АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

DoubleLocker: первый шифратор, использующий службу специальных возможностей Android Accessibility Service

13 октября 2017 года

Специалисты ESET обнаружили Android/DoubleLocker – первый шифратор, использующий службу специальных возможностей Android Accessibility Service. Малварь не только шифрует данные, но и блокирует устройство.

DoubleLocker построен на базе банковского трояна, использующего службу специальных возможностей ОС Android. Тем не менее, DoubleLocker не имеет функций, связанных со сбором банковских данных пользователей и стирания аккаунтов, вместо этого в нем предусмотрены инструменты для вымогательства.

DoubleLocker может изменить PIN-код устройства, блокируя доступ жертвы, а также шифрует найденные данные – мы впервые наблюдаем такое сочетание функций в экосистеме Android. С учетом происхождения от банковской малвари, DoubleLocker может быть превращен в то, что мы называем банкеры-вымогатели. Вредоносная программа действует в два этапа – пытается удалить банковский или PayPal аккаунт, а затем блокирует устройство и данные, чтобы запросить выкуп. Мы обнаружили тестовую версию такого банкера-вымогателя in-the-wild еще в мае 2017 года.

Распространение

DoubleLocker распространяется очень простым способом, как и его предок-банкер – преимущественно под видом фейкового Adobe Flash Player через скомпрометированные сайты.

После запуска приложение предлагает активировать вредоносную службу специальных возможностей под названием Google Play Service. Получив необходимые разрешения, малварь использует их для активации прав администратора устройства и устанавливает себя как лаунчер по умолчанию – все без согласия пользователя.

Самоустановка в качестве лаунчера по умолчанию повышает персистентность вредоносного ПО. Всякий раз, когда пользователь нажимает кнопку «Домой», вымогатель активируется и устройство снова блокируется.

Блокировка устройства и шифрование данных

После выполнения на устройстве DoubleLocker использует два веских аргумента, чтобы вынудить пользователя оплатить выкуп.

Во-первых, он изменяет PIN-код планшета или смартфона, что препятствует использованию устройства. В качестве нового PIN задается случайное значение, код не хранится на устройстве и не отправляется куда-либо вовне, поэтому пользователь или специалист по безопасности не сможет его восстановить. Зато после получения выкупа злоумышленник может удаленно сбросить PIN и разблокировать устройство.

Во-вторых, DoubleLocker шифрует все файлы в основном хранилище устройства. Он использует алгоритм шифрования AES и добавляет расширение *.cryeye*.

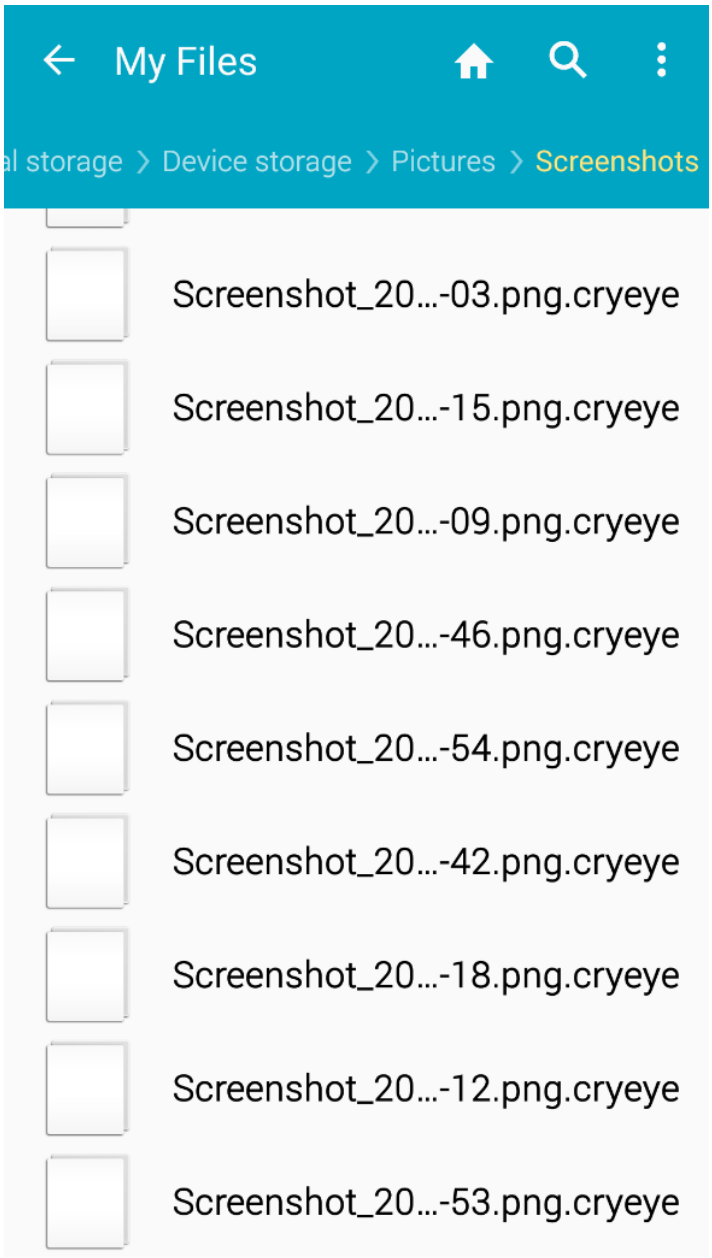

Рисунок 1. Зашифрованные файлы на девайсе, зараженном DoubleLocker

Сумма выкупа составляет 0,0130 биткоина (около 4000 рублей), в сообщении подчеркивается, что оплата должна быть произведена в течение 24 часов. Если выкуп не перечислить, данные останутся зашифрованными, но удалены не будут.

Рисунок 2. Требование выкупа DoubleLocker

Как избавиться от DoubleLocker?

В сообщении о выкупе пользователя предупреждают о последствиях удаления или блокировки DoubleLocker: «Без программного обеспечения вы никогда не сможете вернуть исходные файлы». Чтобы предотвратить нежелательное удаление «программного обеспечения», мошенники даже рекомендуют отключать антивирусное ПО — довольно бессмысленно, поскольку при наличии качественного решения для безопасности устройство защищено от малвари.

Чтобы избавиться от DoubleLocker, рекомендуем принять следующие меры:

- Нерутованное устройство, на котором не установлено решение для управления мобильным устройством, способное сбросить PIN-код: единственный способ избавиться от экрана блокировки – сброс до заводских настроек.

- Рутованное устройство: пользователь может подключиться к устройству через ADB и удалить файл, в котором хранится PIN-код. Для этого необходимо включить отладку устройства (Настройки – Параметры разработчика – Отладка USB). Экран блокировки будет удален, и пользователь вернет доступ к устройству. Затем, работая в безопасном режиме, пользователь сможет деактивировать права администратора устройства для малвари и удалить ее. В некоторых случаях требуется перезагрузка устройства.

Для профилактики рекомендуем защитить Android-устройства качественными продуктами для безопасности и регулярно делать резервные копии.

Продукты ESET детектируют новую вредоносную программу как Android/DoubleLocker.