Социальные сети в роли C&C-сервера

Автор: Administrator
22.03.2016 00:00 - Обновлено 25.03.2016 19:42

Исследователи безопасности нашли метод обхода проверки кода при скачивании вредоносных приложений в App Store и Google Play. Как оказалось, в роли C&C-сервера возможно использовать профиль в социальной сети.

Описание принципа

В процессе загрузки на известных магазинах приложений от Android и Apple в автоматическом режиме производится проверка, к какому именно серверу обращается программа. Если ПО посылает запросы на подозрительный сервис, то приложение подвергается дополнительной проверке. Как оказалось, злоумышленники способны обойти подобные ограничения безопасности и вставить вредоносный код при помощи другого источника, к примеру, приложений социальных сетей.

Исследователи создавали профили на Facebook и размещали на стенах вирусные коды. После этого специалисты написали приложение, которое обращается к странице Facebook для скачивания этого кода. Программа проходила проверку в Google Play и App Store.

При запуске пользователю нужно было идентифицироваться при помощи профиля на Фейсбуке, после этого приложение начинало загрузку и выполняло вредоносные действия с профиля исследователей.

Как защититься

Уберечься от таких способов произведения атак непросто – поверхностная проверка кода в этом случае ничего не даст. Злоумышленники используют такие же способы вставки вредоносных кодов в приложения.

Результаты исследования были представлены в ходе конференции по информационной безопасности RSA в начале марта этого года. Конференция проходила в США в городе Сан-Франциско. Будем надеяться, что специалисты и эксперты главных гигантов в сфере создания ОС для гаджетов разберутся с данной проблемой и найдут выход и пути пресечения таких действий. В противном случае, безопасность находится под настоящей угрозой. А пользователи не могут быть уверены в том, что их гаджет не используется для вставки вредоносных кодов.