Краткая сводка

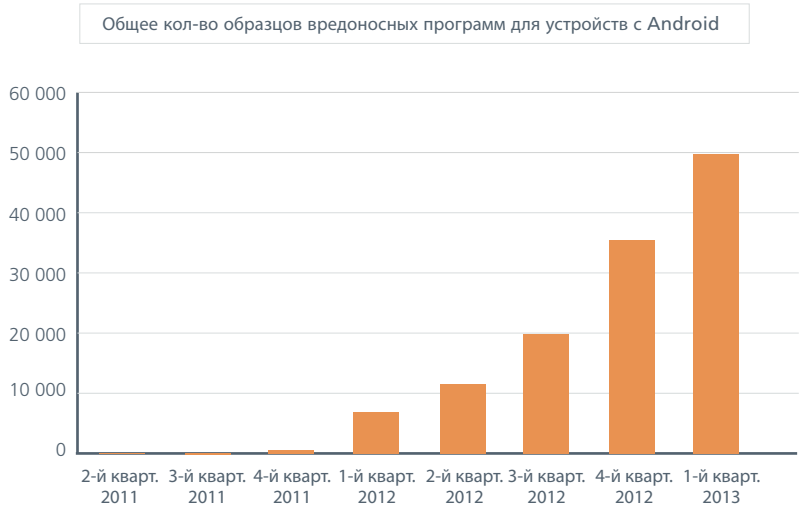
Отчет McAfee об угрозах за первый квартал 2013 года

McAfee® Labs

В I квартале 2013 года международное киберпреступное сообщество сделало большой шаг «назад в будущее» в своей непрерывной погоне за жертвами и прибылями. Многие из наиболее заметных тенденций, наблюдаемых лабораторией McAfee Labs в течение предыдущих трех кварталов, временно ослабли, в то время как число более ранних видов атак и так называемых «ретровредоносных программ» значительно возросло.

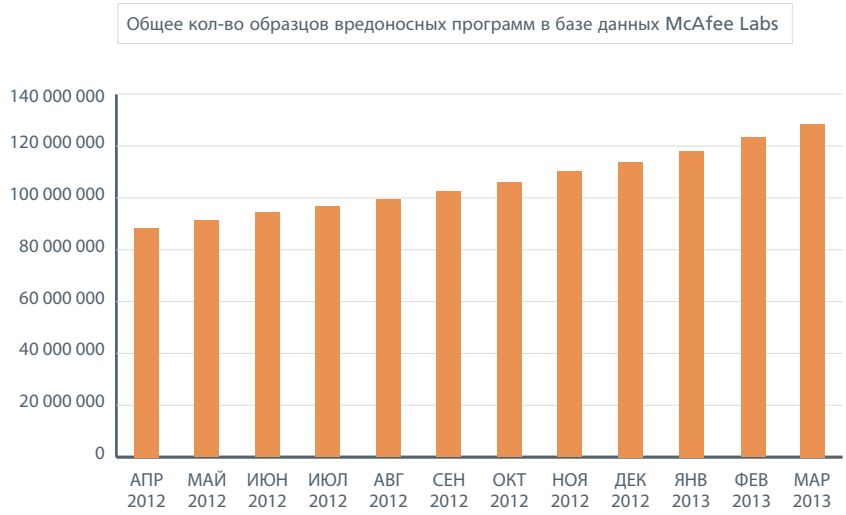
Среди тенденций угроз, бывших недавно актуальными и ставших менее заметными в I квартале 2013 года, следует назвать:

Замедление роста новых вредоносных программ, направленных на мобильные устройства (на платформе Android). Хотя общее число новых образцов вредоносных программ, атакующих Android, увеличилось на 40 процентов, по сравнению с IV кварталом 2012 года темпы роста замедлились на 10 процентов.



Аналогично, число обнаруженных в I квартале злоумышленных веб-сайтов возросло на 12 процентов, однако темпы их роста, составившие в IV квартале более 80 процентов, упали почти на 40 процентных пунктов.

В I квартале несколько замедлился даже темп роста образцов известных вредоносных программ до 28 процентов (для сравнения: в IV квартале 2012 года 38 процентов). В I квартале 2013 года лаборатория McAfee Labs добавила к своему «зоопарку» вредоносных программ более 14 миллионов новых образцов.



Наконец, в первом квартале темпы роста обнаружения общего числа программ для кражи паролей, программ-вымогателей, ложных антивирусов и руткитов оставались относительно невысокими. Хотя абсолютное количество всех этих угроз продолжает расти, темпы их роста несколько снизились.

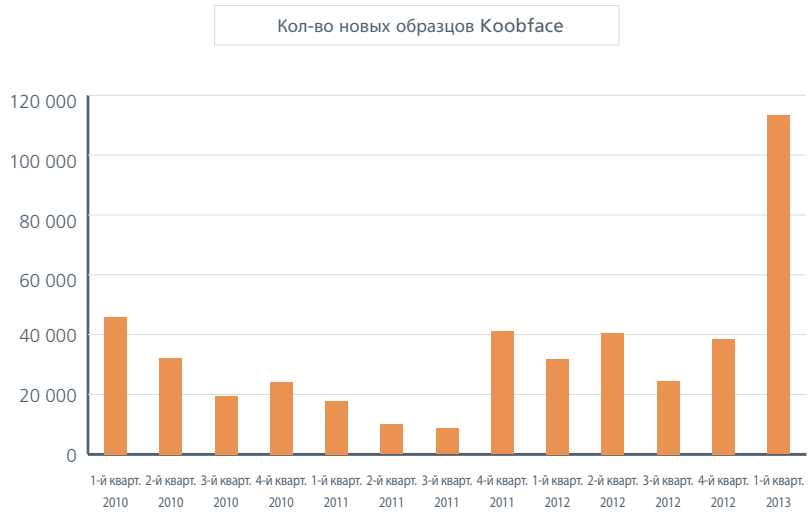
Однако замедление темпов роста не означает, что киберпространство становится безопаснее. Напротив, при рассмотрении этих изменений на фоне других тенденций, отмеченных в первом квартале, становится очевидно, что киберпреступное сообщество становится умнее и дисциплинированнее, начиная отдавать предпочтение целенаправленным атакам, направленным на конкретные группы или регионы. Как и любой бизнес, киберпреступные синдикаты стремятся повысить эффективность своих действий и увеличить прибыль. Представляется, что отмеченная тенденция роста целенаправленных атак сигнализирует о том, что мировой ландшафт угроз меняется в сторону нового и более опасного направления.

Основным примером этой тенденции увеличения целенаправленных атак может служить троян Citadel. Троянская программа Citadel, первоначально разработанная для хищения денежных средств из конкретных банков, была «обновлена», и может теперь использоваться как средство добывания личной информации из компьютерных систем жертв, выбранных преступником.

Ниже приведены примеры других выявленных в I квартале тенденций угроз, истоки которых уходят в более ранние времена, но которые сегодня применяются в целенаправленных и еще более опасных атаках.

Лаборатория McAfee Labs впервые за период, составивший более трех лет, зафиксировала общий рост объема спама в мире. При этом возвращение на сцену этой угрозы отличается массовостью: в I квартале 2013 года объема спама вырос почти вдвое. Однако общие показатели роста спама по всему миру не дают точного представления об темпах роста, поскольку специалисты McAfee Labs наблюдали весьма значительные различия в увеличении объемов спама в разных регионах мира. И вновь представляется, что преступники атакуют конкретные регионы, используя конкретные схемы мошенничества в надежде обмануть новые жертвы. Распространенные виды мошеннических сообщений в I квартале включали в себя возрожденные схемы мошенничества на фондовом рынке (так называемая «накачка и сброс») и предложения препаратов, якобы содержащих гормоны роста.

В прошлом году случаи выявления Koobface (червя, впервые выявленного в 2008 году) были относительно малочисленными, однако в первом квартале 2013 года возросли *втрое* до невиданного прежде уровня. Очевидно, что члены киберпреступного сообщества считают пользователей социальных сетей весьма многообещающей средой для поиска потенциальных жертв.



Среди других «ретроугроз», всплеск которых наблюдался в I квартале, нужно назвать новые образцы вредоносных программ с автозапуском. Традиционно черви с автозапуском распространялись через флеш-накопители USB или компакт-диски. Эта вредоносная программа особенно полезна для киберпреступников, так как черви с автозапуском могут использоваться для установки на зараженных машинах программ обхода систем защиты («черных ходов») или программ для кражи паролей. Всплеск случаев обнаружения червей с автозапуском, вероятно, обусловлен распространенностью облачных сервисов для обмена файлами.

Кроме этих атак, пришедших из прошлого в будущее, специалисты McAfee Labs отметили значительный рост относительно новых атак, использующих «стек памяти». Цель этих атак, известных как атаки на основную загрузочную запись, заключается в том, чтобы заразить систему памяти машины и оттуда получить контроль за всем устройством. В I квартале число образцов атак на главную загрузочную запись возросло на 30 процентов.

Что означают эти новые тенденции для организаций, пытающихся оптимизировать свои системы обеспечения безопасности? Учитывая изменения в ландшафте угроз, для защиты конечных точек требуется использование многослойной защиты, которая включает не только базовые антивирусные программы, но также системы предотвращения вторжений и механизмы фильтрации веб-трафика. В связи с постоянным ростом использования зараженных веб-сайтов с целью распространения вредоносных программ важность этих двух функций возрастает как никогда. В некоторых средах может также потребоваться использовать защитные средства для контроля за устройствами и приложениями с целью защиты критически важной для выполнения задач информации, находящейся на устройствах конечных пользователей.

Кроме обеспечения многослойной защиты конечных точек администраторы систем защиты должны быть вооружены более функциональными инструментами формирования отчетов и реагирования. Важность этого формирующегося «отсека безопасности» будет все более возрастать, что позволит специалистам-практикам реагировать на новые целенаправленные атаки быстро и эффективно.

Защита инфраструктуры также потребует многослойной защиты от угроз, исходящих из Интернета, электронной почты и сети. Оптимальным способом защиты от новых угроз является их блокирование до проникновения в корпоративную инфраструктуру. Однако в результате возрастающего использования «облачных» сервисов помимо стандартной защиты периметра требуется также обеспечить корпоративную защиту данных, находящихся в «облаке», и неизменно применять ее — независимо от места развертывания данных и приложений, критически важных для выполнения задач.

Полный текст отчета находится по этой ссылке: http://www.mcafee.com/ru/resources/reports/rp-quarterly-threat-q1-2013.pdf.

McAfee
An Intel Company

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