Автор: Алина Саратова НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2535 06.07.2016, 16:42
12

Заработок в Сети по-китайски

По миру твердой поступью – нет, даже не поступью, а спринтерским бегом – распространяются два новых вируса: YiSpecter для iOS и HummingBad для Android. Их обнаружили эксперты израильской компании Check Point в феврале текущего года, а первые упоминания программы HummingBad относится еще к 2015 году. Почему же о них заговорили только сейчас? С середины мая 2016 года количество зараженных ими устройств резко выросло.

По данным исследователей, заражено уже более 85 000 000 Android-устройств

и хотя пока приложения используются в основном для отображения нежелательной рекламы, исследователи опасаются, что вскоре это может измениться. А ответственность за распространение вредоносных программ лежит на китайской рекламной фирме Yingmob, что базируется в Чунцине (по другим данным – в Пекине).

> «У этой компании есть несколько команд разработчиков, которые создают законные инструменты отслеживания пользовательского поведения в интернете и рекламные платформы, - сообщает Check Point. - Но есть и команда, которая отвечает за разработку вредоносного ПО, в ней работает около 25 человек».

По оценкам Check Point, приложения и рекламные инструменты от Yingmob установлены на 85 млн устройств на Android, из них на 10 млн - вредоносное ПО. Сообщается, что вирусом HummingBad поражено больше всего устройств в Китае (1,6 млн) и Индии (1,4 млн). В списке 20 стран с наибольшим числом пораженных устройств есть Турция (450 тыс.), США (287 тыс.), Россия (208 тыс.), Египет (140 тыс.), Украина (117 тыс.). Половина зараженных устройств работают на версии Android KitKat, 40% - JellyBean, на Lollipop приходится 7% зараженных устройств, Ice Cream Sandwich - 2%, Marshmallow - 1%.

Израильская компания отмечает, что это одна из наиболее высокоорганизованных вирусных атак, устроенная, к тому же, рекламным агентством, работающим на законных основаниях. В связи с этим исследователи опасаются, что примеру китайской компании по установке вируса для извлечения прибыли от рекламных заходов могут воспользоваться и другие недобросовестные компании.

YiSpecter и HummingBad, по сути, выполняют одни и те же задачи, просто они предназначены для разных ОС. Оба вируса отображают навязчивую рекламу на зараженных устройствах, а также устанавливают дополнительные приложения, что и приносит доход авторам данных программ.

Сообщается, что вирус может проникнуть в телефон посредством скрытой загрузки при посещении ряда сайтов, в том числе порнографических. Другой способ - пользователю выбрасывается баннер-предупреждение об угрозе его устройству и предлагается загрузить защитную программу. Проникнув в телефон, вирус устанавливает программу, которая дает ее разработчикам права администратора на данном устройстве. Кроме того, мобильное устройство начинает идти по рекламным ссылкам, что дает разработчикам вируса основную прибыль.

Исследователи установили, что один только HummingBad показывает до 20 000 000 рекламных объявлений в день, а коэффициент кликов составляет порядка 12,5%, то есть примерно 2 500 000 кликов в день. Кроме того, HummingBad ежедневно устанавливает порядка 50 000 приложений ничего не подозревающим пользователям.

Так как чудесная программка замечена на 85 млн устройств, компания Yingmob зарабатывает около $3000 в день на кликах и порядка $7000 на установке приложений. За месяц HummingBad приносит своим операторам $300 000, а за год может довести прибыль предприимчивых товарищей из Поднебесной $3 600 000.

Более того, все 85 млн зараженных объектов находятся под угрозой, так как

приложения Yingmob получают root-доступ к устройствам и в теории имеют полный контроль над системой

YiSpecter для iOS является очень похожим решением. В 2015 году специалисты компании Palo Alto Networks сумели связать данную программу с Yingmob, так как вредонос был подписан сертификатом компании. Теперь исследователи Check Point установили, что YiSpecter работает с теми же управляющими серверами, что и HummingBad. Еще одним доказательством связи двух вредоносов послужил тот факт, что код HummingBad имеет общую документацию с QVOD - порноплеером, через который распространяется YiSpecter.

Для мониторинга и анализа инфекции HummingBad китайская фирма использует сервис Umeng. По информации Check Point, данные из Umeng показывают, что в августе 2015 года Yingmob использовала для распространения HummingBad почти 200 различных приложений.

85 000 000 зараженных устройств - это не шутка. Если руководство Yingmob решит изменить схему монетизации, доступ к этим устройствам может быть продан третьим сторонам, включая, к примеру, правительственные агентства или киберпреступников.

Представители компании Yingmob пока не комментируют ситуацию.

Автор: Алина Саратова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2535 06.07.2016, 16:42
12
URL: https://babr24.com/?ADE=270727 Bytes: 4884 / 4681 Версия для печати Скачать PDF

Автор текста: **Алина Саратова**.

Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта