Отчет

Прогноз угроз на 2012 год

McAfee® Labs™

Содержание

Для организации, занимающейся исследованием проблем информационной безопасности, прогнозирование будущих угроз может стать игрой в «угадайку». Что и говорить, увлекательно примерить на себя мантию волшебника и погадать о том, что может случиться или не случиться в ближайшие месяцы. Но куда сложнее ответить на вопрос о том, насколько значительно меняется характер угроз в каждом новом году? Во многих аспектах прошедший год был годом изменений. Какими же они были революционными или эволюционными? Мы стали свидетелями больших изменений, происходящих в типах угроз, направленных на мобильные устройства. Хактивизм, тенденции использования уязвимостей клиентских приложений и социальных медиа, а также целенаправленные атаки тоже претерпели серьезные изменения. Многие из этих изменений и тенденций в ближайшие годы будут продолжать оказывать влияние на картину угроз.

Какие изменения в картине угроз произойдут, по мнению McAfee Labs, в наступающем году? Мы ожидаем появления нескольких новых сценариев, а также некоторых значительных изменений даже в самых устоявшихся направлениях угроз:

- Угрозы, направленные на промышленные предприятия, станут более продуманными и направленными на конкретные секторы экономики.
- Атаки на встроенное аппаратное обеспечение расширятся и углубятся.
- Произойдет «перезагрузка» и эволюция хактивизма и деятельности группы Anonymous.
- Системы виртуальной валюты подвергнутся более масштабным и частым атакам.
- Этот год вряд ли станет годом кибервойны, скорее, годом *демонстрации готовности* к кибервойне.
- Спецификации DNSSEC откроют новые направления для сетевых атак.
- Традиционный спам «легализуется», а целевое фишинг-мошенничество преобразуется в направленные атаки путем рассылки сообщений.
- Произойдет усовершенствование и слияние мобильных бот-сетей и руткитов.
- Мошеннические сертификаты и мошеннические сертифицирующие органы будут подрывать доверие пользователей.
- Усовершенствования в операционных системах и системах безопасности повлекут за собой появление бот-сетей и руткитов следующего поколения.

Итак, главные направления угроз ясны. Пора переходить к подробностям!

Угрозы, направленные на промышленные предприятия

В последнее время угрозы, направленные на промышленные и национальные инфраструктуры, привлекают к себе немало внимания, и тому есть весьма веские основания. Это одна из немногих сфер, в которой киберугрозы представляют реальную опасность для имущества и жизни людей. Промышленные системы диспетчерского контроля и сбора данных (Supervisory Control And Data Acquisition, SCADA) так же уязвимы, как и любые другие системы, объединенные в сеть, с той, однако, разницей, что многие из этих систем не предназначены для работы в сетевой среде, на которую переходит весь мир. Теснейшая взаимосвязь между системами и устройствами, не предназначенными для такого вида доступа, — прямой путь к проблемам, вызванных отсутствием информационной защиты во многих средах, в которых развертываются системы SCADA. Распространенной практикой стало подключение критически важных инфраструктур к Интернету и последующее управление ими с помощью обычного, широко доступного программного обеспечения. Уязвимости присущи всем компьютерным программам, однако промышленные системы ИТ требуют особой комплексной проверки, касающейся архитектуры, проектного решения и способов его реализации. В 2012 году злоумышленники будут еще чаще и эффективнее использовать эту неподготовленность, и если бы только в целях шантажа или вымогательства. При рассмотрении целей многих хактивистских групп следует *со всей серьезностью* отнестись к возможному объединению политических целей с уязвимостями в системах промышленного контроля (Industrial Controller Systems, ICS).

Червь Stuxnet показал, как вредоносный код может породить реальную, «живую» угрозу.[1] Недавние инциденты, связанные с системами коммунального водоснабжения в США, показали, что такого рода объекты все чаще попадают в зону внимания злоумышленников. Создается впечатление, что чем больше внимания уделяется системам SCADA, тем больше выявляется брешей в их системах безопасности. Мы предполагаем, что такой недостаток защиты приведет к усложнению угроз, создаваемых с помощью комплектов инструментов и сред создания, тестирования и использования средств использования уязвимостей, а также к учащению атак на системы ICS в коммунальном хозяйстве и энергоснабжении. Как только в объекте, на который нацелена атака, обнаружится незащищенный центр, злоумышленники не преминут использовать его по максимуму.

Злоумышленники обычно охотятся за системами, которые можно успешно взломать, а как показала практика, именно системы ICS представляют собой среду, насыщенную целями. В свете последних событий администраторам систем ICS следует проявлять особую осторожность. Пора проводить обширные испытания на проникновение в систему и готовить планы аварийного реагирования, включающего киберкомпоненты и контакты с правоохранительными органами на всех уровнях. «Какие последствия будет иметь атака на нас?» — вот вопрос, который должны задать себе администраторы.

Угроза изнутри. Встроенное аппаратное обеспечение

За последние несколько лет возросли популярность и значение встроенных систем. В целом, эти системы предназначены для выполнения конкретной функции управления в рамках более крупной системы. Нередко эти системы предъявляют требованиями к вычислительным ресурсам в режиме реального времени. Зачастую они находятся в комплексном устройстве, включающем аппаратное обеспечение и другие механические компоненты. Подобная архитектура, традиционно используемая в таких отраслях промышленности, как авиационная радиоэлектроника, транспорт и энергетика, а также автомобилестроение и медицинское оборудование, теперь все шире используется в продуктах, предназначенных для делового, производственного и бытового применения. Встроенные функции и системы используются в системах навигации GPS, маршрутизаторах и сетевых мостах, а в последние годы и во многих электронных устройствах бытового назначения.

Использование уязвимостей встроенных систем потребует применения вредоносных программ, выполняющих атаки на уровне аппаратного обеспечения. Высокая квалификация злоумышленников вовсе не ограничивается знанием встроенных платформ.

Сегодня авторы вредоносных программ все чаще пишут программы, нацеленные на более низкие уровни операционной системы. Нередко злоумышленники попытаются взломать или «рутировать» систему на низшем уровне, включая основную загрузочную запись и даже уровни системы BIOS. При удачном внедрении кода, который изменит порядок запуска или порядок загрузки операционной системы, преступники получат больший контроль и смогут получить доступ к системе и ее данным в течение длительного периода времени. Для высококвалифицированных хакеров сфера управления оборудованием — «земля обетованная», в которую они стремятся попасть.

Данная тенденция приводит к тому, что уязвимыми к подобным атакам становятся и другие системы, использующие встроенное оборудование. Мы сталкиваемся с концептуальным кодом, нацеленным на встроенное оборудование в автомобильных, медицинских и коммунальных системах. По нашим прогнозам, такие доказательства уязвимости в виде кода, демонстрирующего возможность использования уязвимости (proof-of-concept code), станут более эффективными, начиная с 2012 года.

Хактивизм

Хотя хактивизм сам по себе и не нов, однако благодаря саге про WikiLeaks, появившейся на первых полосах мировых СМИ в 2010 году, хактивизм приобрел более широкую известность и стал использоваться чаще, чем когда-либо раньше. В целом, ситуация для интернет-активистов в 2011 году была сложной и запутанной. Зачастую враждующие группировки не ладили друг с другом и не имели четко заявленных целей. Порой сложно было отделить кампании, имеющие политическую подоплеку, от простых забав взломщиков-дилетантов, однако ясно одно: если хактивисты выбирали объект атаки, целостность этого объекта была нарушена либо посредством взломов, приводивших к утечке данных, либо с помощью атак типа «отказ в обслуживании». Хактивисты — реальная сила. Можно соглашаться или не соглашаться с их целями, однако Anonymous и другие хактивистские группы продемонстрировали упорство, изобретательность и даже маневренность при выборе некоторых объектов и операций.

Наступающий год станет решающим для хактивизма. Истории про группу Anonymous — всего лишь один аспект проблемы.

- «Подлинная» группа Anonymous (ее традиционное крыло) либо возродится и возродит свой статус, либо прекратит свое существование. Если группы, находящиеся под влиянием Anonymous, не смогут организоваться и выработать четкие призывы к действию и заявить о своей ответственности, все группировки, именующие себя Anonymous, в конце концов рискуют оказаться вытолкнутыми на обочину политической жизни. В любом случае, определенно будет наблюдаться значительный рост атак такого рода. Продолжится рост числа распределенных атак по типу отказа в обслуживании (DDoS) и случаев раскрытия личных данных, оправдываемых политическими принципами.
- Организаторы кибератак еще теснее объединятся с организаторами реальных демонстраций. Мы увидим более тесное сращение хактивизма, основанного на социальных медиа, с хактивизмом, координируемым самими социальными медиа. По нашим прогнозам, многие будущие операции будут включать в себя как физические, так и компьютерные компоненты. Будет осуществляться одновременное планирование совместных и координированных действий в реальном и виртуальном мирах. Несложно догадаться, что эволюция группы Occupy и других групп протеста повлечет за собой прямые кибердействия. Как отмечалось в других наших прогнозах, существует весьма реальная возможность использования уязвимостей в системах промышленного контроля или системах SCADA в хактивистских целях. Мы полагаем, что радикальные хактивисты, поддерживающие глобальное движение Occupy, откажутся от названия Anonymous и вскоре начнут действовать под названием Cyberoccupiers («Киберзахватчики»).
- Как по политическим, так и по идеологическим причинам, подробности частной жизни публичных фигур (политиков, руководителей промышленных предприятий, судей, высокопоставленных лиц в правоохранительной сфере и сфере безопасности) в наступающем году будут предаваться огласке еще чаще, чем в предыдущем. Активисты движения протеста не остановятся ни перед чем, чтобы собрать данные из социальных сетей или с веб-серверов в поддержку проводимых ими различных операций.

- Некоторые хактивисты будут действовать в том же направлении, что и «кибермии» разного толка, процветающие главным образом в недемократических или несветских государствах («кибермия» Ирана, «кибермия» Пакистана, китайская группа ChinaHonker и т. д.) Эти «армии», которые в последние два года в основном использовались для дискредитации оппонентов, в новом году перейдут к более разрушительным действиям. Между некоторыми из этих групп произойдут столкновения, которые, возможно, станут причиной непредсказуемого косвенного ущерба (например, столкновения между Палестиной и Израилем, Индией и Пакистаном, Северной и Южной Кореей и т. д.). По слухам, в 2011 году «кибермии» управлялись или поддерживались правительствами своих стран. В следующем году тоталитарные государства пойдут еще дальше и даже признают действия своих «кибермий».

Рис. 1. Множество связей и мотивов хактивизма.

Виртуальная валюта

Виртуальная валюта, иногда называемая «кибервалюта», стала популярным способом денежного обмена в Интернете. Необязательно поддерживаемые материальными активами или даже реальными товарами, такие сервисы как Bitcoin позволяют осуществлять операции посредством децентрализованной одноранговой (пиринговой) сети — в основном, с помощью электронных денег («биткойнов»), — что позволяет выполнять прямые электронные платежи. Все, что нужно пользователю для получения «монет», — это клиентское программное обеспечение и интернет-«кошелек». «Монеты» хранятся в «кошельке» и могут переводиться другим пользователям в качестве оплаты за товары или услуги. Чтобы послать или получить «монеты», пользователю нужен только адрес «кошелька». Вы увидели здесь и проблему, и возможность воспользоваться этой проблемой, не так ли?

Троянские программы могут легко воспользоваться уязвимостями этой архитектуры. В «кошельках» не используется шифрование, транзакции происходят открыто. Это весьма привлекательная цель для киберпреступников. В 2011 году в отношении систем виртуальной валюты произошло несколько событий, которые достойны упоминания:

- Взлом базы данных обменника электронной валюты Mt. Gox, кража злоумышленниками тысяч биткойнов
- Распространение спама, рекламирующего фальшивые инструменты добычи биткойнов (так называемого «майнинга»). Эти инструменты фактически содержали вредоносные программы, предназначенные для отправки файлов «кошелька» жертвы на удаленный узел. Кроме того, они позволяли другим «добытчикам» использовать зараженный компьютер для дальнейшей добычи биткойнов.
- Обнаружение бот-сетей для добычи биткойнов. Используя большое количество зараженных компьютеров, эти бот-сети могли ускорять процесс добычи и обработки биткойнов, а также запускать распределенные атаки по типу отказа в обслуживании (DDoS).

По своему характеру виртуальные валюты и технологии, подобные Bitcoin, представляют собой настолько лакомый кусок, что киберпреступники просто не могли им не воспользоваться. В 2011 году мы наблюдали значительный рост вредоносных программ, нацеленных на подобные технологии. О вредоносных программах, предназначенных для Bitcoin, можно, в частности, сказать следующее:

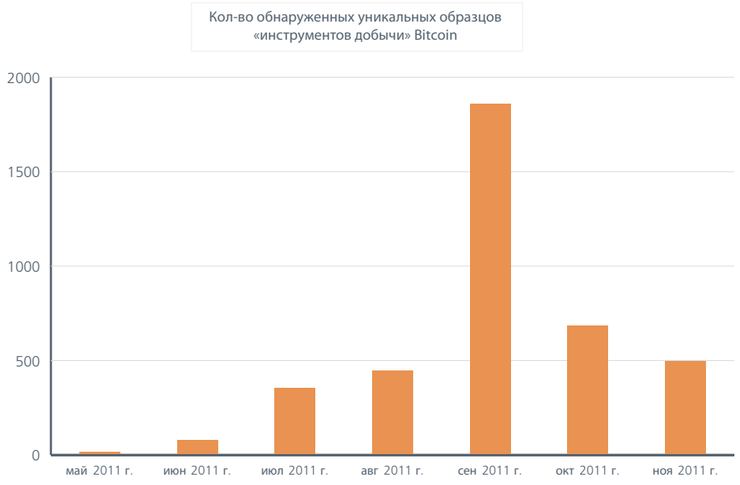

Рис. 2. Число хищений (называемых разработкой) виртуальной валюты Bitcoin в сентябре достигло пика. Мы прогнозируем увеличение числа хищений в 2012 году.

По нашим прогнозам, в следующем году эта угроза разовьется в «кустарный промысел» киберпреступности — со спамом, кражей данных, инструментами, вспомогательными сетями и другими сервисами, предназначенными исключительно для использования уязвимостей систем виртуальных валют. Несомненно, что киберпреступники нашли платежную систему, которая полностью соответствует их потребностям.

Кибервойна

Разразится ли в наступающем году кибервойна, или же этот год станет просто годом бряцания кибероружием и парадом его возможностей? И хотя мы надеемся, что дело ограничится последним вариантом, развитие ситуации в прошедшие годы заставляет полагать, что кибервойна в конце концов неизбежна. Мы нередко становимся свидетелями использования «кибернетических» технологий как дополнения к традиционным методам ведения разведывательных и шпионских операций. Многие участники операций охотно обвиняют в применении таких технологий других, — как союзников, так и врагов. Кибертехнологии — исключительно дешевый способ шпионажа, который всегда оставляет место для правдоподобного отрицания, не ставит под угрозу жизнь людей, а главное — весьма эффективен. Дело пока не дошло до широкомасштабного применения кибертехнологий в качестве оружия в военных конфликтах. До сих пор технологии применялись в ограниченном масштабе, а атаки не отличались высоким уровнем сложности. В качестве примера можно назвать грузинский конфликт.

Теперь же ситуация изменилась. Многие страны осознают разрушающий потенциал кибератак, направленных на критически важную инфраструктуру, и сложность обеспечения защиты от них. Потенциал таких угроз открывает возможности проведения атак со стороны малых стран и организаций, в особенности, если количество целей, способных нанести ответный удар, незначительно. Атака червя Stuxnet во многом изменила правила игры. Одним из уроков, извлеченных из этой атаки, стало ясное осознание реальности угрозы и тех последствий, которые подобные атаки могут иметь.

Соединенные Штаты Америки понимают, насколько они уязвимы — возможно, более уязвимы, чем любая иная страна. Причина кроется в огромной зависимости от компьютерных систем и киберзащиты, которая, в сущности, обеспечивает безопасность только государственных и военных сетей. Представьте себе армию, которая защищает свои военные базы, оголяя другие участки страны. После широкой критики по поводу отсутствия официальной доктрины наконец-то последовала реакция со стороны американского государства.

В июле был выпущен документ Department of Defense Strategy for Operating in Cyberspace (Стратегия Министерства обороны по операциям в киберпространстве).[2] В отчете говорится: «Стратегическая инициатива номер 1. Министерство обороны будет рассматривать киберпространство в качестве сферы военных действий для организации защиты, подготовки специалистов и обеспечения мероприятий, направленных на полное использование Министерством обороны потенциала киберпространства». (Прим. переводчика: свободный перевод) Однако в этом документе вы не найдете обсуждаемого нами ранее вопроса, а именно: возможности нанесения противником удара в ответ на масштабную кибератаку. Вместо этого, в дополнение к стратегии ведения кибервойны, Министерство обороны готовит новую доктрину, представляющую собой конкретное руководство для штабов боевых кибердействий. Если в этой доктрине будет изложено, при каких обстоятельствах может быть нанесен ответный киберудар, она все равно будет далека от доктрины «угрозы всеобщего уничтожения», которая помогла миру уцелеть в период холодной войны.

Тот факт, что возможные ответные действия неизвестны из-за того, что они засекречены, вряд ли способен удержать злоумышленников от совершения атаки.

Согласно некоторым данным, применение кибероружия рассматривалось в ходе революционных действий в Ливии. Этого, впрочем, не произошло, поскольку не нашлось охотников первыми открывать ящик Пандоры. Другим возможным объяснением может служить тот факт, что Ливия не является насыщенной целями средой. В любом случае, пока еще мы не стали свидетелями публичной демонстрации возможностей наступательных военных кибердействий, способных удержать кого-либо от нападения. Все громче раздаются голоса, требующие рассекретить эту информацию, поэтому можно ожидать некой демонстрации, но уже иного рода, чем демонстрация дипломатам иностранных держав видеоклипов с пугающими кадрами отказа оборудования. Эффективная демонстрация может вызвать ответную реакцию других государств, которые захотят показать, что и они обладают такими же возможностями.

В наступающем году мы надеемся увидеть только демонстрацию готовности к кибервойне, но не настоящую войну!

DNSSEC

DNSSEC (Domain Name System Security Extensions, расширения безопасности системы доменных имен) или набор спецификаций IETF, обеспечивающих безопасность информации, предоставляемой средствами DNS в IP-сетях — это технология защиты услуг преобразования имен сетевых узлов в IP-адреса от поддельных сообщений и подделок записей кэша с помощью «сети доверия» на базе шифрования с открытым ключом. Технология предназначена для обеспечения защиты компьютера клиента от самопроизвольной коммуникации с узлом в результате атаки типа «человек посередине» (man-in-the-middle attack), которая перенаправляет трафик от целевого сервера (веб-страницы, электронной почты и т. д.) на другой сервер. Это чрезвычайно важный шаг в эволюции Интернета, направленный на защиту интернет-пользователей и затрудняющий работу злоумышленников.

Конечно, технология DNSSEC также защищает от любых попыток подделки сообщений и перенаправлений со стороны государственных органов, которые перенаправляют интернет-трафик, поступающий на веб-сайты, занимающиеся продажей нелегального программного обеспечения или образов. Для того чтобы государственные органы могли перенаправлять трафик, они должны считаться заслуживающими доверия на уровне корневых доменов. Такой уровень доверия неохотно предоставляется другими государственными органами в случае, если им будет известно, что результатом предоставления уровня доверия будет запрещение интернет-содержимого на основании мнения иностранных государств.

Недавние попытки принять законы, запрещающие выплаты, связанные с правами на интеллектуальную собственность, основаны на понимании текущего состояния современной системы доменных имен (DNS), а не на прогнозах о том, как будет работать завтрашняя технология DNSSEC. В результате этого разрыва могут появиться дополнительные законодательные требования, предъявляемые к управлению сегодняшней инфраструктурой DNS, которая может оказаться несовместима с инфраструктурой DNSSEC. В случае внедрения таких требований, процесс усовершенствования защиты нашей инфраструктуры DNS может быть отложен на тот период, в течение которого всевозможные рабочие группы будут искать технический компромисс между законодательством и DNSSEC.

Поскольку правительственные органы всего мира проявляют все большую заинтересованность в принятии «правил дорожного движения» для интернет-трафика, можно ожидать, что законодательные споры по проблемам вчерашнего дня все чаще будут тормозить процесс принятия решений для дня завтрашнего. В результате Интернет будущего, вероятно, будет оставаться Интернетом прошлого несколько дольше, чем хотелось бы нам, специалистам по информационной безопасности.

«Легализация» спама

За последние четыре года мы наблюдали рост взаимопонимания и укрепления сотрудничества между странами в области борьбы с нежелательными сообщениями (спамом), рассылаемыми бот-сетями. Результатом этого сотрудничества стал ряд громких эпизодов, связанных закрытием инфраструктур, которые играли критически важную роль в управлении бот-сетями (например, бот-сети ISP McColo), веб-хостинге для рассылки спама («Главмед») и обработке кредитных карт, связанных с продажей поддельной фармацевтической продукции. Против крупных интернет-корпораций, которые предоставляли возможности для рекламы нелегальным компаниям, были даже возбуждены судебные иски. Благодаря совместным действием значительно снизились объемы мирового спама по сравнению с пиковыми показателями середины 2009 года. Одновременно на черном рынке существенно подорожали услуги рассылки спама через бот-сети.

И хотя эти шаги ни в коей мере не означают полного прекращения рассылки нежелательных сообщений, как предсказывали некоторые пророки от технологий, они действительно меняют картину сегодняшнего дня. Сегодня мы видим, что все больше нежелательных сообщений рассылается не с хостов, зараженных бот-сетями, а из реальных, «легальных» рекламных агентств, использующих методы, которые жестко критикуют противники спама. Эти методы заключаются во внесении в списки рекламных рассылок электронных адресов пользователей без ведома или согласия последних. В арсенале рекламных агентств имеется множество приемов, начиная с открытой покупки списков электронных адресов, которые представляются как списки пользователей, уже согласившихся получать какую-либо рекламу (заявление, которое требует готовности верить в предлагаемое объяснение) до приема, известного как e-pending (сбор электронных адресов с помощью алгоритмов, определяющих, что их владельцы согласились бы получать рекламу, если бы получили такое предложение, но затем, не спрашивая разрешения, алгоритмы без разрешения добавляют адреса в список для рассылок). Еще один метод — покупка баз данных клиентов у закрывающихся компаний и игнорирование политики защиты конфиденциальности, которая действовала во время работы старой компании. Используется также метод «партнерства» с другими рекламными агентствами или поставщиками списков электронных адресов с целью бомбардировки пользователей, внесенных в эти списки, рекламными объявлениями.

Рекламные компании, использующие подобную практику работы, отдают себе отчет в том, что занимаются рассылкой спама, поэтому, пытаясь избежать обнаружения, берут на вооружение те же приемы, что и операторы бот-сетей. Ежедневно регистрируются тысячи новых доменов электронной почты, используя возможности конфиденциальности, которые обеспечивает сервис Whois, не позволяющий установить личность владельца. В подсетях поставщиков хостинга активируются тысячи новых IP-адресов, которые действуют в течение нескольких часов в качестве «пушки» для рассылки спама, забивающей ящики входящих сообщений плохо форматированными письмами, изобилующими орфографическими и грамматическими ошибками. Большинство из этих писем содержат ссылку, нажав на которую вы сможете отказаться от получения рассылки. Однако все, чего вы добьетесь этим действием — это уведомите спамеров о том, что ваш адрес электронной почты активен, и что вы прочли это письмо. В письме имеется и адрес, на который можно послать письмо обычной почтой и попросить, что вас вычеркнули из списка рассылки. Стоит проверить адрес через Интернет, вы обнаружите что он находиться в гуще канадских лесов или на каменистых участках пустыни в штате Аризона. Бывали случаи, когда на отдельные электронные адреса за один день приходило более 9 000 почти идентичных нежелательных сообщений с рекламой целебных свойств популярного магнитного браслета.

К сожалению, такие нечистоплотные рекламные методы поддерживаются законом. Закон о борьбе со спамом США (CAN-SPAM Act) выхолощен настолько, что не требует от рекламодателей наличия согласия владельцев адресов на получение рекламы. Тот факт, что реклама является прибыльным, плотно и умело лоббируемым бизнесом, не позволяет предположить, что в ближайшее время произойдут какие-либо существенные изменения в методах управления списками электронных адресов или будут наложены крупные штрафы за нечистоплотное поведение.

В таких условиях можно ожидать, что объем «легального» спама будет расти с угрожающей скоростью. Рассылать пользователям спам из рекламных компаний и дешевле, и безопаснее, чем использовать зараженные бот-сетями хосты. Такой вид деятельности, известный как snowshoe spamming («спам на снегоступах», «спам, почти не оставляющий следов») и представляющий собой рассылку спама с многочисленных IP-адресов, приобрел такие масштабы, что среди 10 поступивших во время написания этой статьи сообщений непременно будет одно уведомление о доставке письма, одно нежелательное сообщение с рекламой фальшивых часов Rolex (отправленное через бот-сеть), одно «нигерийское» письмо и семь писем, связанных со «спамом на снегоступах». Трафик такого рода будет продолжать расти намного быстрее, чем фишинговые сообщения и «нигерийские» письма, в то время как объем спама, отправленного через бот-сети, будет по-прежнему снижаться, так как ботмастера найдут гораздо более эффективные и безопасные способы выкачивания денег из армий зараженных компьютеров. Недалек тот час, когда бóльшая часть мирового спама будет рассылаться нечистоплотными, но «легальными» компаниями. И это лишь вопрос времени.

Угрозы безопасности мобильных устройств

В течение последних двух лет мы наблюдаем увеличение числа атак на смартфоны и другие мобильные устройства. Нам встречались руткиты, бот-сети и другие вредоносные программы. От простых деструктивных программ злоумышленники перешли к созданию шпионских программ и программ, приносящих доход. Они используют уязвимости для обхода защиты системы и получения большего контроля над устройствами. В 2012 году мы прогнозируем продолжение этой тенденции и повышение сложности атак. Мы также прогнозируем увеличение доли атак на мобильные банковские системы.

Бот-сети +руткиты = проблемы нижнего уровня ОС

На настольных компьютерах руткиты и бот-сети занимаются показом рекламы и зарабатывают на пользователях зараженных машин. На мобильных устройствах эти типы вредоносных программ используются таким же способом. Руткиты позволяют установить другие программы, в том числе шпионские, а бот-сети способны генерировать автоматические переходы по рекламе и отправлять платные текстовые сообщения.

Мы зафиксировали мобильные варианты семейств вредоносных программ, например Android/DrdDream, Android/DrdDreamLite, Android/Geinimi, а также Android/Toplank и Android/DroidKungFu. Некоторые из этих вредоносных программ для получения доступа к телефону жертвы с правами root и контроля над ним используют уязвимости, изначально появившиеся при попытке помочь пользователям разблокировать собственные устройства. В следующем году разработчики и исследователи будут разрабатывать новые методы получения прав root на телефонах, а злоумышленники учтут опыт создания вредоносных программ для ПК, в большей степени основывая свои атаки на аппаратном обеспечении устройств. Вредоносные программы для ПК получают доступ все более низкого уровня, используя особенности оборудования; мы прогнозируем, что вредоносные программы для мобильных устройств будут развиваться в том же направлении.

Буткиты, то есть вредоносные программы, которые способны обойти или заменить процедуры, выполняемые при загрузке, также представляют угрозу для мобильных устройств. Получение прав root на своем телефоне или на электронной книге дает пользователю доступ к дополнительным функциям и возможность заменить ОС, но также позволяет злоумышленникам установить собственную модифицированную ОС. Если мобильный руткит просто изменит существующую ОС, чтобы избежать обнаружения, то буткит дает атакующему гораздо большую степень контроля над устройством.

Например, Weapon of Mass Destruction («Оружие массового поражения») — набор средств для испытания на проникновения — работает на телефонах со старыми версиями Windows Mobile. Для своей установки WMD использует средства, разработанные для загрузки Linux на телефонах с Windows Mobile и позволяющие вернуться к исходной ОС. Злоумышленники уже используют старые уязвимости, дающие права root и возможность скрыть атаку. В конце концов, развитие средств использования уязвимостей позволит атакующим установить на устройство собственную микропрограмму.

Атаки на мобильные банковские системы

Злоумышленники используют вредоносные программы для ПК, такие как Zeus и SpyEye, для хищения средств со счетов в интернет-банках. И Zeus, и SpyEye стали использовать мобильные вспомогательные программы для обхода двухуровневой проверки подлинности и получения доступа к счетам жертв.

Zitmo (Zeus-in-the-mobile) и Spitmo (SpyEye-in-the-mobile) — два семейства мобильных вредоносных программ, пересылающих текстовые сообщения атакующим. С помощью таких программ злоумышленники вручную входят в интернет-банк для похищения денег пользователей.

В июле прошлого года исследователь в области информационной безопасности Райан Шерстобитофф (Ryan Sherstobitoff) описал способ отслеживания транзакций, выполненных с помощью Zeus и SpyEye, так как они значительно отличались от действий, выполняемых настоящими пользователями. В прошлом месяце он продемонстрировал, как злоумышленники изменили свой подход, разработав способ хищения средств во время нахождения жертвы на сайте. Таким образом, мошеннические транзакции выглядят так, как будто они выполнены авторизованными пользователями, а добавление задержек создает впечатление, что эти действия выполняет не программа, а человек. Злоумышленники быстро адаптируются ко всем новшествам, призванным защитить использование банковских счетов с компьютера. По мере того как мобильные устройства все чаще используются для выполнения банковских операций, злоумышленники переключаются с ПК на приложения для мобильных банковских систем. Мы прогнозируем повышение частоты атак такого рода по мере увеличения числа пользователей, управляющих своими финансами с мобильных устройств.

Фальшивые сертификаты

Мы склонны доверять файлам и документам, имеющим цифровую подпись, так как мы доверяем цифровым подписям и организациям, выдающим их. Многие системы белых списков и контроля за приложениями основываются на подлинности цифровых подписей. Эти решения позволяют создавать политики и средства управления службами, приложениями и даже отдельными файлами, имеющими подлинную цифровую подпись. В основе защищенного просмотра сайтов и безопасных интернет-транзакций также лежат доверенные цифровые подписи. Удостоверяющие центры и их сертификаты фактически говорят операционной системе: «Мне можно доверять, я подлинный, за меня ручаются».

Что происходит при появлении подложных или фальшивых сертификатов на фоне такого уровня доверия? В частности, каковы последствия успешной атаки на удостоверяющий центр? Цифровые сертификаты дают нам некоторый уровень уверенности в файле, процессе или транзакции. Выдавая и используя фальшивые или скомпрометированные сертификаты, злоумышленники смогут совершать атаки, которые практически невозможно обнаружить. Для веб-обозревателей это означает возможность атаки типа «человек посередине»: данные, которые должны быть зашифрованы и не видны атакующему, будут читаться как обычный текст, потому что у злоумышленника есть к ним ключ. Для систем безопасности файлы, подписанные правильным ключом, будут незаметны, так как они попадут в белый список: благодаря сертификату, такому файлу разрешен доступ к системе.

Использование фальшивых сертификатов в значительной степени помогало новейшим угрозам, таким как Stuxnet и Duqu, успешно избегать обнаружения. Хотя это не первый случай обнаружения такого поведения (фальшивые антивирусы, некоторые варианты Zeus, Conficker и некоторые старые вредоносные программы для Symbian использовали их), мы прогнозируем распространение этой тенденции на будущий 2012 год и последующие годы.

Наиболее серьезная угроза для удостоверяющего центра — риск выдачи фальшивых сертификатов — останется проблемой завтрашнего дня, так как этот тип атаки позволит злоумышленникам создать множество ключей для атак на веб-обозреватели и системы защиты, фактически подрывая доверие к ним, заложенное в операционную систему. Мы очень обеспокоены возможными последствиями крупномасштабного использования фальшивых сертификатов в системах белых списков и контроля за приложениями. Голландский удостоверяющий центр DigiNotar, ранее уже испытывавший проблемы с обеспечением своей безопасности, недавно объявил себя банкротом после выявленного нарушения системы безопасности, в результате которого были выписаны поддельные сертификаты. Была ли эта атака последним гвоздем в крышке его гроба? Расследование выявило, что 531 поддельный сертификат был выпущен DigiNotar. Вероятно, крах этой компании только приоткрывает завесу над нарушениями безопасности в этой области. Теперь нам следует задать себе вопрос о том, кому мы доверяем и какой ущерб был нанесен.

Широкомасштабные атаки на удостоверяющие центры и распространение поддельных, но действительных сертификатов имеет крайне серьезные последствия для инфраструктуры открытых ключей, безопасного просмотра веб-страниц, интернет-транзакций, а также белых списков и систем контроля за приложениями. Злоумышленники получают значительное преимущество, пользуясь нашим доверием к этим системам. Мы прогнозируем уверенный рост активности в этой области.

Развитие операционных систем

Информационная безопасность — это всегда обмен ударами, при котором масштабы действий и противодействий равны. Злоумышленники пишут вредоносный код — мы нейтрализуем его. Производители операционных систем внедряют защитные системы в ядро ОС — злоумышленники находят способы их обойти. Это естественный фактор динамического развития картины угроз, который никогда не исчезнет. Но приведет ли развитие технологий информационной безопасности и операционных систем к тому, что авторы вредоносных программ будут вынуждены атаковать оборудование напрямую, минуя ОС?

В последних версиях Windows реализованы защита от исполнения кода в области данных и случайное распределение адресного пространства. Эти методы защиты затрудняют получение несанкционированного доступа к компьютеру. Технологии шифрования также повысили уровень защищенности ОС в последние годы. Однако злоумышленники быстро нашли способы обойти их, точь-в-точь как ранее им удавалось обойти большинство мер безопасности, встроенных в ОС. Компания Microsoft анонсировала выпуск операционной системы Windows 8, которая будет включать многие защитные функции: защищенное хранилище паролей, возможность безопасной загрузки ОС, защита от вредоносных программ и даже возможности управления репутацией. Куда приведет злоумышленников необходимость противодействия этой архитектуре безопасности?

Отвечаем: приведет «вниз и в обход», на более низкие уровни доступа к оборудованию, в обход операционной системы.

В течение нескольких последних лет McAfee Labs отмечает значительное развитие технологии руткитов и буткитов. Руткиты предназначены для установления контроля за операционной системой и защитными программами, а буткиты противодействуют системе шифрования и могут подменить исходные загрузчики ОС. Это современные способы перехвата ключей шифрования и паролей, которые даже способны обойти требование использовать только подписанные драйверы, накладываемое в некоторых ОС.

Атаковать оборудование и микропрограммы непросто, но в случае успеха злоумышленники смогут хранить постоянный «образ» вредоносного ПО в сетевых картах, на жестких дисках и даже в BIOS. Мы прогнозируем, что в 2012 году и в последующие годы злоумышленники уделят более пристальное внимание уязвимостям в оборудовании и микропрограммах и основанным на них атакам.

Исследователи уже продемонстрировали возможность обхода новой защиты загрузчика Windows 8 при использовании прежних версий BIOS; заметьте кстати: коммерческая версия Windows 8 еще не выпущена. Мы прогнозируем, что с дальнейшим развитием технологии Intel EFI (объединенной расширяемой микропрограммы) — программного интерфейса между микропрограммой оборудования и операционной системой, предназначенного для замены устаревших BIOS и позволяющего выполнять безопасную загрузку, — злоумышленники в ближайшие годы будут прилагать большие усилия к разработке способов обхода этой защиты.

Мы будем внимательно следить за тем, как злоумышленники используют данные низкоуровневые функции для управления бот-сетями. Возможно, управляющие модули будут перемещены в память видеоадаптеров, в BIOS или в главную загрузочную запись. В то же время мы прогнозируем, что злоумышленники будут использовать в своих целях более современные протоколы, например IPv6, по мере того как их поддержка добавляется в новые операционные системы.

Несмотря на наши попытки противодействовать стремлениям злоумышленников, они явно видят преимущества переключения с традиционных атак ОС на атаки оборудования.

Об авторах отчета

В подготовке и написании данного отчета принимали участие сотрудники McAfee Labs Чжэн Бу (Zheng Bu), Гийерм Венер (Guilherme Venere), Адам Восотовски (Adam Wosotowsky), Торальв Дирро (Toralv Dirro), Паула Греве (Paula Greve), Дэвид Маркус (David Marcus), Франсуа Паже (François Paget), Райан Пермех (Ryan Permeh), Питер Сзор (Peter Szor), Крейг Шмугар (Craig Schmugar) и Джимми Ша (Jimmy Shah).

О лаборатории McAfee Labs

McAfee Labs — это глобальная исследовательская группа McAfee. Являясь единственной организацией, занимающейся всеми направлениями угроз, включая вредоносные программы, веб-угрозы, угрозы электронной почте, сетевые угрозы и уязвимости, McAfee Labs собирает информацию посредством миллионов датчиков и «облачной» технологии McAfee Global Threat Intelligence™. Группа McAfee Labs, насчитывающая 350 исследователей различных профилей из 30 стран, отслеживает весь спектр угроз в реальном времени, выявляя уязвимости приложений, выполняя анализ и корреляцию рисков, что позволяет выполнять мгновенные исправления с целью защиты корпоративных и частных пользователей.

О компании McAfee

McAfee — стопроцентная дочерняя компания Intel Corporation (NASDAQ: INTC), является крупнейшим в мире предприятием, специализирующейся на технологиях информационной безопасности. Компания McAfee поставляет проверенные упреждающие решения и услуги, которые обеспечивают безопасность систем, сетей и мобильных устройств по всему миру, позволяя пользователям безопасно работать и совершать покупки в Интернете. Наличие непревзойденной технологии Global Threat Intelligence, позволяет компании McAfee создавать инновационные продукты, которые помогают частным пользователям, компаниям, государственным организациям и поставщикам услуг Интернета обеспечивать соответствие нормативно-правовым требованиям, защищать данные, предотвращать нарушения работы, определять уязвимости, а также постоянно следить за уровнем собственной безопасности и повышать его. Компания McAfee непрерывно ведет постоянный поиск новых путей защиты своих клиентов. www.mcafee.com/ru

[1] https://blogs.mcafee.com/mcafee-labs/stuxnet-update

[2] Версия без грифа секретности находится на сайте http://www.defense.gov/news/d20110714cyber.pdf.

ООО «МакАфи Рус»
Адрес: Москва, Россия, 123317
Пресненская набережная, 10
Бизнес центр «Башни на набережной»
4ый этаж, офис 405 – 409
Телефон: +7 (495) 967 76 20
Факс: +7 (495) 967 76 00
www.McAfee.ru

40302rpt_threat-predictions_1211_fnl_ETMG