ЗАЩИТА ОТ ВРЕДОНОСНОГО КОДА НА МОБИЛЬНЫХ УСТРОЙСТВАХ

Николай ПЕТРОВ
CISSP, Заместитель генерального директора АО «ДиалогНаука»

Прочитав название статьи, вы, наверно, подумали, что я буду рассказывать про антивирусы?

Совсем нет, в данной статье я бы хотел как раз рассмотреть вредоносный код, который не обнаруживается стандартными средствами, например, межсетевыми экранами, системами обнаружения/предотвращения вторжений, антивирусным программным обеспечением.

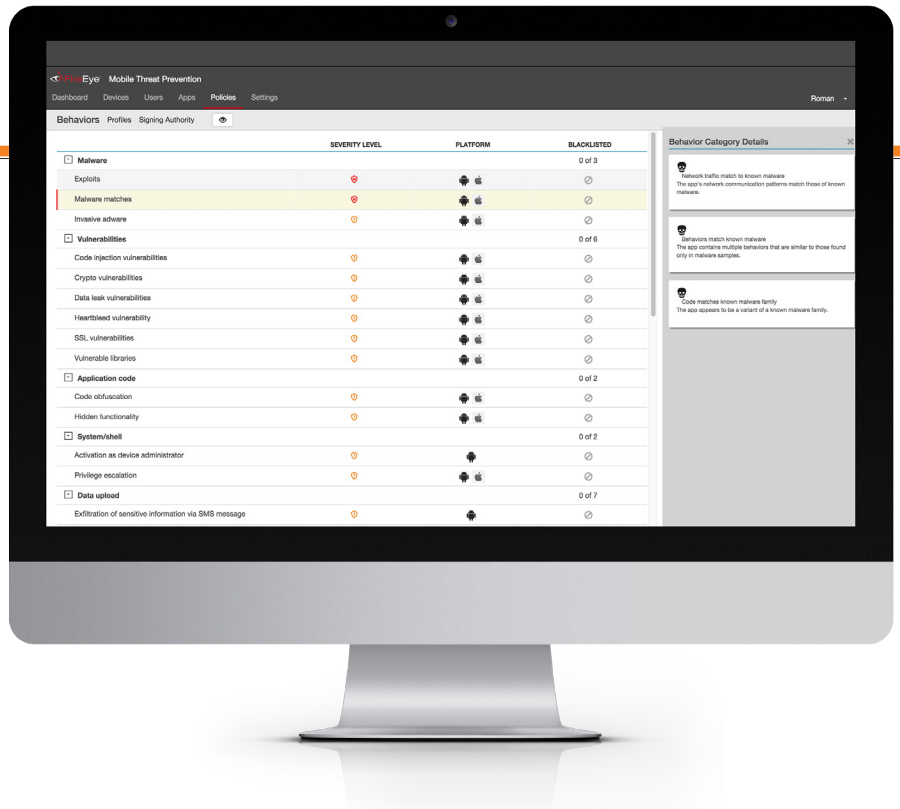
Мы все используем мобильные устройства в повседневной жизни, кто-то смартфоны, кто-то планшеты, а некоторые — и то, и другое.

Кроме просмотра сайтов сети Интернет и работы с электронной почтой, мы используем мобильные устройства для бронирования отелей, покупки билетов, аренды машин. Мы используем мобильные устройства для доступа к нашим сбережениям, к нашим банковским счетам.

При этом мы пребываем в полной уверенности, что, например, СМС-подтверждение от банка получаем только мы и никто другой.

А наш банк, как мы знаем, очень надежный, уделяет огромное внимание информационной безопасности. И поэтому — мы в безопасности. Но так ли все просто?

Что если вредоносный код, не определяемый антивирусом, находится в вашем смартфоне или планшете и что-то делает без нашего ведома?



Чем может грозить нам и нашим деньгам эта скрытая активность?

Что может произойти в этом случае?

В качестве иллюстрации позвольте упомянуть случай, имевший место в апреле 2015 года в одном из ТОП-5 банков России.

Клиенты этого банка даже не думали, что деньги с банковских счетов могут пропасть, когда устанавливали новый, но, увы, фальшивый Flash-проигрыватель.

После установки вредоносная программа отправляла СМС-сообщение на закрепленный за этим банком «короткий» номер, с банально простым запросом: «Баланс».

Если она получала ответ, это означало, что данный телефонный номер привязан к банковскому счету, с возможностью управления с помощью СМС.

После этого вредоносная программа отправляла денежные переводы на счета злоумышленников.

Естественно, что вредоносная программа стирала отправляемые и получаемые сообщения, включая подтверждения проведения операций от банка.

Проблема состоит в том, что случаи получения вредоносного программного обеспечения на мобильные устройства не единичны.

Так, в феврале 2015 года, Google удалил 3 вредоносных приложения из Google Play, которые были скачаны 15 миллионов раз!

Вот эти приложения: «Durak» — предназначенное для англоговорящих пользователей, «IQ Test» и «Russian History» — для русскоговорящих пользователей.

Причем, что интересно, вредоносное ПО начало действовать, когда после его инсталляции прошло 30 дней. Умно, правда?

Что же оно делало? Каждый раз, когда пользователь обращался к устройству, ему выводилось сообщение о проблеме, например, устройство заражено, ПО устарело или выводилась порно-картинка на весь экран, которую нельзя было убрать.

После этого предлагалось совершить определенные действия: посетить фальшивый сайт, скачать новую версию приложения, отправить платный СМС, провести оплату с помощью банковской карты.

Что же делать? Все безнадежно?

Защититься от описанных выше атак можно.

Рассмотрим FireEye, решение мирового лидера в защите от целенаправленных атак, в том числе — для защиты мобильных устройств.

Компания помогает защищаться от целенаправленных атак, использующих уязвимости нулевого дня, с 2006 года. 16 из 22-х опубликованных уязвимостей нулевого дня в 2013–2014 годах были обнаружены именно FireEye.

Решения FireEye применяют более трети компаний из Fortune 100.

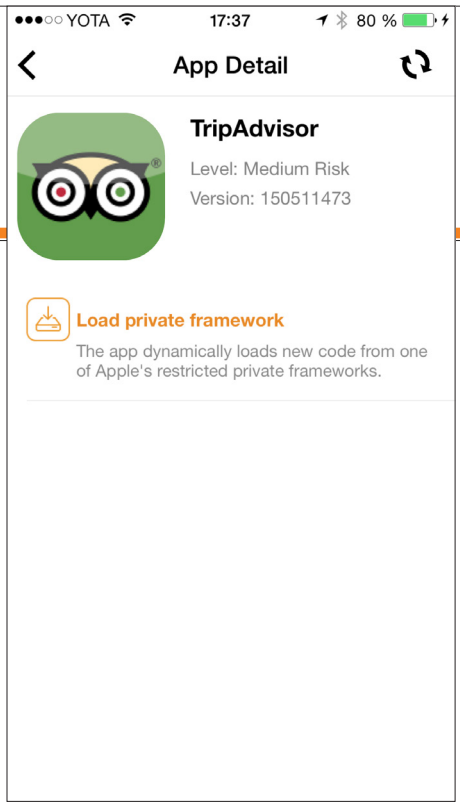
На сегодняшний день это единственное решение, которое поддерживает пользовательские операционные системы Microsoft и Mac OS X, и мобильные операционные системы iOS и Google Android.

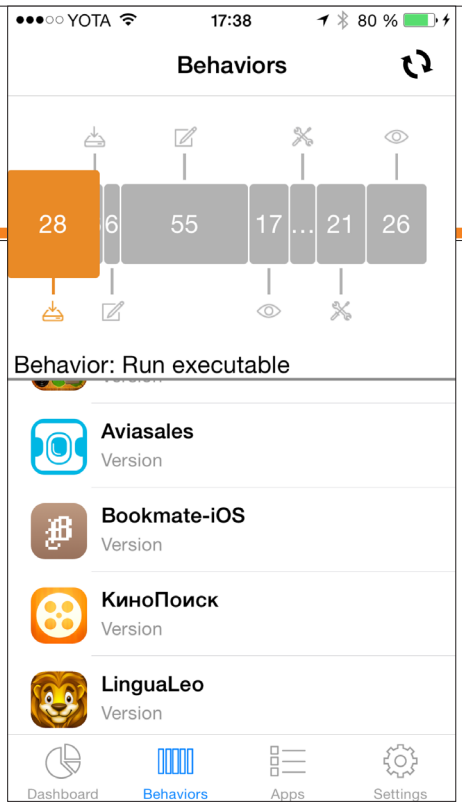
Для того чтобы разобраться с работой решения, давайте рассмотрим алгоритм работы системы при защите корпоративной сети.

Система анализирует входящий и исходящий трафик, обнаруживает известные типы атак, а также проверяет наличие соединений с серверами управления злоумышленника. Если известная атака или связь с сервером управления обнаружена, то система блокирует соединение.

Для атак нулевого дня, система помещает файлы или веб-страницу в виртуальную среду для анализа. FireEye использует собственную систему виртуализации для выявления признаков вредоносной активности. Наличие собственной системы виртуализации позволяет «обманывать» вредоносный код, заставляя его полагать, что он запускается на реальной, а не на виртуальной машине.

В виртуальной среде запускаются различные версии операционной системы Mac OS X, Microsoft Windows и приложений Microsoft Office, Microsoft Internet Explorer, Adobe Reader и т.п. С их помощью обрабатываются подозрительные файлы и веб-ссылки. При обнаружении атаки, например, вследствие создания нового сервиса, изменения в корневом разделе файловой системы, попытке установления соединения с сервером управления, виртуальная машина перезапускается. Виртуальная машина существенно затрудняет свое обнаружение, она имитирует действия пользователя: движение мыши, набор с клавиатуры и т.п.





Не секрет, что многие варианты вредоносного ПО, попадая на компьютер жертвы «засыпают» и ничем себя не обнаруживают в течение определенного времени. Это могут быть часы, дни, недели. Решение FireEye способно «ускорить время», вынуждая вредоносное ПО перейти к запрограммированным во времени действиям.

Если подтверждается атака нулевого дня, система записывает последующие действия вредоносного ПО. На основе полученных данных система формирует новый профиль защиты для блокирования ставшей уже известной атаки.

Новый профиль защиты передается на другие устройства FireEye, которые находятся в сети организации.

Для защиты мобильных устройств разработано решение FireEye Mobile Threat Prevention, поддерживающее мобильные операционные системы Android и iOS. Работает оно следующим образом. На мобильное устройство устанавливается пассивный агент FireEye Mobile Threat Prevention, который можно загрузить из Google Play или AppStore. Управление агентами осуществляется с помощью сервера управления, размещаемого в корпоративной сети. Виртуальная машина, используемая для анализа приложений, находится в Облаке FireEye. Проанализировать приложение можно несколькими способами: самостоятельно загрузить его в облако FireEye, передать URL ссылку на его файл или указать, что для анализа нужно использовать версию, находящуюся в Google Play или AppStore.

Работа агента заключается в инвентаризации установленных приложений. Для того чтобы отличать установленные версии приложений, агент использует криптографические хеши. Решение обнаруживает:

- неизвестное вредоносное ПО, которое пропускают антивирусы;
- библиотеки, используемые для рекламы (adware);
- уязвимости в приложениях;
- подозрительное/нестандартное поведение приложений.

Если анализ приложения уже проводился, то FireEye оповещает пользователя об опасном приложении до того, как оно будет установлено. Если приложение находится в Google Play или AppStore, то очень вероятно, что оно уже было проанализировано по автоматическому запросу другого пользователя FireEye.

FireEye Mobile Threat Prevention интегрируется с MDM решениями от MobileIron, AirWatch, Samsung Knox. Использование MDM решений позволяет блокировать и удалять вредоносное ПО, при необходимости уничтожать корпоративную информацию или блокировать устройство в случае потери или кражи.

ДиалогНаука активно применяет решение FireEye для защиты своих клиентов.

За последний год мы провели десятки пилотных проектов и внедрений решения FireEye для защиты корпоративной сети.

Я хотел бы поделиться статистикой.

Практически в каждом пилотном проекте решение FireEye обнаружило внутри корпоративной сети персональные компьютеры, управляемые извне.

Иными словами, злоумышленники могли получать любой доступ к информации на этих компьютерах, читать и копировать документы и электронную почту, знать все пароли пользователя.

Уникальность решения FireEye обеспечивается следующим:

- поддержка Microsoft Windows, Mac OS X, мобильных операционных системы iOS и Google Android;
- выявление вредоносного кода, который не могут обнаружить антивирусы, межсетевые экраны, системы IDS/IPS и другие средства защиты;
- контроль всех каналов распространения вредоносного ПО: Web, e-mail, HDD, CD, DVD, USB и др.;
- собственная система виртуализации для выявления признаков вредоносной активности;
- предустановленный набор операционных систем и приложений, не требующих установки;
- анализ не только исполняемых файлов и MS Office, но и других (более 30 типов файлов, включая графические, аудио, видео);
- минимальное количество ложных срабатываний;
- выявление вредоносного кода, который уже присутствует в сети и в мобильных устройствах компании.

* * *

Подробнее ознакомиться с характеристиками решения можно по ссылке http://fireeye-russia.ru.