Летом активность киберпреступников обычно спадает (ведь даже им иногда нужно отдыхать), однако количество и степень изощренности новых угроз в третьем квартале 2013 года заставляют предположить, что в этот раз киберпреступники на «летние каникулы» не уходили. Количество новых образцов вредоносных программ для ПК в отчетном квартале росло относительно стабильно: «зоопарк» McAfee пополнился 20 млн новых образцов, теперь их в нем свыше 170 млн. «Зоопарк» вредоносных программ для Android увеличился почти на 700 000 образцов, и теперь в нем 2,8 млн образцов.

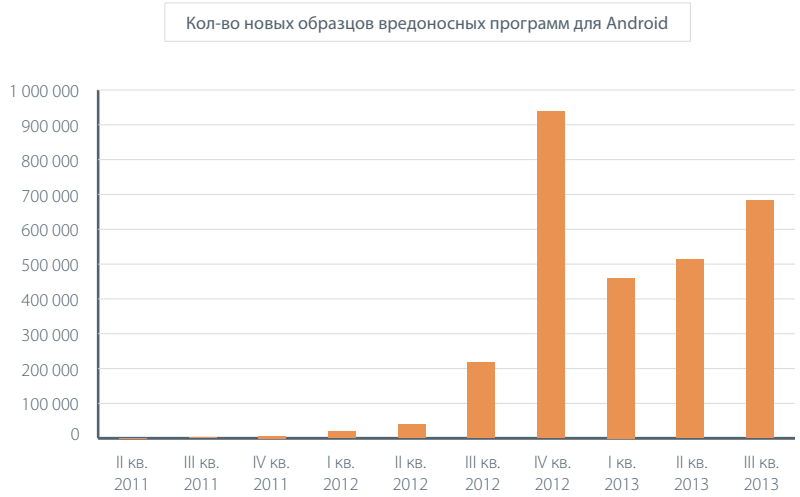
Были отмечены четыре основные тенденции, свидетельствующие о том, что при защите конфиденциальных данных предприятиям и физическим лицам нужно проявлять постоянную бдительность.

- Количество атак на мобильную операционную систему Android выросло более чем на 30 %, что отчасти обусловлено появлением средств использования хорошо задокументированной уязвимости в мастер-ключе Android, которая дает злоумышленникам возможность обходить процедуру проверки подписи, предназначенную для выявления вредоносных приложений.
- Появление все большего количества «подписанных» вредоносных программ по-прежнему ставит под сомнение достоверность многих из используемых в настоящее время цифровых сертификатов и заставляет задуматься о том, как предприятия и пользователи могут отличать достоверные сертификаты от недостоверных.
- Общемировой объем спама вырос на 125 %.
- Использование киберпреступниками новых виртуальных денег как для проведения нелегальных транзакций, так и для отмывания прибылей, полученных в результате сетевых и внесетевых преступных действий, привело к невиданному прежде уровню преступной деятельности в так называемом «глубинном вебе» (Deep Web).

### Вредоносные программы для мобильных устройств

Атаки на платформу Android по-прежнему шли непрерывной чередой. В отчетном квартале было зарегистрировано почти 700 000 новых образцов вредоносных программ для Android. В 2012 году резкий скачок количества вредоносных программ для Android наблюдался в четвертом квартале; посмотрим, повторится ли этот сценарий в 2013 году.

Аналитики McAfee Labs выявили совершенно новое семейство вредоносных программ для Android: Exploit/MasterKey.A. Эти программы дают злоумышленнику возможность обходить процедуру проверки цифровой подписи приложений. Поскольку процедура проверки цифровой подписи является ключевым компонентом системы обеспечения безопасности в Android, данное открытие не может не вызывать тревогу. Аналитики McAfee Labs обнаружили также новый класс вредоносных программ для Android, которые после завершения установки без ведома пользователя загружают на устройство вредоносный код для запуска «второй ступени».



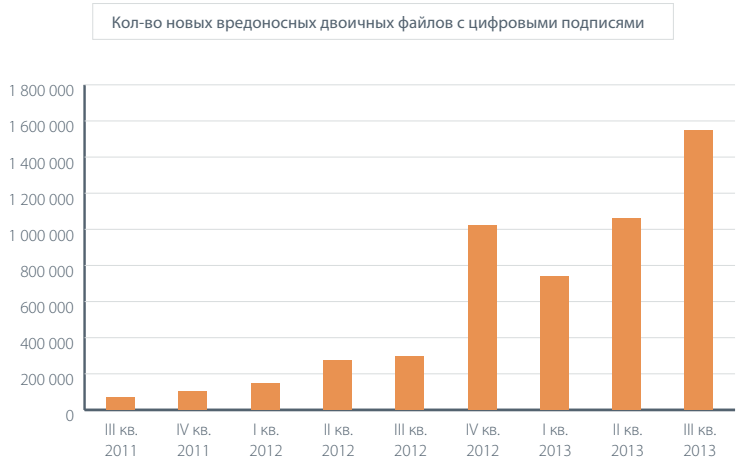
## Вредоносные программы с цифровыми подписями

Исторически сложилось так, что для обнаружения вредоносных программ многие компании создают в своих межсетевых экранах и других средствах защиты сетевой периферии правило, позволяющее проверять, имеет ли двоичный файл цифровую «подпись». При этом все исходят из того, что двоичные файлы, подписанные с помощью сертификата, выпущенного известных органом сертификации, являются достоверными. К сожалению, киберпреступники это хорошо понимают и теперь все чаще подписывают свой вредоносный код либо с помощью похищенных сертификатов, либо с помощью сертификатов, выпущенных ненадежными органами сертификации.

Некоторое время назад специалистами McAfee Labs был отмечен рост вредоносных программ с цифровыми подписями. Данный прием продолжает набирать популярность, потому что позволяет киберпреступникам относительно легко обходить один из самых распространенных методов фильтрации двоичных файлов. Согласно нашим наблюдениям, в отчетном квартале количество вредоносных программ с цифровой подписью выросло почти на 50 %.

В октябре сотрудники McAfee Labs сообщили о том, что доля вредоносных программ с цифровой подписью выросла с 1,3 % в 2010 году до 5,3 % в 2013 году. Данное изменение может показаться небольшим, однако в абсолютных цифрах это означает, что в обороте находится более 5 млн образцов вредоносных программ с цифровой подписью. Еще отчетливее эта тенденция проявляется на мобильном «фронте»: за последние три года доля вредоносных программ с цифровой подписью выросла практически с нуля до почти 25 % от всех известных образцов вредоносных программ для Android.

Как отметили сотрудники McAfee Labs на конференции FOCUS 2013, несмотря на то, что в обороте находится большое количество недостоверных цифровых сертификатов, у киберпреступников, похоже, нет явных предпочтений в выборе сертификатов. Нами выявлено всего несколько сертификатов, каждый из которых был использован для создания цифровой подписи более чем для 1 000 отдельных вредоносных двоичных файлов. Еще около десятка обнаруженных нами сертификатов было использовано для создания цифровой подписи порядка 500 различных экземпляров вредоносных программ. Время покажет, поможет ли такая концентрация сертификатов на «вершине» пирамиды блокировать и изолировать вредоносный код на практике.



## Всплески объемов спама

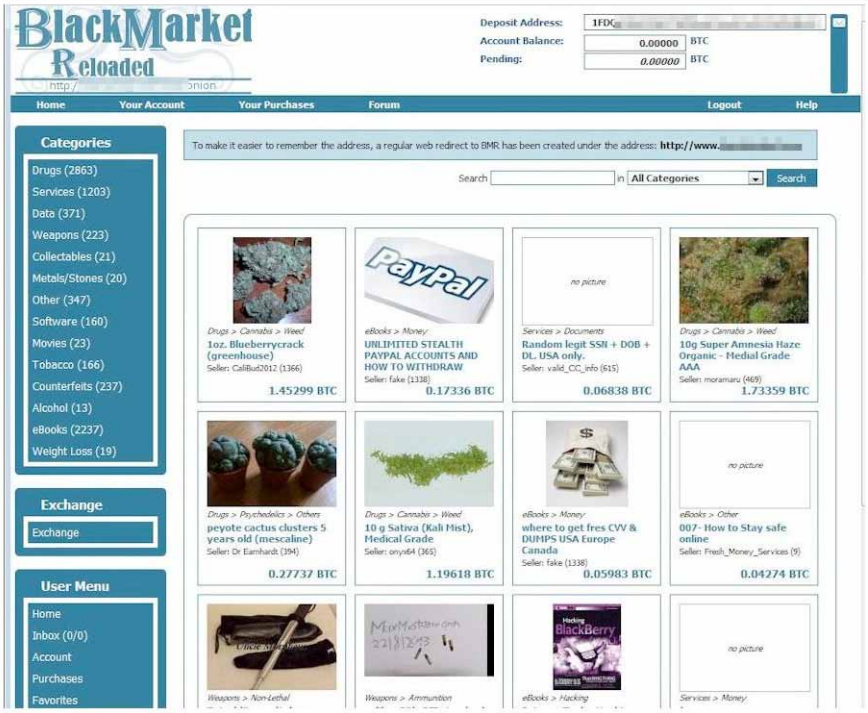
После многих лет падения и наблюдавшегося в прошлом году относительно стабильного роста общемировой объем спама в третьем квартале 2013 года резко вырос. Основная часть этого всплеска пришлась собственно на последние четыре недели квартала. За весь квартал общемировой объем спама вырос на 125 %. Аналитики McAfee Labs считают, что этот всплеск в значительной степени обусловлен тем, что маркетинговые фирмы приобретают и используют списки адресов, полученные ими из источников с сомнительной репутацией. Эти фирмы, занимающиеся партнерским маркетингом и называемые «спаммерами на снегоступах», продают свои услуги компаниям, продвигающим потребительские бренды, и используют все доступные им методы и списки адресов для максимально широкого распространения рекламы и повышения коэффициента реагирования. Сообщения, рассылаемые в рамках таких массовых кампаний, обычно не содержат вредоносных программ, однако у пользователей почти нет возможности отличить одно от другого.


## Виртуальные деньги

За последние двенадцать месяцев одной из самых животрепещущих тем в киберпространстве стало появление новой разновидности виртуальных денег, стоимость которых не привязана к традиционным денежным единицам (долларам, евро, йенам и т. п.) По оценкам Yankee Group так называемый рынок виртуальных денег в 2012 году вырос до 47,5 млрд долларов США. Эти новые виртуальные деньги имеют реальную практическую ценность: они позволяют продавать и покупать товары и услуги в Интернете без тех ограничений, которые накладывает использование обычной кредитной или дебетовой карты, и без тех технических сложностей, с которыми связан перевод денежных средств в электронном виде. Их дополнительное преимущество заключается в возможности анонимно совершать транзакции.

Именно эта анонимность и привлекает киберпреступников: она позволяет им заключать сделки по продаже нелегальных товаров и услуг, лишая правоохранительные органы возможности отслеживать транзакции. Кроме того, она дает им исключительно эффективный способ «отмывания» прибылей, полученных в результате сетевых и внесетевых преступных действий. В недавно опубликованном отчете McAfee Labs под названием «Цифровая „прачечная“ по отмыванию денег. Анализ виртуальных валют и их использования в киберпреступности»[1] описывается, как благодаря виртуальным деньгам киберпреступники получили возможность предлагать в Интернете наркотики, оружие и другие нелегальные товары и услуги. В отчете также рассказывается о том, как с помощью площадок обмена виртуальных денег производится отмывание огромных прибылей, полученных незаконным путем.

Появление виртуальных денег и их анонимный характер привели также к возникновению в «глубинном вебе» целого ряда сайтов купли-продажи, специализирующихся на розничном сбыте нелегальных продуктов и услуг.




Крупнейшим из этих сайтов был сайт Silk Road, закрытый сотрудниками правоохранительных органов 1 октября текущего года. Он был известен в первую очередь как место торговли наркотиками, хотя на нем продавалось более 200 категорий товаров и услуг, включая услуги по взлому банкоматов. Хотя закрытие Silk Road стало крупной победой правоохранительных органов, необходимо отметить, что по-прежнему в «глубинном вебе» по всему миру работает множество подобных площадок купли-продажи. BlackMarket Reloaded — лишь одна из них. Очевидно, что решения этой проблемы в ближайшее время не предвидится.

Полный текст отчета находится по этой ссылке: www.mcafee.com/ru/resources/reports/rp-quarterly-threat-q3-2013.pdf.

[1] http://www.mcafee.com/ru/resources/white-papers/wp-digital-laundry.pdf

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


60653exs_qtr-q3_1113_fnl_ETMG