G Data SecurityLabs делает прогноз на тяжелый 2012 год

20 декабря 2011г., Москва – Лаборатория G Data SecurityLabs подвела итоги 2011 года, выявила основные тенденции рынка информационной безопасности в этом году и сделала прогноз на 2012 год. Важнейшими событиями уходящего года аналитики назвали бум вредоносного ПО для устройств на базе Android, увеличение количества таргетированных атак и банковских троянских программ. В следующем году пользователей ожидают спам и фишинг в преддверии крупных международных мероприятий, использование виртуальной валюты для создания ботсетей и попытки заражения новых устройств.

Мобильные зловреды на подъеме

Доля рынка мобильных устройств на платформе Android непрерывно росла в 2007 года, демонстрируя поразительные результаты и уверенно обгоняя конкурентов. Начав с 2% в середине 2008, эта мобильная операционная система стала абсолютным лидером в третьей четверти 2011 года уже с 52,2% рынка (по числу проданных устройств за определенный период). На ее фоне Symbian (16,9%) и iOS (15,0%) выглядят аутсайдерами. Но такое лидерство привлекает не только новых клиентов, рассчитывающих на огромный выбор приложений для Android, но и мошенников, готовых поживиться за счет этих приложений и специального вредоносного ПО для смартфонов и планшетных компьютеров. Среди популярных способов обмана – звонки и отправка тестовых сообщений без ведома пользователя, подписка на премиальные SMS, похищение персональной информации с телефона, угрозы из «корневого каталога» устройства и многое другое. Скорость, с которой появляются новый вредоносный код для Android, возрастает, в то время как небольшое количество обновлений для мобильной платформы шокирует.

В 2012 году аналитики **G Data SecurityLabs** ожидают еще большее распространение вредоносного ПО для Android, причем эта платформа будет напоминать Windows в том отношении, что зловредов станет гораздо больше, но это никак не повлияет на рост ее популярности среди пользователей. «Если сегодня вредоносный код попадает на мобильное устройство с подачи самого пользователя (он принимает все условия и разрешения определенного приложения), то через какое-то время пользователи столкнуться с автоматическим атаками и заражениями, в которые они будут вовлечены. Например, с вирусами «попутной загрузки», что характерно для компьютерных угроз, – рассказывает **Эдди Уильямс**, евангелист по безопасности **G Data SecurityLabs**. – Это позволяют технические характеристики мобильной платформы».

Классификация мобильных зловредов по новым функциям

Вредонос	Новая функция	Появление
FakePlayer	Премиальные SMS	08/2010
Geinimi	Ботнет	12/2010
ADRD	SEO	02/2011
DroidDream	«Корень»	03/2011
Plankton	Загружает дополнительный код	06/2011
Spitmo	Атака "Man-in-the-middle"	07/2011
NickySpy	Отчеты о звонках и фоновый шум; функции ботнета по SMS	08/2011
Walkinwat	Кибер-ловушки	10/2011
RuFraud	Премиальные SMS в Центральной Европе	12/2011

Популярность таргетированных атак

В 2012 году увеличится число таргетированных атак, как и мобильных вирусов, в первую очередь вследствие того, что представители компаний и их незащищенные рабочие смартфоны являются особенно «прибыльными» жертвами для преступников. Они могут получить не только корпоративную информацию с таких устройств, но и доступ в корпоративную сеть, если смартфон подключен в офисному Wi-Fi.

Такой способ проникновения вредоносного кода будет использован для последователей Stuxnet и Duqu, которые станут «грозой» корпоративных сетей в 2012 году. Идея о том, что мошенники могут получить доступ к критическим системам управления компании, перестала быть частью научной фантастики после отчета о Stuxnet на Иранском ядерном заводе или на Бушерской АЭС. Но создатели Duqu адаптировали этот вредонос для любой компании, и атака будет

направлена не на разрушение цели, а последовательный собор корпоративной информации, которая может быть использована для саботажа и промышленного шантажа. К этому готовы некоторые страны, например, ФБР объявило, что угрозы кибербезопасности станут причиной значительного увеличения численности состава их киберподразделений в течение 12-18 месяцев.

«2012 год станет годом таргетированных атак, причем с ними столкнутся не только крупные корпорации, но и более мелкий бизнес, – рассказывает **Эдди Уильямс**. – Я специально делаю акцент на компании из СМБ сегмента, потому что они меньше других защищены от внешних угроз, а значит, более привлекательны для атаки».

Атаки в преддверии международных событий
В следующем году запланированы важные международные события, в ряду которых:

- Чемпионат Европы по футболу, UEFA Euro (Польша и Украина) – 8 июня - 1 июля 2012 г.
- Летние Олимпийские Игры (Лондон) - 27 июля - 12 августа 2012 г.
- Президентские выборы в России - 4 марта 2012 г.
- Президентские выборы в США – 6 ноября 2012 г.

Например, британской полиции для обнаружения традиционных и киберпреступлений на этих мероприятиях уже выделено более 600 млн. фунтов.
В связи с этими событиями эксперты лаборатории **G Data SecurityLabs** ожидают следующие возможные угрозы:

- Волны спама и манипуляции с поисковиками для онлайн-мошенничества с поддельными билетами и распродажей атрибутикой мероприятий.
- Фальшивые и зараженные сайты для продажи билетов, которые будут использоваться для фишинга (для Олимпийских игр существуют уже с 2010 года).
- Атаки на официальные сайты мероприятий в качестве протеста.
- Создание специальных подложных точек доступа WLAN для участников мероприятий, с помощью которых можно получить доступ к их персональной информации.
- Многочисленные атаки на смартфоны и планшетные компьютеры.

Этот список можно продолжать бесконечно. Также не стоит забывать о целенаправленных атаках на инфраструктурные объекты мероприятий в целях саботажа или шантажа.

Если говорить о президентской гонке 2012 года в России и США, то среди уловок из разряда «социальной инженерии», на которые попадаются все больше пользователей, будут зараженные сайты с эксклюзивными и шокирующими фотографиями и видео кандидатов, уникальными подробностями из их личной жизни, а также спам-письма с предложениями посетить подобные сайты. Другим способом обмана будущих избирателей станут письма с предложением денег за их голос в пользу определенного кандидата. Но для получения денег им необходимо отправить злоумышленники свои банковские данные; это классический прием фишинга, который даже может повлиять на результаты выборов.

Банковские трояны облегчат карманы
По данным лаборатории **G Data SecurityLabs** в 2011 году самым популярным способом заполучения денег ничего не подозревающих жертв было использование банковских троянских программ, и нет никаких признаков того, что в следующем году эта тенденция пойдет на убыль. Дело в том, что количество пользователей онлайн-банкинга, подобно пользователям смартфонов, только увеличивается, и такая ситуация удобна мошенникам. По данным MForum Analytics в России интерет-банкинг использует каждый 10 пользователь сети Интернет, и этот показатель будет расти в следующем году, в том числе и с помощью любителей онайлн-банкинга че-

рез мобильный телефон. А если говорить о количестве преступлений в банковской сфере, то по информации МВД России, число зарегистрированных преступлений в этом году практически в два раза превышает аналогичный показатель в прошлом году. А еще есть пользователи, которые не сообщают о банковском мошенничестве в полицию.

Виртуальные деньги – реальные преступления
2012 год откроет для мошенников новые возможности махинаций с виртуальными деньгами благодаря веб-приложениями, играм и виртуальным сообществам, в которых реальные деньги используются для приобретения дополнительных опций. В этом огромном сегменте существует безграничные возможности для сложных атак (фишинг и вредоносное ПО), предназначенных для облегчения карманов пользователей с виртуальными долларами, золотыми монетами или другими платежными средствами. Таким образом, виртуальная валюта, которая с легкостью может быть реализована на подпольных форумах, будет иметь реальную денежную стоимость.

Одной из наиболее популярных в последнее время валютой считается BitCoint. Любой пользователь может заработать монеты, если он сделает мощности своего компьютера доступными для внешних операций. Такой с одной стороны безобидный проект не сулит какой-либо опасности, но мошенники так не думают. Если говорить о подобных проектах, то злоумышленники создают такую систему для вовлечения большего количество компьютеров в ботсети, регулярно выплачивая им виртуальные деньги. Помимо компьютеров вовлечь в ботсети можно и маршрутизаторы: их мощность ниже, но большинство из них редко обновляются и подключены к сети Интернет 24 часа в сутки. Объявления об аренде таких ботсетей можно найти на любом хакерском форуме.

Угрозы для новых устройств
Помимо классических «переносчиков» вредоносного кода в 2012 году все чаще будут встречаться случаи вирусного заражения среди других электронных товаров: телевизоров, подключенных к сети Интернет, или современных игровых консолей. Эти устройства обладают мощными графическими процессорами, что делает их привлекательными для вовлечения в ботсети для добычи виртуальной валюты. Зачастую эти устройства не защищены, и кросс-платформенные вирусы могут с легкостью на них проникнуть.

«Если говорить о росте количества вредоносного ПО, то в последние годы он наиболее заметен и драматичен. И по нашим данным эта тенденции продолжится в 2012 году. По-прежнему зловреды останутся лучшим оружием киберпреступников для мошенничества, кибершпонажа и даже хактивизма, – резюмирует **Эдди Уильямс**».