Киберворы никак не уймутся

На сегодняшний день каждый из нас уже усвоил, что преступления в интернете – не только одна из самых обширных областей для злоумышленников, но и самая развивающаяся. Периодические исследования аналитических компаний демонстрируют неуклонный рост все новых форм киберпреступности, увеличение преступлений в социальных сетях и атак, направленных на мобильные устройства.

Например, недавно эксперты «Лаборатории Касперского» обнаружили две новые вредоносные программы для Android: вместе они способны красть файлы cookie, сохраненные в браузере на смартфонах и в приложениях популярных социальных сетей, в частности Facebook. В дальнейшем зловреды позволяют злоумышленникам незаметно получать контроль над аккаунтом жертвы в социальной сети и распространять контент от ее лица.

Файлы cookie – это небольшие фрагменты данных, которые используются веб-сайтами для хранения информации на устройствах пользователя и делают серфинг в сети удобнее (например, с их помощью сайты запоминают, что человек вошел в аккаунт, и не требуют каждый раз вводить пароль). Хотя они воспринимаются как нечто безвредное, на самом деле, попав не в те руки, могут представлять угрозу безопасности. Когда веб-сайты запоминают пользователя, они сохраняют в файлах cookie уникальный ID сеанса, который в дальнейшем позволяет идентифицировать человека. Получив такой ID, злоумышленники могут обмануть веб-сайты: представиться жертвой и взять под контроль ее учетную запись. Именно для этого они разработали двух троянцев с похожим стилем написания кода и использующих один и тот же управляющий сервер.

Первый троянец, попав на устройство, получает root-права (они дают доступ к данным любых приложений на смартфоне) и передает на сервер злоумышленников cookie-файлы браузера и установленного приложения социальной сети.

Однако зачастую иметь только ID сессии недостаточно, чтобы взять под контроль чужой аккаунт. У некоторых веб-сайтов предусмотрены меры безопасности, которые позволяют предотвратить подозрительные попытки входа в систему. Например, когда пользователь, ранее активный в Чикаго, пытается авторизоваться с Бали всего через несколько минут после предыдущего сеанса. Именно для таких случаев предназначен второй троянец. Это вредоносное ПО может запустить прокси-сервер на телефоне и предоставить злоумышленникам доступ в интернет с устройства жертвы, чтобы обойти меры безопасности и таким образом войти в аккаунт, не вызывая подозрений.

При этом можно утверждать, что троянцы не эксплуатируют какие-либо уязвимости в мобильном браузере или приложении Facebook. Используя подобный метод, злоумышленники могут красть файлы cookie, сохраненные на любом сайте.

Хотя конечная цель кражи файлов cookie остается неизвестной, страница, обнаруженная на том же командном сервере, дает подсказку: на ней рекламировались услуги по распространению спама в социальных сетях и мессенджерах. То есть злоумышленники могут пытаться получить доступ к чужим учетным записям, чтобы запускать масштабные спам- и фишинговые рассылки и атаки.

«Объединив два типа атак, злоумышленники нашли способ получать контроль над аккаунтами пользователей, не вызывая подозрений. Относительно новой угрозе пока подверглись не более тысячи человек. Это число растет и скорее всего будет продолжать расти, учитывая, что веб-сайтам трудно обнаруживать такие атаки. Злоумышленники все время изобретают новые способы нажиться на пользователях, поэтому не стоит пренебрегать защитой своего устройства», – комментирует Игорь Головин, вирусный аналитик «Лаборатории Касперского».

Чтобы не стать жертвой мобильных троянцев и других угроз, эксперты рекомендуют придерживаться простых правил безопасности:

• не скачивать приложения из сторонних источников;

• регулярно обновлять устройство и сканировать систему на предмет заражения;

• использовать надежное мобильное защитное решение, которое умеет распознавать различные виды угроз.