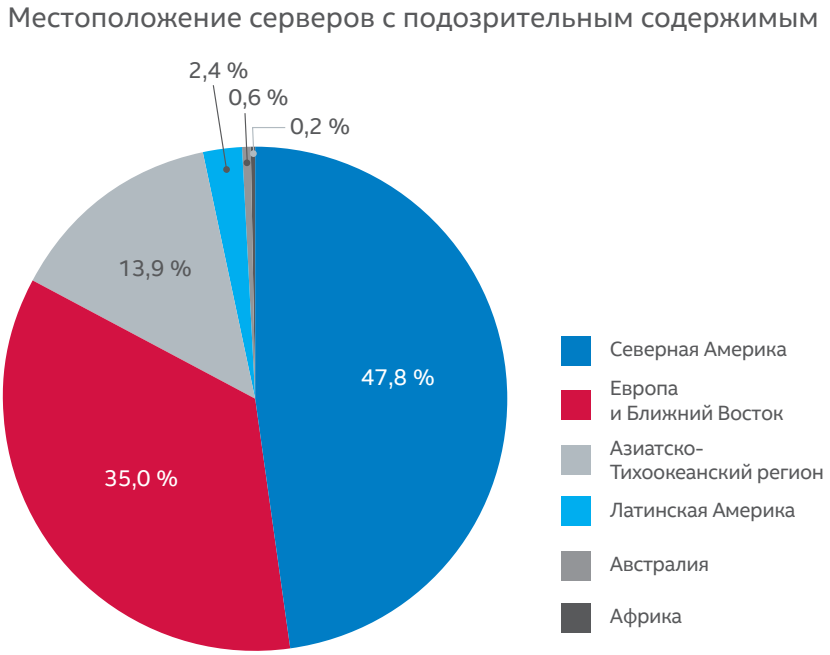
Рекомендовать отчет

Веб-угрозы

В этом квартале стремительно возросло количество новых подозрительных URL-адресов. Частично это связано с удвоением количества новых коротких URL-адресов, часто используемых для сокрытия вредоносных веб-сайтов, и с резким увеличением числа фишинговых URL-адресов.



Источник: McAfee Labs

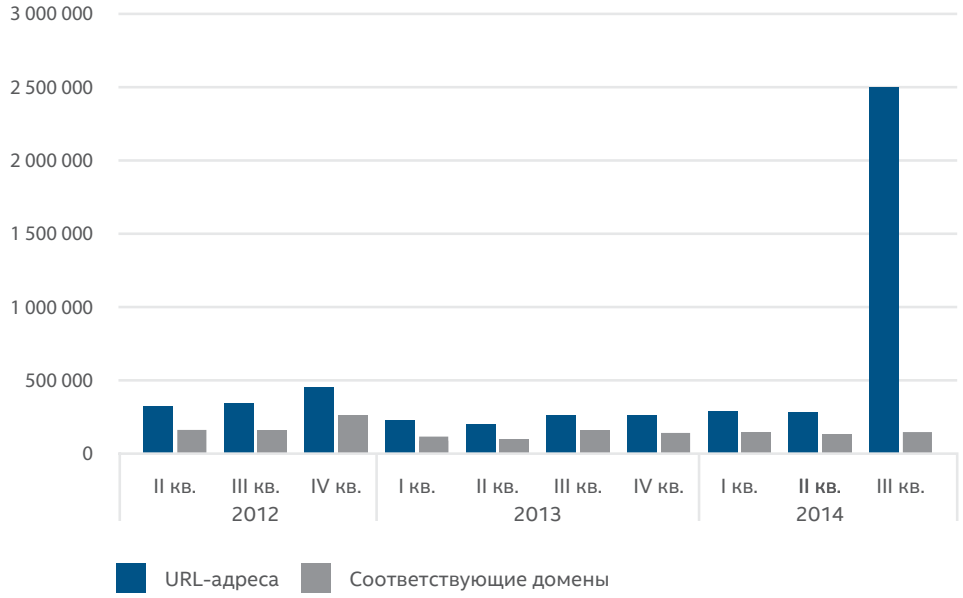


Источник: McAfee Labs

Рекомендовать отчет

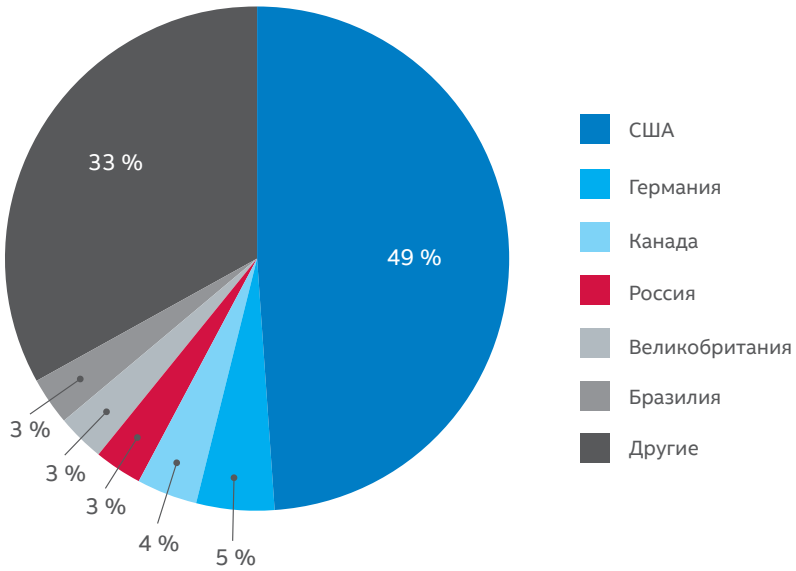
В основном мы относим значительный всплеск активности в этом квартале на счет происходящей из России кампании по рассылке нежелательной рекламы лекарственных препаратов, в ходе которой для каждого адресата создавался отдельный фишинговый поддомен. Наши системы сбора данных учитывали каждый из этих поддоменов.

Кол-во новых URL-адресов для фишинга



Источник: McAfee Labs

Основные страны,
в которых размещены домены для фишинга

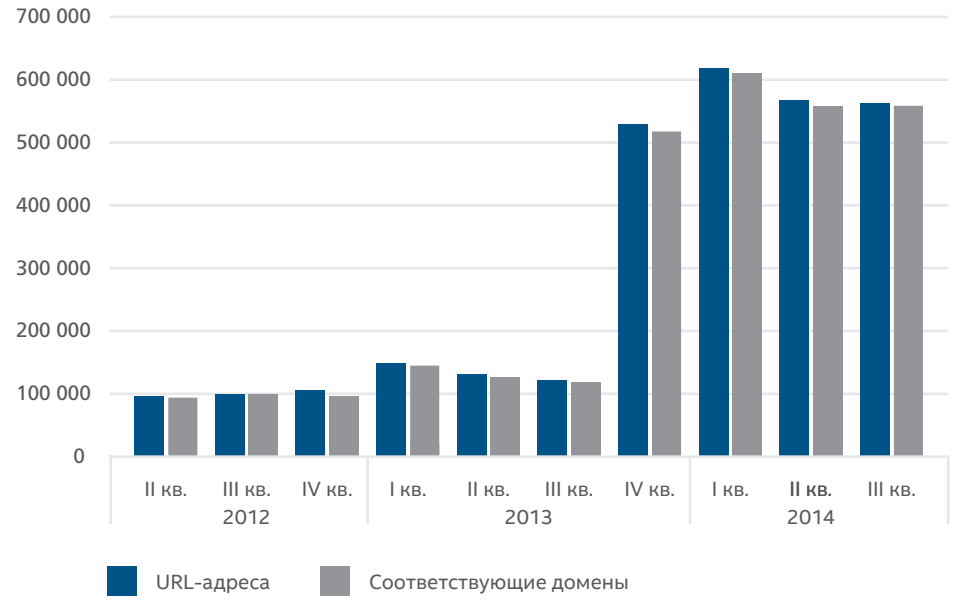


Источник: McAfee Labs

Рекомендовать отчет

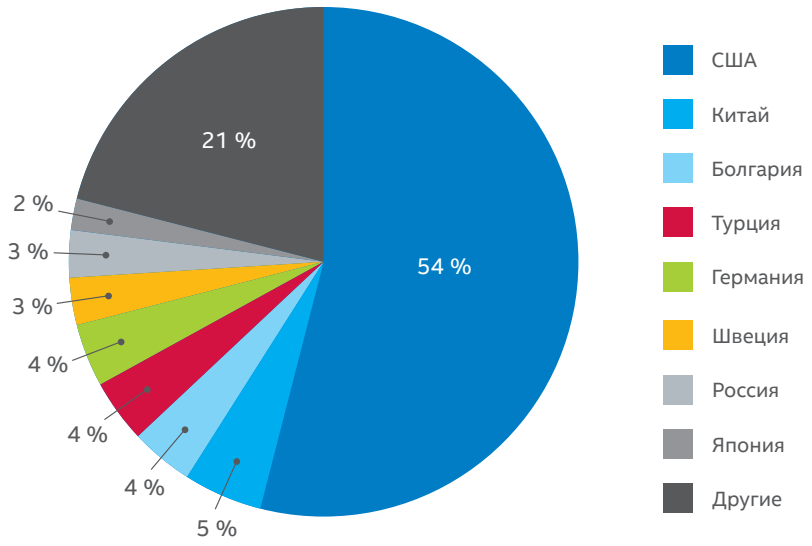
Начиная с этого квартала мы представляем информацию об общем количестве новых URL-адресов, используемых для рассылки спама, в мировом масштабе. Количество новых URL-адресов в третьем квартале немного сократилось по сравнению со вторым кварталом. Резкий скачок был отмечен в четвертом квартале прошлого года, когда мы усовершенствовали наш алгоритм сбора данных.

Кол-во новых URL-адресов для рассылки спама



Источник: McAfee Labs

Основные страны, в которых размещены домены для рассылки спама



Источник: McAfee Labs

Рекомендовать отчет

Опасные сообщения и сетевые угрозы

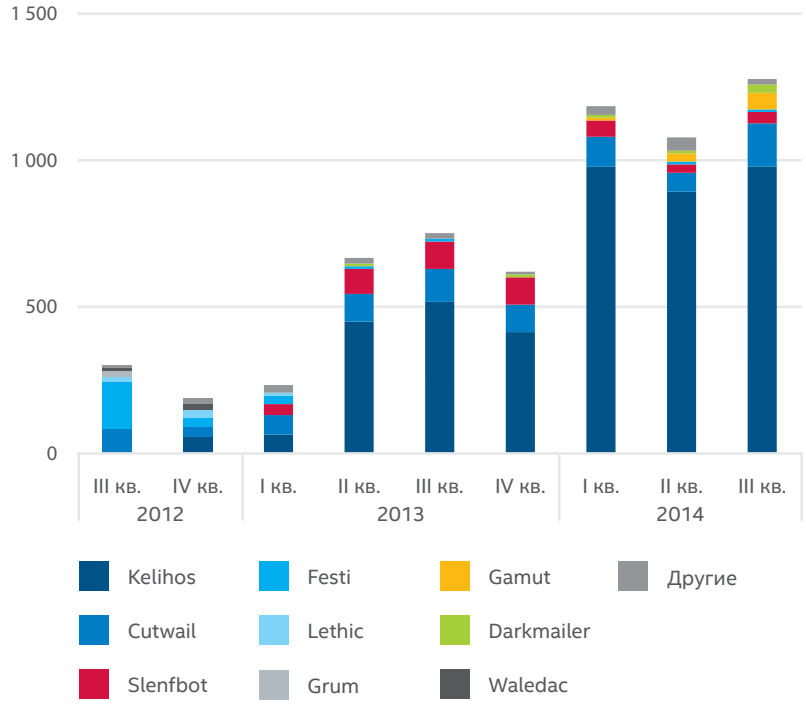
Зарегистрированное в этом квартале увеличение числа легитимных электронных сообщений на 148 % — это результат усовершенствования процесса сбора данных. Пока что этот показатель несопоставим с цифрами прошлых кварталов, но в будущем у нас будут более точные исторические данные об объемах почты. Объем спама за то же время увеличился на 40 %. Мы полагаем, что частично это является следствием изменения методов сбора данных, частично — следствием роста клиентской базы, активизации бот-сетей и увеличения количества «спама на снегоступах».

Источник: McAfee Labs

Рекомендовать отчет

Начиная с этого квартала мы представляем новую сводку о самых крупных бот-сетях, рассылающих спам. В этом году на первое место вышла бот-сеть Kelihos. В третьем квартале рассылки бот-сети Kelihos составили 76 % от общего объема спама, рассылаемого 20 крупнейшими бот-сетями. Совсем недавно бот-сеть Kelihos была замешана в рассылке нежелательных сообщений с советами по оптимизации бизнеса («8 простых правил, раскрывающих суть корпоративных продаж»), рекламой лекарственных препаратов («Дешевые лекарства. Скидка до 70 %») и предложениями быстро разбогатеть («376 $ за ОДИН ДЕНЬ? Разве это возможно? Мы докажем, что да!»). Kelihos — это обширная сеть, отправившая в этом году нежелательные сообщения с IP-адресов 226 стран.

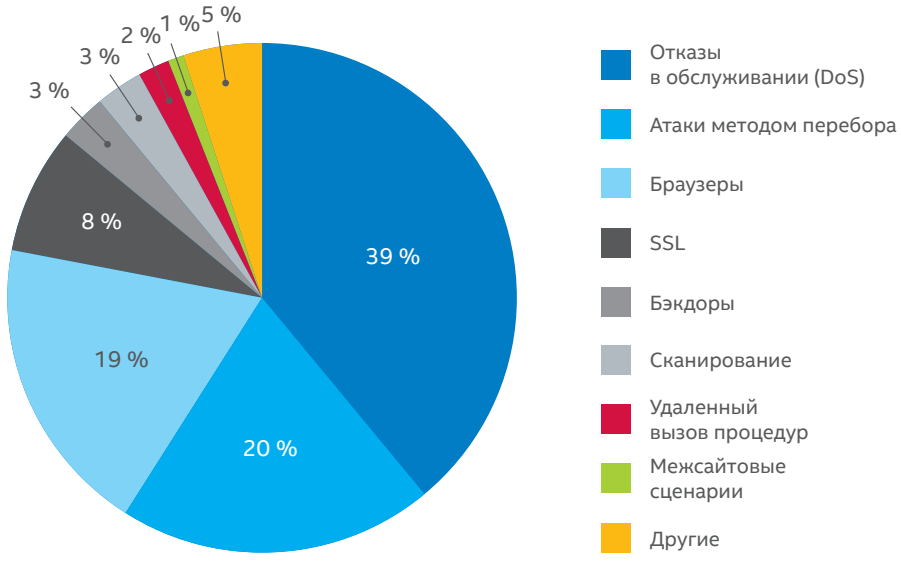
Нежелательная электронная почта от 20 крупнейших бот-сетей
(миллионы сообщений)



Источник: McAfee Labs

Три наиболее распространенных в этом квартале вида угроз составили 78 % от общего числа. Количество атак на SSL в третьем квартале увеличилось до 8 %, что на 5 % больше, чем во втором квартале. Этот рост, вероятно, связан с текущей эпидемией Heartbleed.

Лидеры среди сетевых угроз



Источник: McAfee Labs

Рекомендовать отчет

Отзывы. Ваши отзывы помогают нам определить направление дальнейшей работы. Если вы хотите поделиться с нами своими соображениями, щелкните **здесь** и потратьте несколько минут на заполнение анкеты.

Подпишитесь на McAfee Labs

О подразделении Intel Security

McAfee теперь входит в состав Intel Security. Следование стратегии Security Connected, инновационный подход к обеспечению программно-аппаратной защиты и наличие уникальной технологии Global Threat Intelligence дают подразделению Intel Security возможность направить все усилия на разработку проверенных решений и услуг по обеспечению упреждающей защиты систем, сетей и мобильных устройств, используемых в коммерческих и личных целях в разных странах мира. Сочетая опыт и знания McAfee с инновациями и проверенным качеством продуктов и услуг Intel, подразделение Intel Security работает над тем, чтобы средства защиты стали неотъемлемой составляющей любой архитектуры независимо от используемой вычислительной платформы. Основная задача Intel Security — дать всем, кто живет и работает в цифровом мире, уверенность в собственной безопасности и защищенности.

www.intelsecurity.com

McAfee. Part of Intel Security.
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
БЦ «Башни на набережной», Башня «А», 15 этаж
Телефон: +7 (495) 653-85-13
www.intelsecurity.com