Отчет IBM X-Force по итогам первой половины 2012 года.

АРМОНК, штат Нью-Йорк, 20 сентября 2012 года — Корпорация IBM (NYSE: IBM) опубликовала отчет о тенденциях и рисках информационной безопасности по итогам первого полугодия 2012 г. ("2012 Mid-Year Trend and Risk Report"), подготовленный группой исследований и разработок в области информационной защиты IBM X-Force. Результаты исследования свидетельствуют о резком увеличении числа эксплойтов, использующих уязвимости браузеров, а также о новых проблемах с защитой паролей социальных медиа и мобильных устройств, в т.ч. в связи с BYOD-программами, поощряющими использование личных устройств на работе.

Новые атаки, использующие универсальные кросс-платформенные эксплойты

Со времени публикации предыдущего отчета Trend and Risk Report, группа IBM X-Force отметила увеличение числа вредоносных программ и рост активности злоумышленников в Интернете:

- Атакующие продолжают выбирать своей целью компьютеры пользователей, направляя их по не вызывающим сомнения ссылкам на давно проверенные и надежные сайты, которые теперь заражены вредоносным кодом. Через уязвимости браузеров злоумышленники могут установить вредоносное ПО на целевой системе. Веб-сайты многих известных и заслуживающих доверия организаций по-прежнему восприимчивы к такого рода угрозам.

- Рост числа атак с применением метода SQL-инъекций (SQL injection – модифицирование кода SQL-запросов к базам данных, с которыми взаимодействует легитимный веб-сайт) «идет в ногу» с расширением использования уязвимостей веб-приложений посредством таких методик, как «межсайтовый скриптинг» (cross-site scripting – возможность вставки постороннего HTML-кода в Web-страницу) и «обход директорий» (directory traversal – выход за пределы корневого каталога в ftp-серверах).

- По мере увеличения базы пользователей операционных систем Mac во всем мире, эта платформа все чаще становится объектом т.н. «постоянных угроз повышенной сложности» (Advanced Persistent Threat, APT) и соответствующих эксплойтов, начиная конкурировать по киберугрозам с платформой Windows.

«Мы зафиксировали рост числа сложных и целенаправленных атак, особенно на компьютеры Mac и системы парольной защиты сайтов социальных сетей, — сообщил Клинтон Макфадден (Clinton McFadden), старший управляющий операциями IBM X-Force по исследованиям и разработкам. — В качестве ответных мер, организации должны применять для своей безопасности проактивный подход, чтобы лучше защитить свои бизнес-процессы и данные, поскольку эти кибератаки будут продолжаться снова и снова, пока это приносит выгоду злоумышленникам».

Возникающие тенденции в области мобильной безопасности

Несмотря на то, что уже есть информация о появлении вредоносного мобильного ПО, большинство пользователей смартфонов в основном подвержены риску традиционного мошенничества с использованием платных SMS-сообщений. Этот вид мошенничества осуществляется путем автоматической рассылки SMS-сообщений на привилегированные телефонные номера в разных странах из установленных приложений. Для этого может применяться несколько подходов:

- Приложение, которое выглядит легитимным в магазине приложений, однако создано со злым умыслом;
- Приложение, которое представляет собой копию легитимного, но с другим именем и дополнительным вредоносным кодом;
- Реальное легитимное приложение, которое было инфицировано вредоносным кодом и, как правило, предлагается в альтернативном онлайновом магазине приложений.

Одним из революционных преобразований, меняющих правила игры в сфере мобильной безопасности, является распространение BYOD-инициатив. Многие компании все еще находятся на самой ранней стадии процесса приведения своих корпоративных политик в соответствие с современными реалиями и разрешения персоналу подключать свои личные ноутбуки и смартфоны к внутренней сети организации. А для того, чтобы принцип BYOD успешно заработал в компании, необходимо выработать и установить тщательно продуманные и ясные правила, регламентирующие эту практику, прежде чем первое личное мобильное устройство сотрудника будет интегрировано в корпоративную инфраструктуру. (См. полную версию отчета IBM X-Force Mid-Year Trend and Risk Report, где приводятся рекомендации по политикам BYOD.)

Надежный пароль – что это означает?

Связь между веб-сайтами, облачными сервисами и веб-почтой обеспечивает удобство работы, особенно при использовании для доступа к ним разных устройств, но пользователи должны быть очень осторожными с тем, что имеет отношение к учетным записям, паролям, а также той личной информации, которую они предоставляют для восстановления пароля или перенастройки учетной записи. Настоятельно рекомендуется использовать длинные пароли, состоящие из нескольких слов, а не неудобные сочетания букв, цифр и символов.

На стороне сервера, X-Force рекомендует шифровать пароли к базе данных с использованием хэш-функции, которая подходит для хранения паролей. Хеш-функция должна быть криптографически стойкой и использовать "salt value" (произвольный символ и подстроку, добавляемую к хэшируемуму тексту в целях повышения надежности) для каждой пользовательской учетной записи, чтобы снизить эффективность применения «радужных таблиц» ("rainbow tables" – используются для ускоренного взлома паролей) и атак с помощью методики «полного перебора по словарю» (brute force dictionary attack).

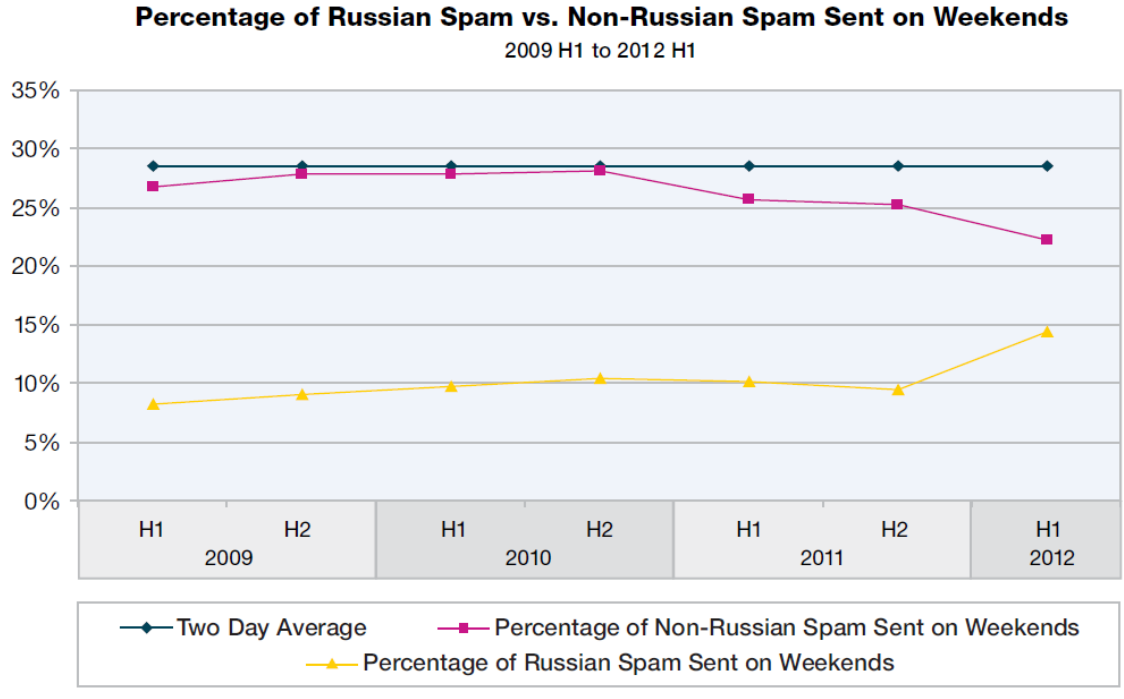
Интернет-безопасность повышается

В отчете 2011 IBM X-Force Trend and Risk Report отмечался определенный прогресс в некоторых областях интернет-безопасности. В текущем году продолжается снижение числа новых версий эксплойтов, есть также улучшения в выпуске десятью ведущими поставщиками программных исправлений, устраняющих уязвимости в их продуктах. Кроме того, наблюдается значительный спад по числу уязвимостей PDF-формата, что, как считает IBM, напрямую связано с новой технологией «песочницы» (Sandboxing), предложенной в версии Adobe Reader X. (Технология Sandboxing работает по принципу ограничения активности потенциально вредоносных приложений, что достигается за счет выполнения таких приложений в специально выделенной изолированной среде – песочнице.)

Цель методов защиты, использующих технологию Sandboxing – изолировать приложение от остальной системы, чтобы в случаях, когда приложение инфицировано вредоносным кодом, выполнение этого кода для деструктивных действий (таких как несанкционированный доступ, кража конфиденциальных данных) было ограничено. Эта технология на поверку оказалась весьма успешной инвестицией с точки зрения безопасности. Как сообщается в отчете X-Force, в первой половине 2012 года отмечено резкое уменьшение числа выявленных уязвимостей формата Adobe PDF, и эта тенденция совпадает по времени с появлением и широким распространением программного обеспечения Adobe Reader X, в котором реализована технология Sandboxing.

Статистика по регионам

- Хотя количество рассылаемого по всему миру спама в первом полугодии 2012 г. зафиксировалось на низкой отметке, начиная с четвертого квартала 2011 года и до нынешнего момента наибольшее количество ресурсов, упоминаемых в спам-рассылках, было зарегистрировано на домене .ru. Второе и третье места по количеству зарегистрированных сайтов, ссылки на которые содержатся в спаме, занимают, соответственно, домены .com и .info. Домен .рф также остается среди лидеров по этому показателю.
- Согласно данным X-Force, по итогам 1 половины 2012 года Россия опустилась на седьмое (около 3%) место по количеству рассылаемого спама в сравнении со вторым местом за аналогичный период прошлого года. Странами-лидерами по количеству рассылаемого спама остаются Индия (16 % – максимальный показатель за историю исследований) и США (чуть более 8%); также в «первую тройку» снова вышел Вьетнам (9%).
- Как выяснила группа X-Force, российские спамеры, в противоположность мировой статистике и тенденциям за последние 3 года исследований, стали активнее заниматься рассылкой писем в выходные дни. Согласно отчетам X-Force за 2009-11 годы, не более 10% спама на русском языке рассылалось в выходные (по миру этот показатель составлял в разное время не менее 25%, показывая незначительную разницу со средним арифметическим показателем – 28,6%). В первом полугодии 2012-го эта доля выросла до 14%, в то время как активность спамеров по миру в выходные дни снизилась до 22% – минимальный показатель за последние 3 года (см. график ниже). X-Force предлагает несколько объяснений этим данным: 1) российские спамеры продолжают автоматизировать процесс рассылки, вследствие чего выравниваются показатели их активности в будние и выходные дни; 2) возможно, российские спамеры рассчитывают на то, что сотрудники компаний, занимающихся защитой от спама, отдыхают от работы в выходные дни; 3) в то же время, не исключено, что спамеры по всему миру сокращают объемы рассылки в выходные, так как многие пользователи «чистят» свои почтовые ящики в начале недели; 4) также возможно, что схождение показателей происходит непреднамеренно, из-за ограничения количества инструментов, используемых для рассылки.



График, демонстрирующий разницу в активности спамеров в России и по всему миру в выходные дни

Об отчете IBM X-Force Trend & Risk Report

Отчет исследовательской группы IBM X-Force о тенденциях и рисках информационной безопасности (Trend and Risk Report) представляет собой ежегодную оценку общего состояния безопасности, выполняемую с целью помочь клиентам лучше понять и осмыслить новейшие риски, связанные с нарушением безопасности, и предпринимать необходимые меры по опережению этих угроз. Отчет содержит фактическую информацию из многочисленных источников, включая: каталог X-Force с более 68 тыс. уязвимостями компьютерной безопасности; глобальный поисковый робот (Web crawler), сканирующий веб-страницы; многоязыковые спам-коллекторы; а также системы мониторинга в реальном времени, ежедневно регистрирующие, в среднем, 15 млрд. событий безопасности для почти 4000 клиентов в более 130 странах мира. Эта регистрация 15 млрд. событий в день (или свыше 150 тыс. событий в секунду) является результатом работы десяти международных центров IBM по управлению безопасностью (Security Operations Centers, SOC), которые предоставляют клиентам профессиональные услуги категории Managed Security Services. Полная версия отчета X-Force 2012 Mid-Year Trend and Risk Report опубликована на www.ibm.com/security/xforce.

.