АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Фейковые приложения для торговли криптовалютами из Google Play попались на краже данных

23 октября 2017 года

Пользователи популярной криптовалютной биржи Poloniex стали целью новой мошеннической кампании в Google Play. Под видом легитимного софта биржи в магазине распространялись два приложения для кражи данных. Фейки позволяют перехватывать логины и пароли от учетной записи в Poloniex, а также от аккаунта в Gmail.

Poloniex — это одна из ведущих бирж с возможностью торговать более чем 100 криптовалютами. Популярность площадки привлекает всевозможных мошенников. В данном инциденте злоумышленники воспользовались отсутствием у биржи официального мобильного приложения.

На фоне хайпа вокруг криптовалют мошенники тестируют разные методы – от скрытого использования вычислительной мощности пользовательских машин для добычи криптовалют в браузере и заражения непропатченных устройств до фишинговых схем.

Вредоносные приложения

Первое вредоносное приложение проникло в Google Play под названием POLONIEX от разработчика Poloniex. С 28 августа по 19 сентября его установили до 5000 пользователей, несмотря на противоречивые оценки и негативные отзывы.

Второе приложение POLONIEX EXCHANGE от POLONIEX COMPANY появилось в Google Play 15 октября и было установлено 500 раз. После предупреждения ESET подделку удалили из магазина.

Помимо Google, мы сообщили о мошенниках в Poloniex.

Рисунок 1. Фейковые приложения в Google Play

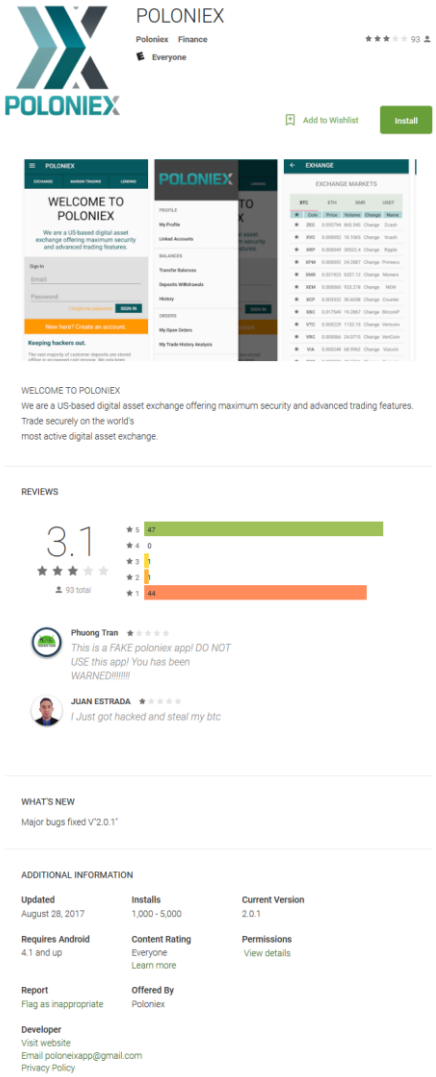

Рисунок 2. Отзывы об одном из приложений

Принципы работы

Для успешного захвата аккаунта на бирже Poloniex с помощью вредоносного приложения атакующим сначала нужно получить учетные данные. Далее – доступ к почтовому аккаунту,

связанному со скомпрометированной учетной записью на бирже для управления уведомлениями о входах в систему и транзакциях. Наконец, атакующим нужно сделать так, чтобы фейковое приложение выглядело убедительно и не вызывало подозрений.

Оба приложения используют одни и те же методы для решения этих задач.

Кража учетных данных производится сразу после запуска приложения. На экран выводится фальшивая форма ввода учетных данных Poloniex (рисунок 3). Если пользователь введет логин и пароль и нажмет на кнопку Sign In, данные будут отправлены злоумышленникам.

Если пользователь не использует двухфакторную аутентификацию в Poloniex, атакующие получают доступ к аккаунту. Они смогут выполнять транзакции самостоятельно, менять настройки и запретить доступ пользователя к учетной записи, сменив пароль.

Если пользователь все же использует двухфакторную аутентификацию, его аккаунт защищен от взлома. Poloniex обеспечивает 2FA через Google Authenticator. Случайные пароли для входа в аккаунт отправляются через текстовые сообщения, голосовую связь или приложение Google Authenticator, к которым у злоумышленников нет доступа.

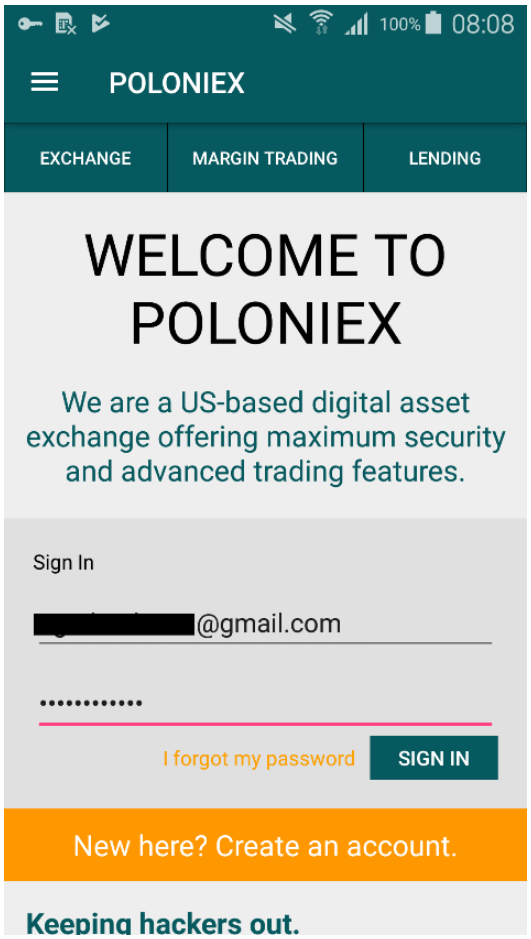

Рисунок 3. Фальшивая форма ввода для кражи учетных данных Poloniex

Перехватив логин и пароль от Poloniex, злоумышленники пытаются получить доступ к аккаунту Gmail. Пользователь видит активность, на первый взгляд, со стороны Google, в процессе которой от него требуют войти в аккаунт Gmail для «двухступенчатой проверки безопасности» (рисунок 4). Когда пользователь нажмет на кнопку входа, вредоносное приложение запросит разрешение на просмотр сообщений электронной почты, настроек и базовой информации профиля (рисунок 5).

Если пользователь дает эти разрешения, приложение получает доступ к входящим письмам.

Получив доступ к аккаунту Poloniex и связанному аккаунту Gmail, атакующие могут проводить транзакции от лица пользователей и удалять любые уведомления о неавторизованном входе и транзакциях из входящих писем.

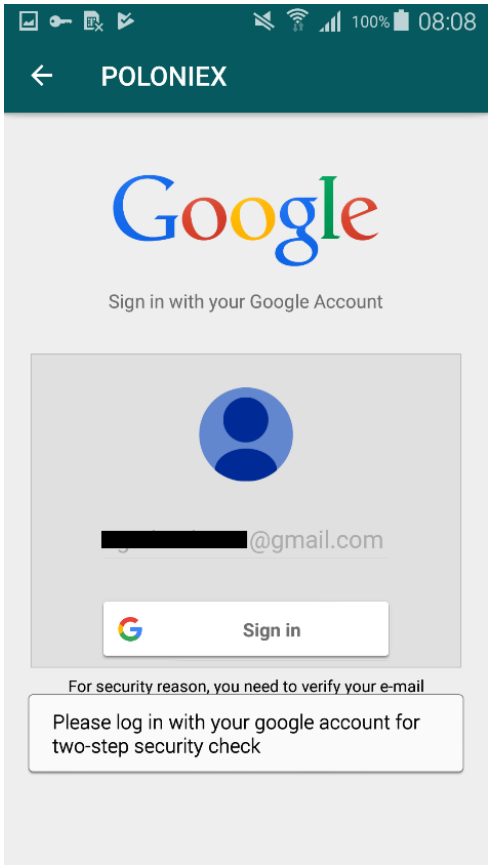

Рисунок 4. Запрос входа в аккаунт Gmail

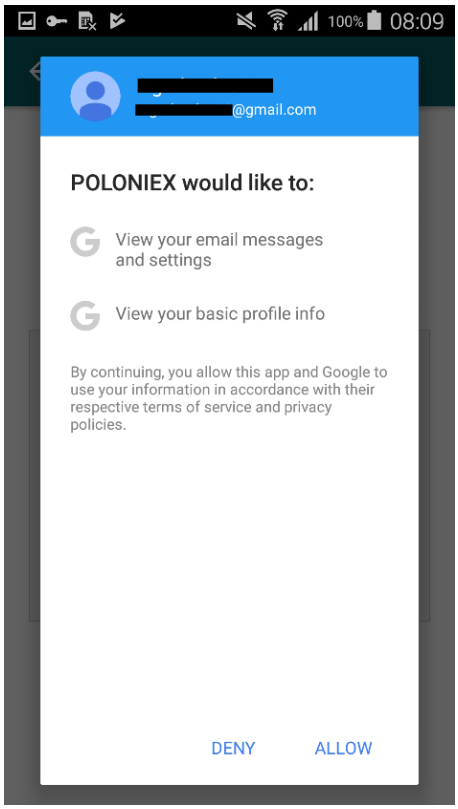

Рисунок 5. Вредоносное приложение, запрашивающее доступ к почте

Наконец, чтобы обеспечить видимость нормальной работы, приложение переадресовывает пользователя на мобильную версию легитимного сайта Poloniex. Сайт требует от пользователя авторизоваться (рисунок 6). После входа в систему пользователь может начать работу с биржей Poloniex. Приложение будет открывать легитимный сайт при каждом запуске.

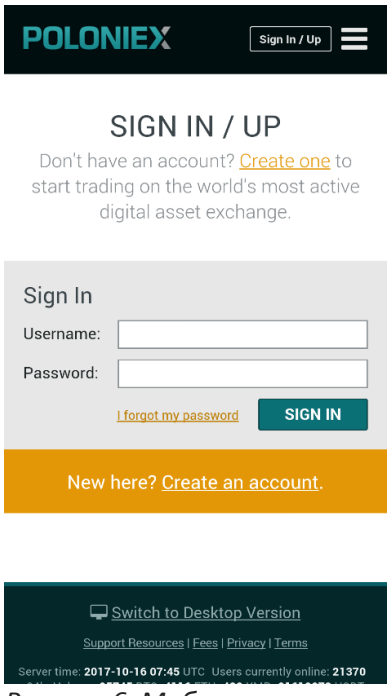

Рисунок 6. Мобильная версия легитимного сайта Poloniex, открываемого вредоносным приложением

Как обезопасить себя?

Если вы пользователь Poloniex и установили вышеперечисленные приложения, удалите их. Обязательно смените пароли к аккаунтам Poloniex и Gmail, по возможности включите двухфакторную аутентификацию.

На всякий случай перечислим здесь классические рекомендации по профилактике заражения:

- убедиться, что у сервиса действительно есть свое мобильное приложение (со ссылкой на него с официального сайта)
- проверять рейтинг приложения и отзывы пользователей
- обращать внимание на уведомления и окна, связанные с Google, которые появляются при работе со сторонними приложениями (мошенники нередко пользуются доверием пользователей к «корпорации добра»)
- использовать двухфакторную аутентификацию в качестве дополнительного (и часто ключевого) уровня безопасности
- использовать надежное решение для безопасности мобильных устройств

Антивирусные продукты ESET детектируют фейковые приложения как Android/FakeApp.GV.

Индикаторы компрометации

Имя пакета	Хеш
com.poloniex.exchange	89BE9AF09BB3B2CAD9EAF88FE0EF175E5F150044
com.poloniexap.poloniex	427CBAFD6E28C50708E26A481A9C8665C3315BCD