Анатомия вымогателей для Android

Вымогатели (ransomware) представляют из себя особый тип вредоносных программ для мобильных устройств, количество которых постоянно растет. Вымогатели можно разделить на две большие группы: первые специализируются на блокировании экрана устройства пользователя (lock-screen ransomware), а вторые шифруют на нем данные (crypto-ransomware). За несколько лет своей деятельности оба этих типа уже привели к значительным финансовым потерям пользователей, а также потерям их личных данных.

Подобно другим типам вредоносного ПО для Android, таким как, например, SMS-трояны, вымогатели существенно эволюционировали в течение последних нескольких лет, при этом VX-авторы адаптировали многие вредоносные техники, доказавшие свою эффективность в аналогичных вредоносных программах, для настольных систем.

Общие сведения

Вымогатели как для Windows, так и для Android используют тему «полицейского вымогания» (police ransomware) в качестве темы для экрана блокировки. Данная тема является вполне эффективной, так как злоумышленники используют чувство вины пользователя, обвиняя его в просмотре или хранении нелегального контента на устройстве. Схожие черты мобильные вымогатели имеют и с печально известным семейством таких вредоносных программ для Windows как Cryptolocker, например, они используют стойкие криптографические алгоритмы при шифровании файлов таким образом, чтобы у пользователя не было пути восстановления доступа к зашифрованным файлам. Поскольку пользователь хранит на смартфоне значительно большее количество личных данных, угроза потери значительного количества данных пользователя существенно возрастает.

Одно из интересных наблюдений, которое нам удалось сделать, заключается в изменении географической ориентации злоумышленников со стран Восточной Европы на прочие страны. Например, подавляющее большинство жертв вымогателей семейств Android/Simplocker и Android/Lockerpin располагаются в США.

Оба вышеупомянутых типа вымогателей были очень распространенной проблемой для пользователей Windows начиная с 2013 г., когда популярность этих вредоносных программ у киберпреступников стала существенно повышаться, несмотря на то, что они были распространены и гораздо раньше. Заражение вымогателями приносило серьезные неприятности как для простых пользователей, так и для корпоративных.

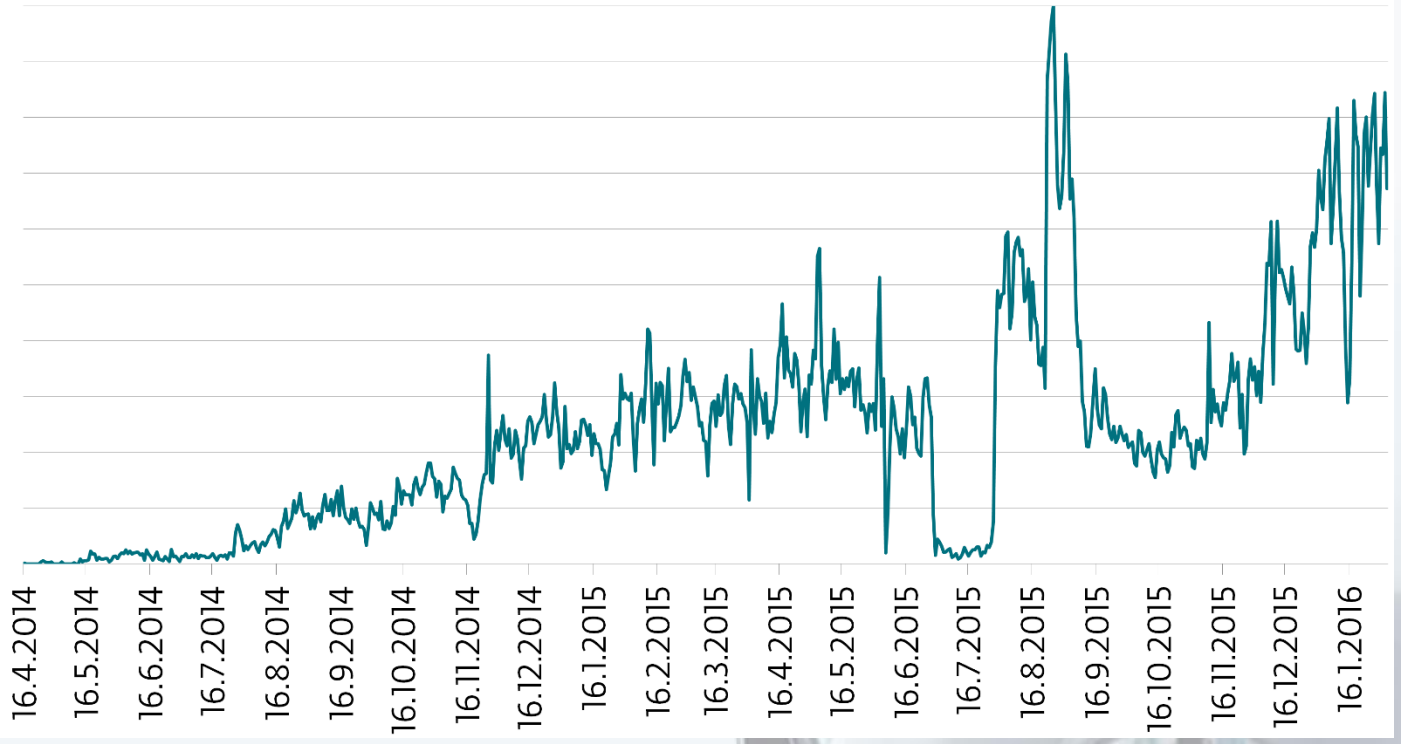


Рис. Статистика обнаружений вымогателей для Android по данным ESET LiveGrid.

Использование злоумышленниками вымогателей именно для Android не является случайностью. Поскольку количество смартфонов на этой ОС растет из года в год, пользователи все чаще выбирают именно их для хранения личных и ценных данных. Соответственно, такой бизнес принесет им максимальное количество выгоды.

Возможные векторы заражения

Злоумышленники используют для вымогателей Android такую же маскировку, как и для других вредоносных программ, которая заключается в том, что пользователя убеждают в легитимности приложения. Различные популярные приложения, такие как игры, а также связанные с порнографией приложения, часто выбираются в качестве прикрытия и для увеличения вероятности компрометации потенциальной жертвы. В некоторых случаях, вредоносные APK-файлы снабжены значком и названием легитимного приложения. Другой сценарий предполагает прямое использование злоумышленниками легитимного приложения, в которое вставляется вредоносный код, при этом исходные функции приложения сохраняются. Поведение вредоносной программы может быть и незаметным для пользователя устройства, это происходит в том случае, когда авторы не полагаются на механизм блокировки экрана или шифрования файлов, как в случае с бэкдорами или SMS-троянами. Нужно отметить, что такое изменение легитимного приложения приведет к его нарушению целостности и несоответствию указанных в цифровой подписи данных.

Нужно отметить, что ни один из описываемых нами вымогателей не был обнаружен в магазине приложений Google Play. Однако, существуют случаи успешного обхода вредоносными программами постоянно улучшаемых мер безопасности Google для магазина Play. Наши аналитики обнаруживали и отправляли в Google сотни примеров вредоносного ПО для Android, включая, такое вредоносное ПО как Fake AV, шпионское ПО с функциями кражи учетных данных, трояны для кликфрода, бэкдоры, потенциально нежелательные приложения (PUA) с показом рекламы, прочие PUA-приложения и другие. Вирусописатели также применяют специальные методы заражения устройства таким образом, чтобы отложить срабатывание фактической полезной нагрузки путем использования загрузчиков (даунлоадеров), а также дропперов. С другой стороны, использование таких продвинутых техник как автоматическая установка вредоносного ПО drive-by download не является распространенным в Android.

Взаимодействие с управляющим C&C-сервером

После успешной установки в системе, большинство вредоносных программ для Android сообщают об этом «домой», т. е. на удаленный C&C-сервер. Как правило, это отправленное сообщение включает в себя некоторую основную информацию об устройстве, такую как, модель устройства, номер IMEI, используемый язык и т. д. В случае установки постоянного подключения между C&C-сервером и ботом, злоумышленник может отправлять ему команды для исполнения. Таким образом, злоумышленник может контролировать ботнет из устройств под управлением Android.

Некоторые примеры удаленных команд, которые поддерживают вымогатели для Android, приведены ниже:

- открыть нужный URL-адрес в веб-браузере;
- отправить SMS-сообщение всем контактам;
- заблокировать или разблокировать устройство;
- отправить злоумышленникам SMS-сообщения с устройства;
- отправить злоумышленникам информацию о контактах жертвы;
- выбрать нужный текст сообщения с требованием выкупа;
- обновиться до новой версии;
- разрешить или запретить хранение данных на устройстве;
- разрешить или запретить подключение Wi-Fi;
- отслеживать географическое расположение пользователя с использованием GPS.

Обычно для связи бота с удаленным сервером используется протокол HTTP, но в некоторых случаях мы также наблюдали использование для взаимодействия с C&C такого публичного сервиса как Google Cloud Messaging. Этот сервис позволяет приложениям под управлением Android на смартфонах обмениваться данными. Для вредоносных целей также используется сервис Baidu Cloud Push. Некоторые образцы вредоносных программ, которые мы анализировали, использовали анонимный сервис Tor (домены .onion) и протокол XMPP (jabber). Трояны для Android могут получать команды и посылать удаленно данные с использованием SMS-сообщений.

Методы самозащиты

Задача заражения устройства пользователя под управлением Android вредоносной программой не является тривиальной задачей для злоумышленников. Даже для пользователей без установленного антивирусного решения, такого как ESET Mobile Security, существуют механизмы защиты от вредоносного ПО самой ОС. После обхода защитных механизмов злоумышленниками, они заинтересованы в том, чтобы вредоносная программа оставалась там как можно дольше.

Мы наблюдали использование вредоносными программами для Android различных механизмов самозащиты, которые препятствовали нарушению их деятельности или удалению из системы. Например, вымогатель Android/Lockerpin мог внештатно завершать процессы антивирусных решений. Одним из самых универсальных методов, который мы наблюдаем в использовании вирусописателями, причем все больше и больше, является получение привилегий администратора устройства (Device Administrator). Несмотря на то, что такой режим работы не является настолько опасным как получение прав root, он все равно предоставляет злоумышленникам расширенные полномочия будучи полученным на устройстве.

Рис. Примеры вредоносного ПО для Android, которое запрашивает права администратора в системе.

Легитимные приложения с привилегиями администратора устройства используют такие расширенные полномочия в ОС для различных целей, которые, как правило, связаны с безопасностью. Вредоносные приложения, напротив, используют их для своей самозащиты от удаления из системы. Перед удалением такого приложения из Android, его права Администратора должны быть отозваны. Некоторые вредоносные программы, такие как Android/Lockerpin, используют полученные привилегии для установки или изменения PIN-кода экрана блокировки.

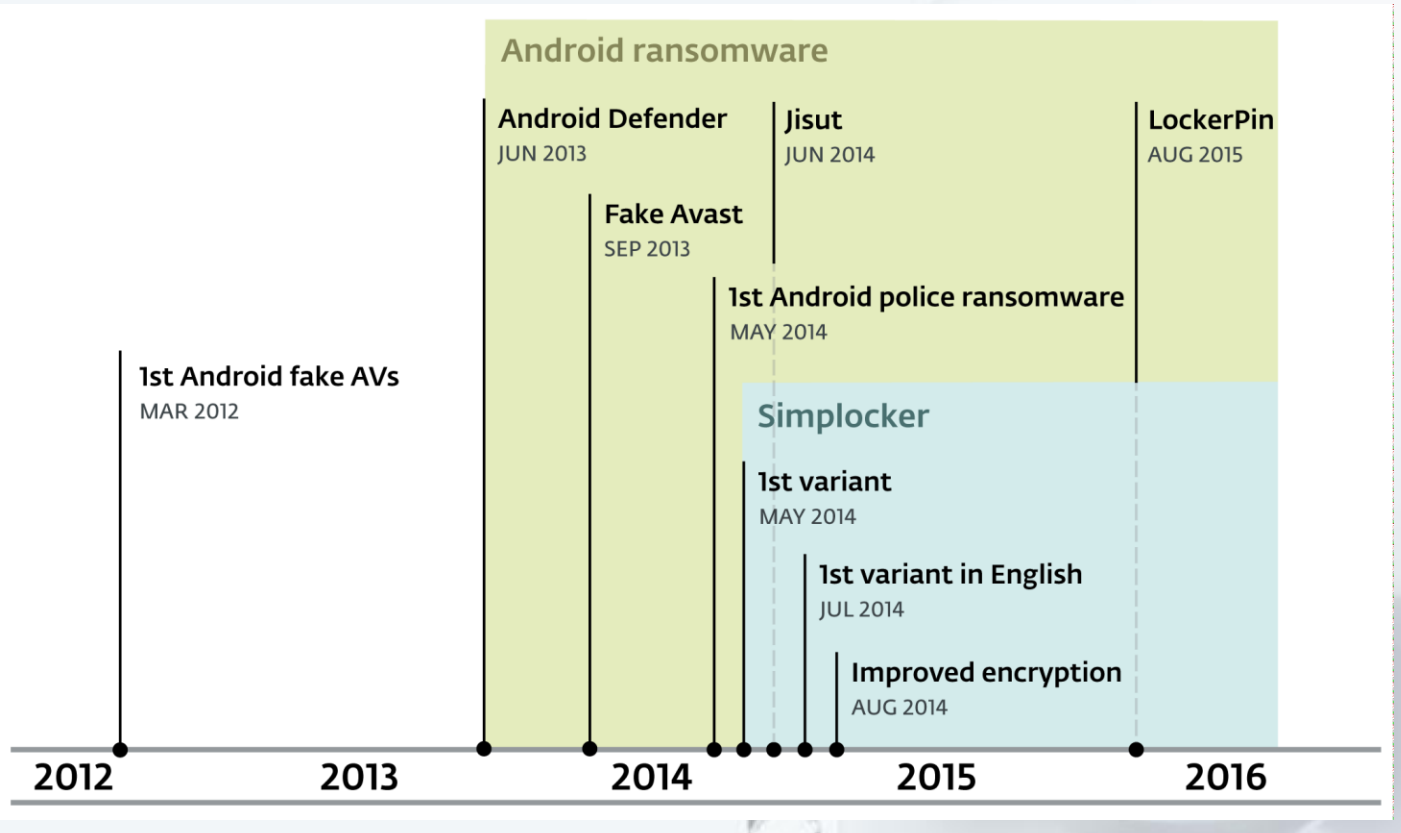


Рис. Хронология появления вымогателей для Android.

Первые случаи появления вымогателей для Android сопровождались добавлением вредоносных функций к фальшивым антивирусам. Такие поддельные антивирусы были распространены уже долго время, начиная с 2012 года для Android и с 2004 года для компьютеров. Как следует из названия, такие программы показывают пользователю фальшивые сообщения о сканировании файлов на устройстве, а затем пытаются обмануть его, показывая сообщение с требованием оплаты дальнейших действий антивируса по обезвреживанию угрозы. Эти программы также называются «scareware», поскольку они вымогают денежные средства у жертвы после ее запугивания присутствием активного заражения устройства.

Большинство вымогателей с функцией блокировки экрана устройства для Windows используют тему правоохранительных органов (police ransomware) при запугивании пользователя. Схожий метод злоумышленники начали использовать в вымогателях и для Android. Подобный вид вымогателей существенно увеличивает возможность успешного вымогания денежных средств у пользователя, поскольку к жертве обращаются от имени правоохранительных органов, при этом им сообщается, что на устройстве были обнаружены незаконные действия.

Первым вариантом вымогателя-шифровальщика для Android стало семейство вредоносных программ под названием Simplocker в мае 2014 г. Последние три года вымогатели для Android продолжают свое развитие, за это время было обнаружено несколько новых семейств этого вредоносного ПО.

Android Defender

Эта вредоносная программа была впервые обнаружена в середине 2013 г. и является примером фальшивого антивируса для Android, а также, фактически, первым вымогателем для Android. Как видно на рисунке ниже, пользовательский интерфейс вредоносного приложения пытается имитировать его законный аналог. Злоумышленники предусматривают такую функцию для убеждения пользователя в легитимности антивируса. Интересно отметить, что во время фальшивого сканирования файлов на диске, троян отображает названия действительно присутствующих на карте памяти файлов, что делает этот процесс еще более правдоподобным в глазах пользователя. Названия семейств вредоносных программ также указаны существующие, однако,

никакого отношения к устройству пользователя они не имеют.

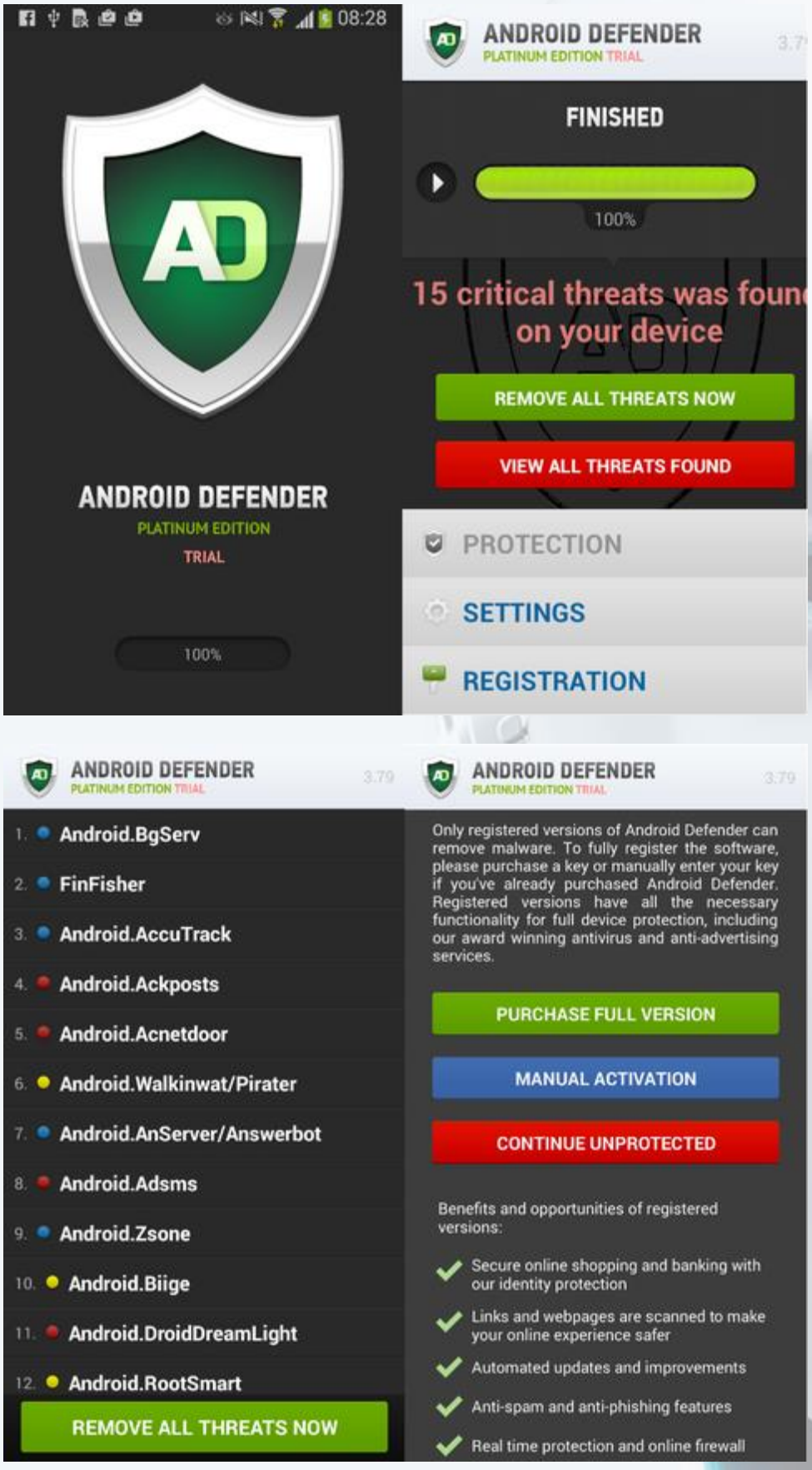


Рис. Внешний вид фальшивого антивируса Android Defender (Fake AV).

На данном этапе пользователь по-прежнему имеет доступ к настройке под названием «continuing unprotected», а также может закрыть приложение. Однако, запущенный вспомогательный сервис ОС, который принадлежит

фальшивому антивирусу, делает смартфон практически непригодным для использования, постоянно отображая специальные окна с предупреждениями каждый раз, когда пользователь пытается запустить приложение. Выбрав настройку «Stay unprotected», пользователь всего лишь избавит себя от текущего всплывающего окна, при этом сразу же получив новое.

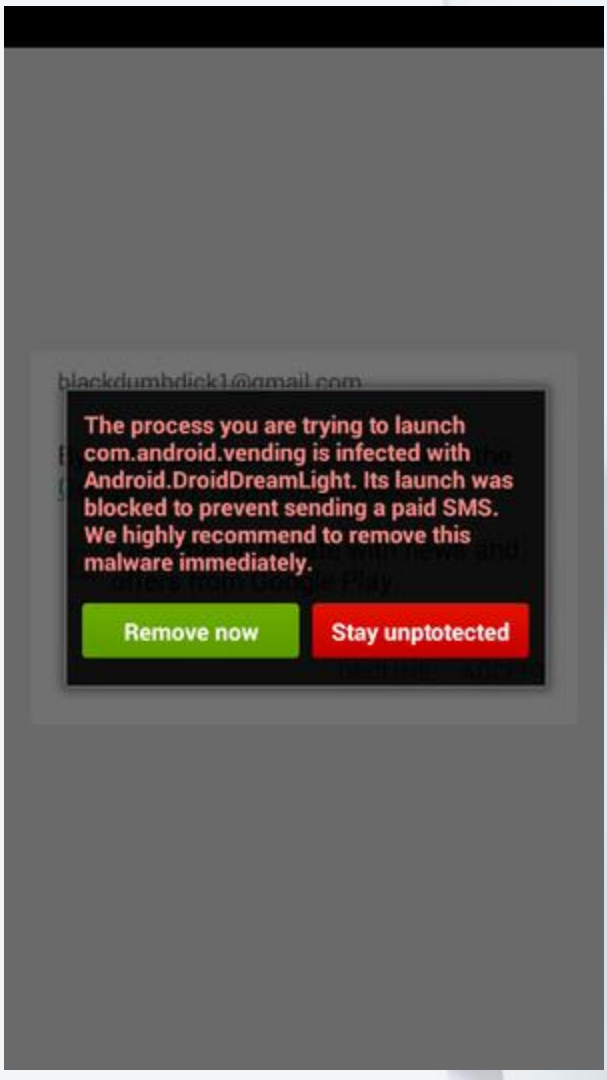


Рис. Закрепленное вредоносной программой сообщение лишает пользователя возможности нормальной работы с устройством.

В том случае, если владелец смартфона поддается на уловку злоумышленников и решает заплатить требуемую сумму для перехода на «полную версию антивируса», его разочарования на этом не заканчиваются. Спустя шесть часов после своего запуска в системе, вредоносная программа отобразит на весь экран устройства окно с порнографическими картинками, которое не может быть закрыто.

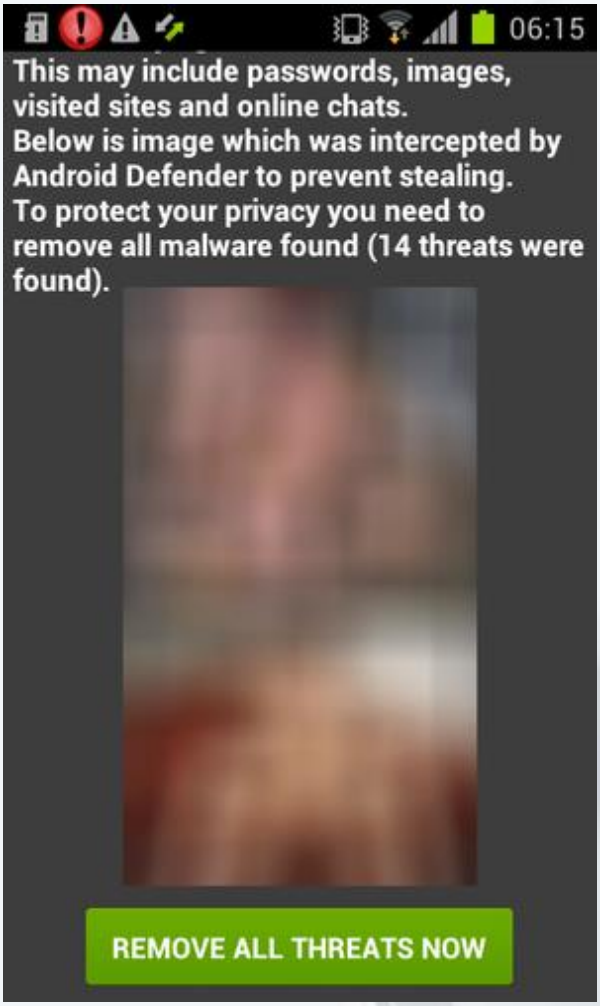


Рис. Экран блокировки Android Defender с порно-картинкой.

При оплате, владелец смартфона также оставляет злоумышленникам данные своей кредитной карты, которая может быть использована для проведения мошеннических транзакций. Как указано на скриншоте, мошенники предлагают пользователю скидку, снижая сумму до $89,99.

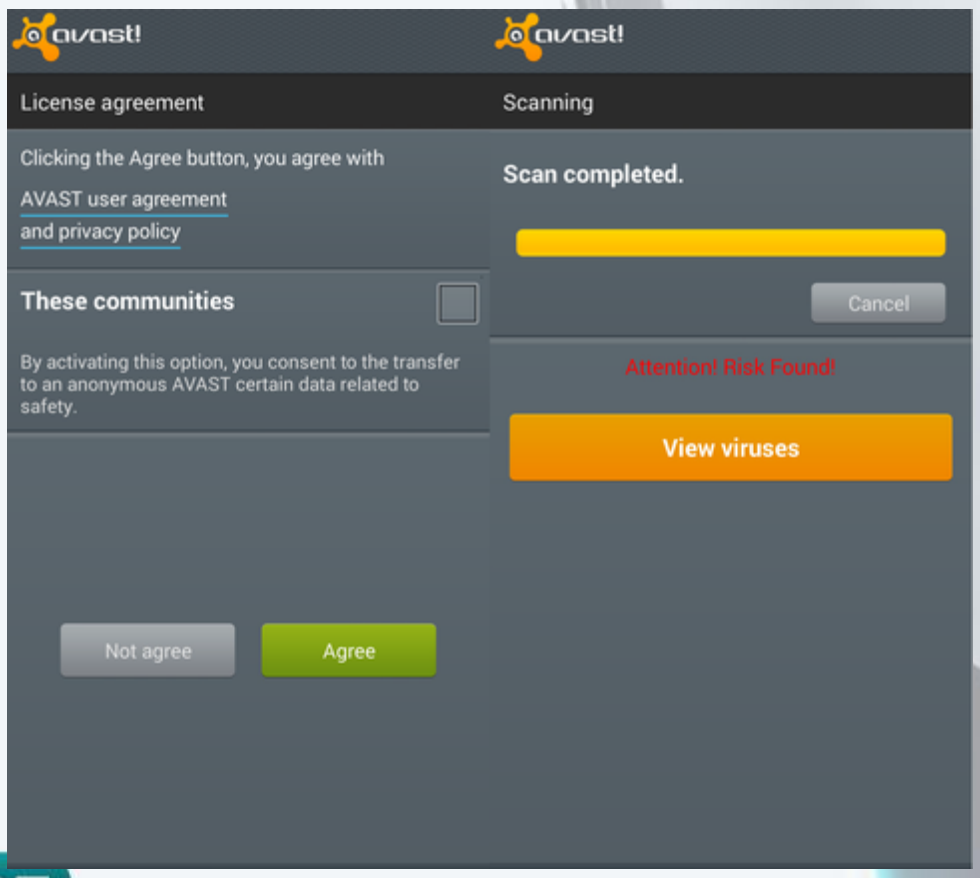
Антивирусный продукт ESET Mobile Security обнаруживает Android Defender как Android/FakeAV.B.

Вымогатель с функциями фальшивого антивируса и порно

Еще один тип вымогателя в виде поддельного антивируса копирует интерфейс не продукта Android Defender, а название легитимного приложения безопасности от Avast. Речь идет о вредоносной программе, которая обнаруживается антивирусными продуктами ESET как Android/FakeAV.E. Она использует бренд известного ресурса PornHub, чтобы найти свою аудиторию среди посетителей этого ресурса.

Рис. Вымогатель маскируется под приложение для просмотра порно.

После запуска приложения, пользователь вместо просмотра порнографических роликов получает сообщение, что его устройство нужно проверить на вирусы. После нажатия на кнопку OK, фальшивый антивирус, который внешне похож на Avast, запускает псевдо-сканирование.



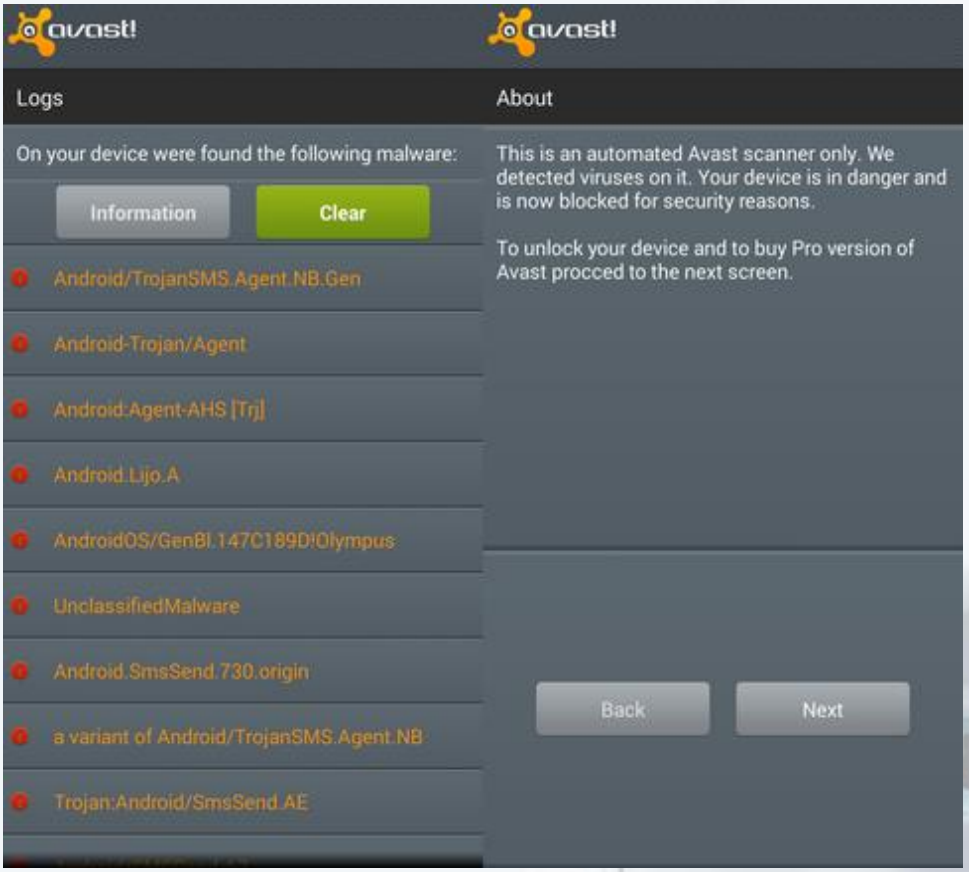


Рис. Вымогатель Android/FakeAV.E маскируется под фальшивое антивирусное приложение Avast.

Информация, которую мошенники выводят пользователю, является довольно странной. Во-первых, само показываемое сообщение говорит о том, что «устройство находится в опасности и было заблокировано по соображениям безопасности». Далее, предлагается приобрести расширенную версию псевдо-защитного ПО. Подобное поведение выдает пользователю истинные намерения полученного им ПО, так как блокирование устройства явно не соответствует функциям легитимного антивируса. Отображаемый для пользователя экран с сообщением требует от него выплату штрафа в размере $100, чтобы избежать возможных правовых последствий.

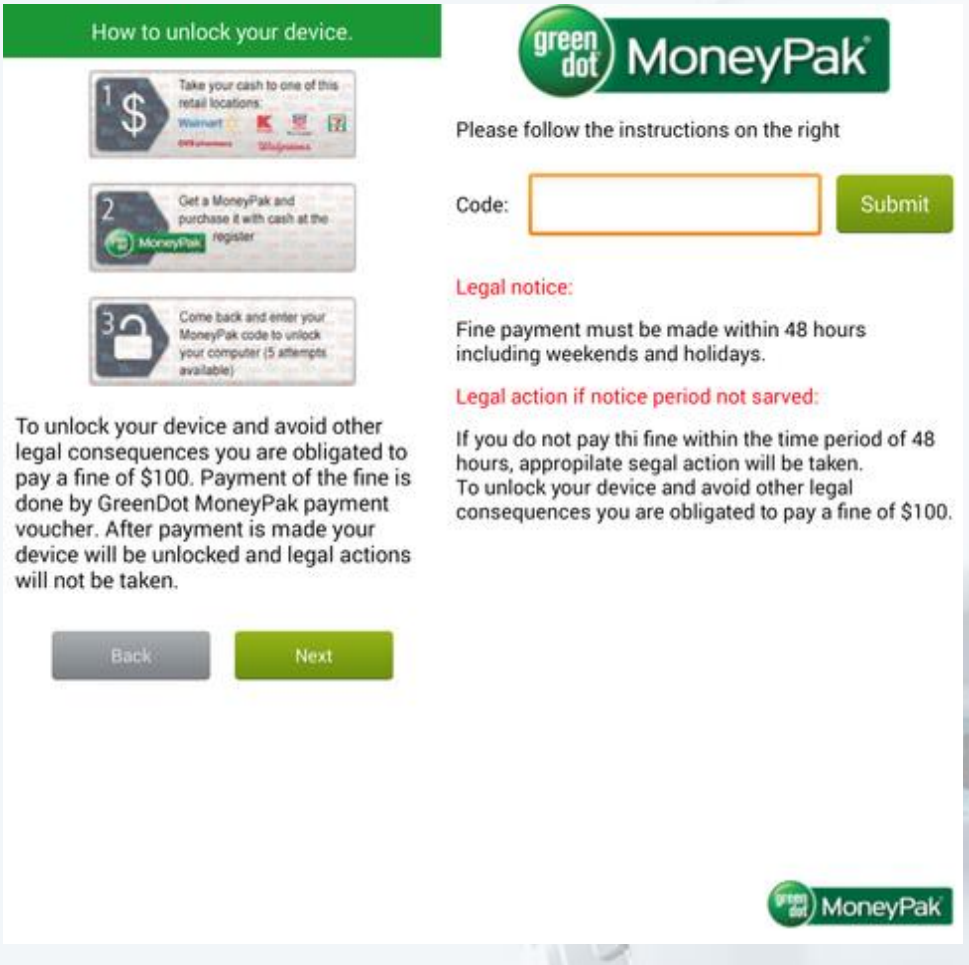


Рис. Оплата выкупа для Android/FakeAV.E.

У нас сложилось впечатление, что авторы этого вымогателя скопировали текст сообщение с требованием выкупа у другой вредоносной программы, так как в тексте встречаются те же грамматические ошибки.

Полицейские вымогатели

Вымогатели для Windows использовали различные темы для демонстрации в качестве экрана блокировки. Некоторые более ранние образцы использовали тему синего экрана смерти (BSOD) или сообщение об активации Windows. Мы обнаруживали различные темы, которые злоумышленники использовали для экрана блокировки, однако, наиболее распространенным из них была тема правоохранительных органов (полиции).

Такие полицейские вымогатели утверждали, что устройство было заблокировано местными правоохранительными органами, так как на нем было обнаружен незаконное содержимое, либо с устройства осуществлялась противоправная деятельность. В качестве текста для экрана блокировки использовался, иногда, брались статьи из уголовного кодекса. Текст также утверждал, что при оплате соответствующей суммы, пользователь освобождается от ответственности. Этот тип вымогателей часто использует геолокацию на основе IP-адреса, чтобы выбрать нужный баннер со значком правоохранительных органов нужного государства.

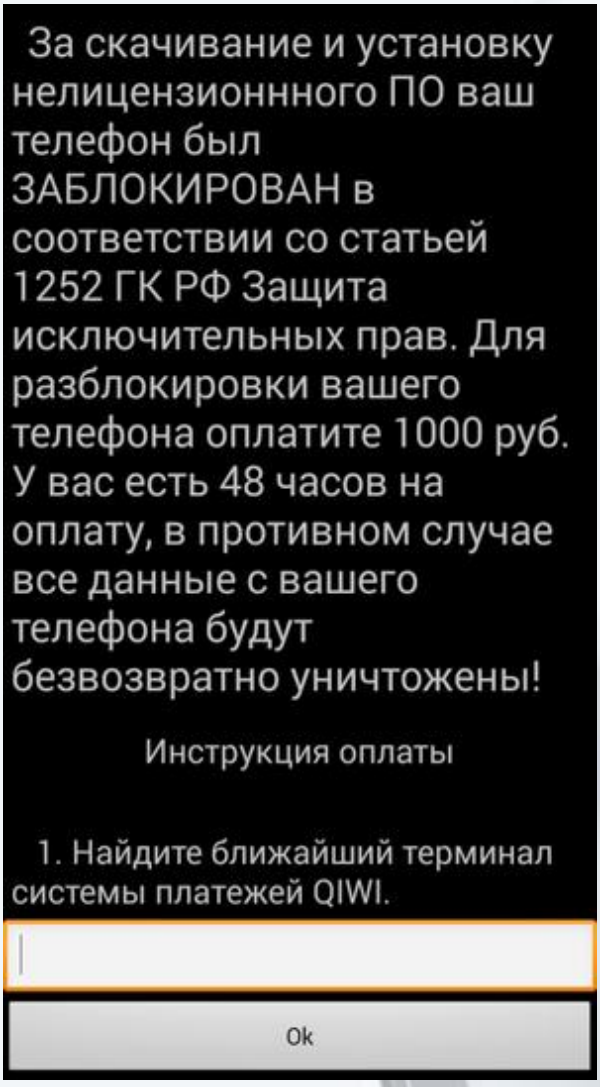


Рис. Первый полицейский вымогатель был нацелен на русскоговорящих пользователей Android.

Первые экземпляры полицейских вымогателей для Android появились в первой половине 2014 г. и были направлены против русскоговорящих пользователей. Вскоре после этого, были обнаружены варианты и на английском языке.

Рис. Вымогатель Android/Locker использует снимки камеры и геолокацию для запугивания пользователя, на примерах указаны экраны блокировок для России, Украины, Казахстана.

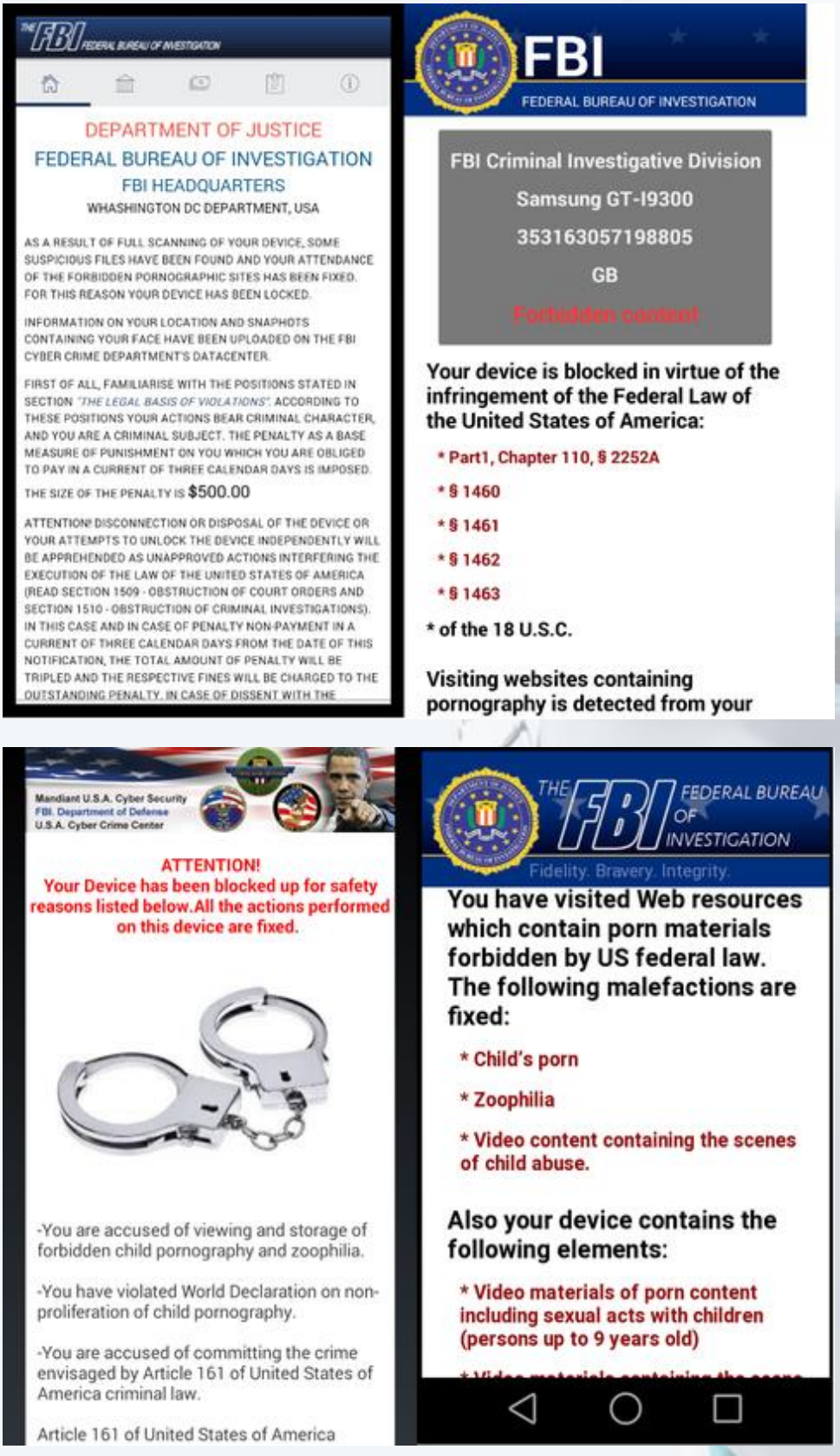


Рис. Вымогатель Android/Koler переключился на компрометацию англоязычных пользователей.

Антивирусные продукты ESET обнаруживают экземпляры вышеприведенных вымогателей как Android/Koler и Android/Locker.

Simplocker

В мае 2014 г., специалисты ESET обнаружили первый вымогатель с функцией шифрования файлов для Android.

Аналогичное вредоносное ПО для Windows ранее уже получило достаточно широкую распространенность и успешно использовалось злоумышленниками для вымогания значительных сумм с их жертв. Среди ярких представителей можно выделить такие семейства как Cryptolocker, Cryptowall, CTB-Locker, Torrentlocker.

После своего запуска на устройстве, вымогатель отображает пользователю сообщение с требованием выкупа, как это показано на рисунке ниже. Шифрование файлов осуществляется Simplocker в отдельном программном потоке. Вредоносная программа Android/Simplocker.A осуществляет поиск на SD-карте определенных типов файлов, таких как изображения, документы, видео со следующими расширениями: JPEG, JPG, PNG, BMP, GIF, PDF, DOC, DOCX, TXT, AVI, MKV, 3GP, MP4. Файлы шифруются с использованием симметричного шифра AES. Сам ключ шифрования был жестко зашит в тело вымогателя, при чем находился там в открытой форме. Таким образом, не составляло большого труда расшифровать файлы и получить к ним доступ. По этой причине, мы назвали семейство этих вымогателей именно Simplocker (простой блокировщик). Мы также полагаем, что из-за простоты его реализации, это был либо proof-of-concept (PoC) угрозы, либо ранняя версия ее более сложного аналога.

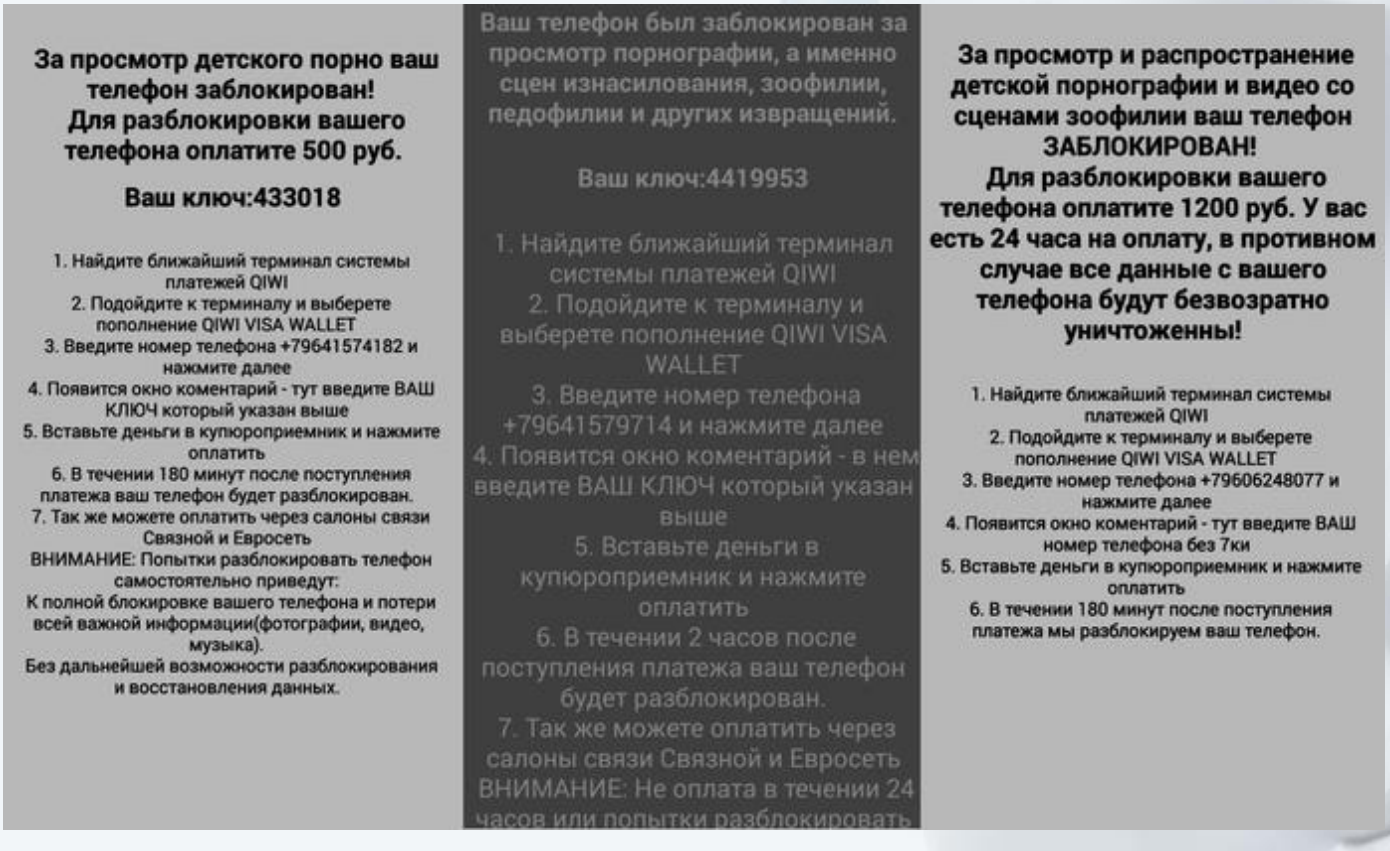


Рис. Сообщения с требованием выкупа Android/Simplocker первых версий.

Рис. Для запугивания жертвы вымогатель использует снимки фронтальной камеры устройства.

Текст сообщения вымогателя был написан на русском языке, а оплата требовалась в рублях или в украинских гривнах, что свидетельствует об ориентации злоумышленников на пользователей в Украине. Сообщение также указывало жертве каким образом следовало оплатить выкуп. В качестве платежных систем указывались MoneXy или QIWI, так как в этом случае получателя выполненного платежа не так просто отследить, как, если бы, он был выполнен с использованием кредитной карты.

Некоторые модификации Simplocker также отображали в сообщении с требованием выкупа фото жертвы, которые было захвачено путем доступа к камере устройства. Такой метод использовался злоумышленниками для усиления негативного воздействия на жертву.

Векторы распространения Simplocker

Киберпреступники, которые зарабатывали на Simplocker, использовали для его распространения эффективную схему маскировки вредоносного приложения в легитимное или известное. Как правило, маскировка выполнялась под приложение, которое имело отношение к порно, это могло быть приложение для его просмотра или сам порно-ролик. В другом случае приложение маскировалось под игры, например, Grand Theft Auto: San Andreas или под такие общие приложения как проигрыватель Flash Player.

Распространение Simplocker осуществлялось и с помощью менее известного способа, такого как загрузчик или даунлоадер (downloader). Использование загрузчиков очень распространено в мире вредоносного ПО для Windows, однако, для Android, такой метод не пользовался популярностью у злоумышленников. Загрузчик

является очень компактным по размеру и используется злоумышленниками для загрузки на скомпрометированное устройство нужного им содержимого (вредоносной программы).

Использование загрузчиков для распространения вредоносного ПО дает злоумышленникам некоторые преимущества для сокрытия вредоносной активности от глаз проверяющих, в частности, от программы проверки программ на легитимность со стороны инструмента Bouncer, работающего в Google Play. Это достигается следующими свойствами загрузчиков.

- Приложение специализируется на выполнении только одной функции - открытии URL-адреса. Само по себе, такое действие не может квалифицироваться как вредоносное.
- Загрузчик не требует специальных прав (permissions) для работы в Android, как это делают «потенциально опасные приложения». Поэтому тот пользователь, который контролирует запрашиваемые приложением права в процессе установки, не сможет узнать его истинные функции.

Кроме этого, злоумышленники используют еще один специальный трюк для того, чтобы скрыть истинные функции загрузчика, приведенный выше URL-адрес не указывает напрямую на APK-файл. Вместо этого, ссылка ведет на промежуточный сервер, а оттуда перенаправляется на загрузку файла.

Мы не наблюдали распространение злоумышленниками вымогателя Simplocker через магазин приложений Google Play.

Simplocker на английском

Спустя месяц после обнаружения первых вариантов Simplocker, мы начали обнаруживать новые версии этого вымогателя, которые содержали несколько значительных улучшений. Одним из наиболее заметных стало изменение языка текста сообщения для вывода на экране блокировки. Для этих целей был выбран английский язык.

Для мотивации оплаты выкупа пользователем, была выбрана тема блокирования устройства со стороны ФБР (FBI) за осуществления противоправных действий: использование пиратского ПО, просмотра детской порнографии, и др. Сумма выкупа в новой версии составляла от 200 до 500 долларов, а в качестве средства оплаты была выбрана платежная система MoneyPak. Как и в предыдущей версии Simplocker, новая модификация также использовала снимки камеры пользователя для его запугивания. Данная модификация обнаруживается нашими антивирусными продуктами как Android/Simplocker.I.

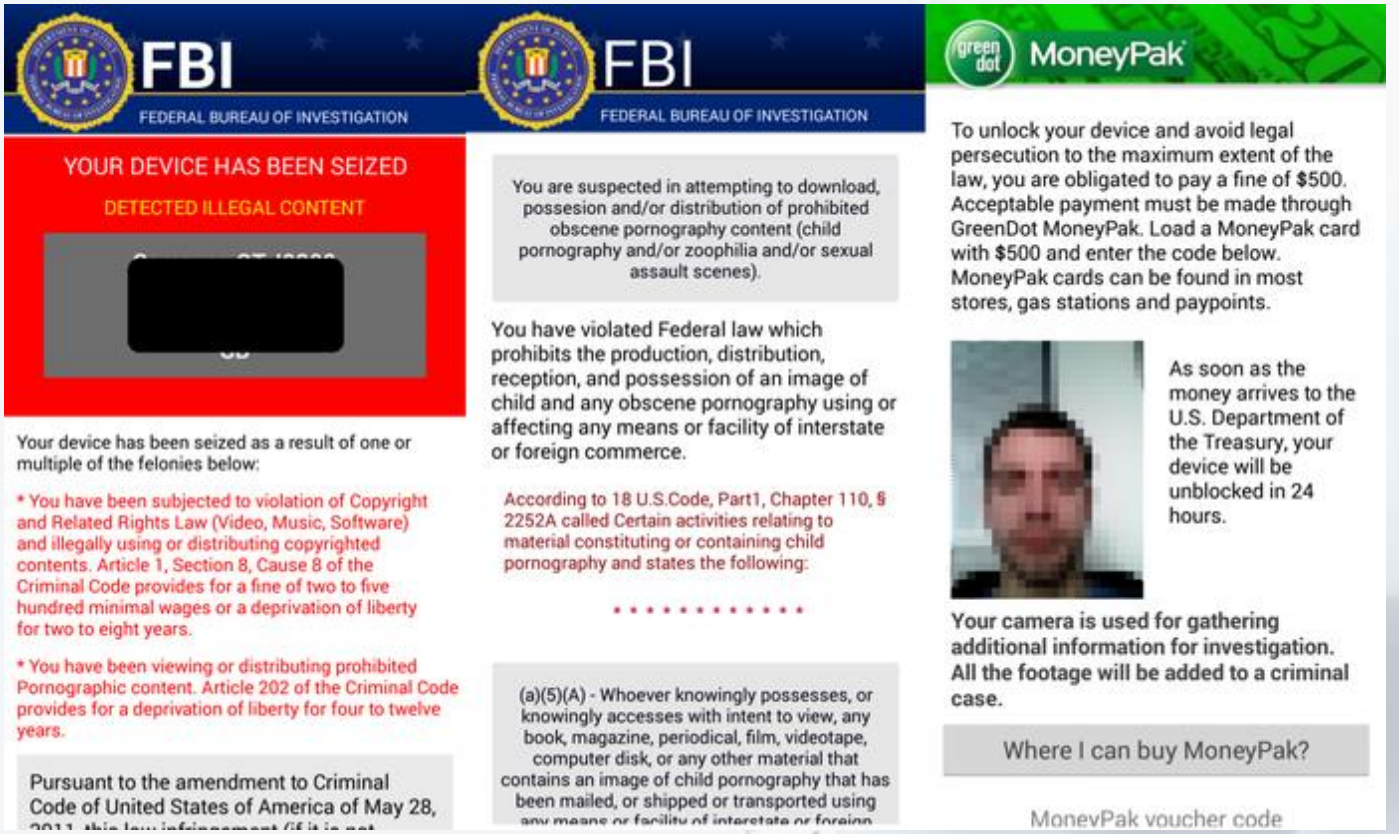


Рис. Сообщения с требованием выкупа Android/Simplocker последующих версий на английском.

Последние варианты вымогателя также содержали некоторые изменения. Вместо ФБР была выбрана служба АНБ (NSA), которая обвиняла жертву в посещении "запрещенных порнографических сайтов" и требовала 500 долларов в качестве выкупа.

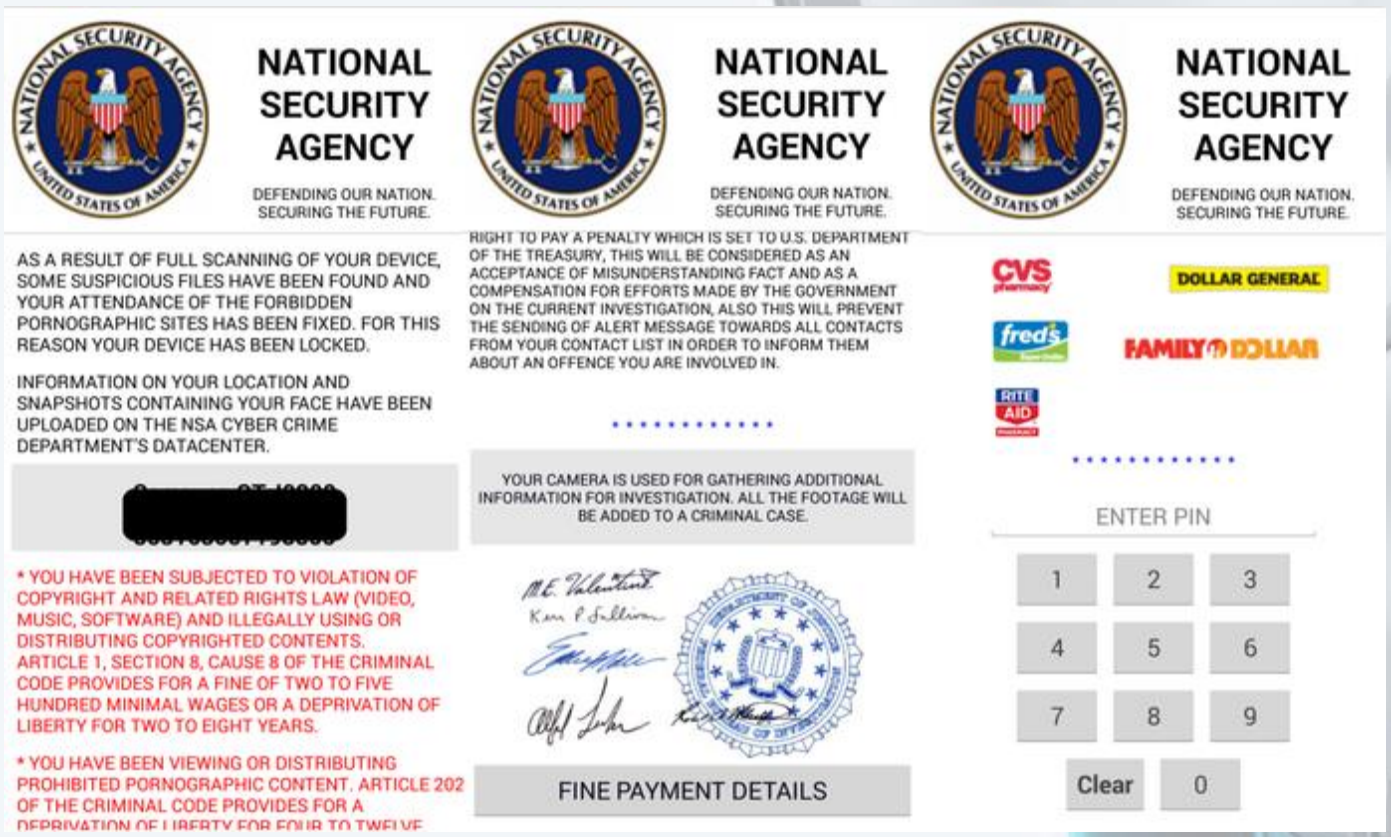


Рис. Сообщения с требованием выкупа Android/Simplocker от АНБ.

В дополнение к списку файлов, которые подвергаются шифрованию, для этого были включены различные архивы: ZIP, 7z, RAR. Это "обновление" вымогателя стало весьма неприятным для пользователей, поскольку лишает их доступа к архивам с содержимым резервных данных устройства, которые хранятся в формате таких архивов. После потери доступа к таким файлам, пользователь уже не сможет восстановить свои данные оттуда.

Более продвинутые варианты Simplocker, запрашивают у пользователя режим администратора устройства для своей установки, что делает их дальнейшее удаление сложной задачей. Перед удалением вымогателя, пользователю будет нужно отозвать у него расширенные права. Эта операция является трудно осуществимой, поскольку экран устройства заблокирован.

Другим примечательным изменением в новой версии вымогателя стал переход злоумышленников на протокол Jabber XMPP (Extensible Messaging and Presence Protocol) для взаимодействия со своим управляющим C&C-сервером. Данный протокол помогает киберпреступникам существенно усложнить процесс отслеживания передачи трафика между вымогателем и удаленным сервером. Вымогатель Android/Simplocker использует его для отправки информации о зараженном устройстве на C&C-сервер и получения команд для исполнения. Некоторые модификации этого вымогателя также использовали .onion домены анонимной сети Tor для той же цели.

Наиболее важным шагом в процессе эволюции Simplocker стал переход злоумышленников на новый механизм хранения ключей шифрования, которые используются для шифрования файлов. Через несколько месяцев после появления первых версий, мы обнаружили новые модификации вредоносной программы, использующие уникальные ключи шифрования, которые Simplocker получал с удаленного сервера. Этот шаг ознаменовал собой переход авторов от этапа тестирования вымогателя на получение от него реальной прибыли, поскольку в таком случае расшифровка файлов становится практически невозможной.

Lockerpin

В предыдущих версиях вымогателей для Android, возможность блокировки экрана, как правило, реализовывалась путем постоянной прорисовки окна с сообщением о выкупе в бесконечном цикле. Таким образом, пользователь лишался возможности работать с устройством. Обратно получить контроль над устройством было возможно с использованием интерфейса Android Debug Bridge (ADB) или отключением режима администратора с последующим удалением вредоносного приложения в безопасном режиме (Safe Mode).

В случае с Android/Lockerpin, вирусописатели прибегли к новому изощренному приему блокировки устройства путем смены его PIN-кода. Для выполнения этого приема, вымогатель должен получить права администратора устройства при своей установке. После смены PIN-кода у пользователя остается мало шансов, чтобы восстановить доступ к устройству. Он может получить к нему доступ, если для устройства ранее использовалась операция рутинга (root), либо на устройстве установлен инструмент MDM. Еще одним методом возвращения контроля над устройством остается его заводской сброс (factory reset), который уничтожит на нем все данные.

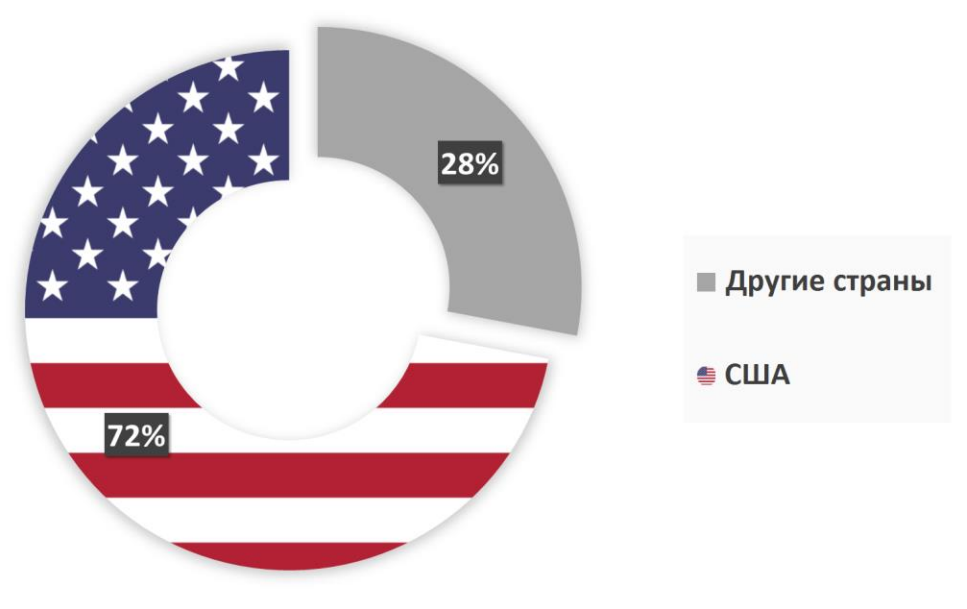


Рис. География распространения Android/Lockerpin.

Согласно статистике ESET LiveGrid, наибольшее количество заражений устройств приходится на США и составляет 72% от общего количества заражений. Такое распределение заражений Lockerpin по странам является тенденцией, согласно которой злоумышленники переходят от заражения пользователей в России и Украине на США, где они могут получить больше прибыли. Злоумышленники маскируют Lockerpin под приложение для просмотра порно.

Более ранние версии семейства Android/Locker получали права администратора устройства аналогично многим другим троянам для Android, которые используют этот механизм в качестве защиты от удаления из ОС. При этом они полагаются на пользователя, соглашающегося поднять привилегии приложения до такого уровня при его установке.

Последние версии вымогателя содержат хитрый прием получения прав администратора устройства. Lockerpin показывает пользователю специальное окно с просьбой установить «обновление», которое перекрывает системное окно Android с просьбой подтвердить предоставление расширенных прав приложению. Окно вымогателя оформлено таким образом, что кнопка «Continue» точно совпадает с кнопкой «Activate» системного окна. Таким образом, пользователь не инициирует установку обновления, а подтверждает предоставление расширенных прав на устройстве вредоносному приложению.

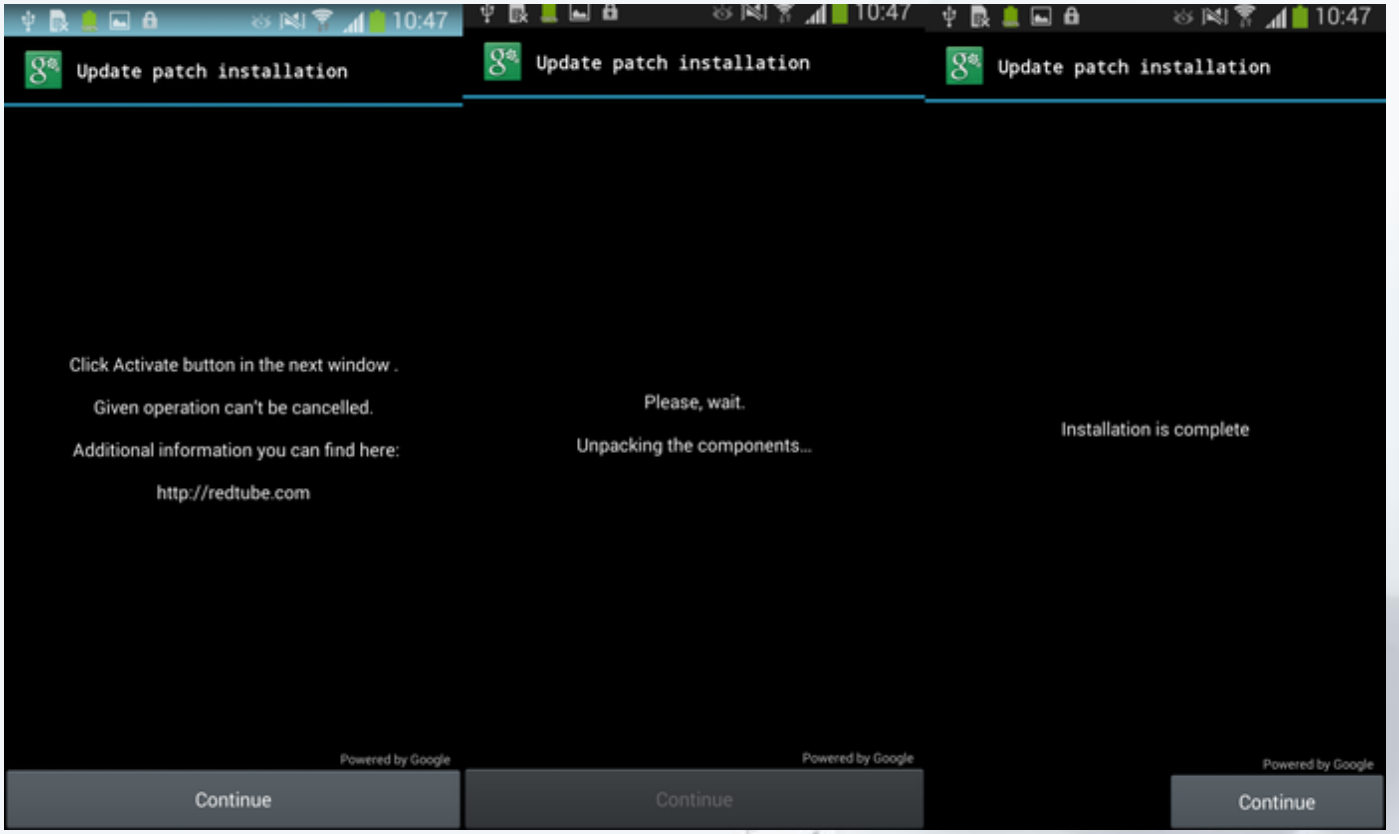


Рис. Демонстрация используемого Android/Lockerpin приема по обману пользователя для подтверждения получения прав администратора.

После успешной установки в систему, Android/Lockerpin действует как полицейский вымогатель. Пользователю отображается сообщение от «правоохранительных органов» с требованием выкупа размером $500 за просмотр и хранение запрещенных порнографических материалов.

Рис. Сообщение с требованием выкупа от Android/Lockerpin.

Рис. Экран блокировки вымогателя Android/Lockerpin на скомпрометированном устройстве.

По истечению определенного таймаута, который следует за отображением текста вымогателя пользователю, вредоносная программа меняет PIN-код или устанавливает его в случае отсутствия. Этот PIN-код представляет из себя произвольно сгенерированное четырехзначное значение, которое не отсылается на сервер злоумышленникам. Некоторые модификации Lockerpin снабжены функцией сброса установленного PIN-кода.

Механизмы самозащиты Lockerpin

Кроме получения расширенных прав администратора устройства в системе, Android/Lockerpin также использует агрессивные методы самозащиты для поддержания своего присутствия в системе. Для этого вымогатель регистрирует функцию обратного вызова (callback) для повторного получения прав администратора сразу же после попытки их удаления. При этом пользователю опять отображается фальшивое окно с запросом на установку обновления.

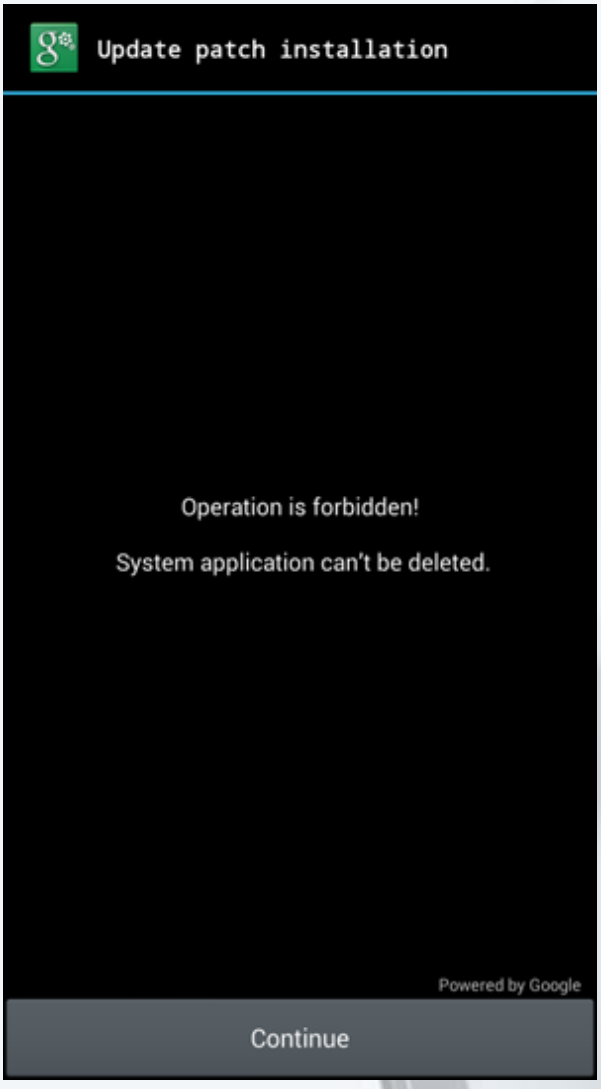


Рис. Вымогатель блокирует попытки пользователя отозвать у него права администратора.

В качестве дополнительной меры самозащиты, Lockerpin также пытается завершить все работающие процессы антивирусных программ в Android. Это происходит в том случае, когда пользователь пытается отозвать у вредоносного приложения права администратора. Lockerpin имеет функцию завершения процессов трех антивирусных программ: ESET Mobile Security, Avast и Dr.Web.

```
if(v26.get(v19).processName.contains(((CharSequence)v11))) {
    this.killProc(v26.get(v19));
    this.KickAv(v17, v26, v19);
}
```

com.eset
com.avast
com.drweb
com.android.settings

Рис. Lockerpin специализируется на убийстве запущенных процессов.

Вредоносная программа не сможет завершить процессы ESET Mobile Security или удалить его из системы, однако, она также пытается убить процесс com.android.settings в целях предотвращения удаления вредоносного приложения встроенным менеджером приложений.

JISUT

Семейство вымогателей, которое антивирусные продукты ESET обнаруживают как Android/LockScreen.Jisut, является довольно странным. В отличие от остальных вымогателей, которые были созданы для извлечения финансовой выгоды, эта модификация используется как шалость. Наибольшее распространение она получила

в Китае и, скорее всего, представляет из себя результат работы подростка из Китая.

Большинство вымогателей требуют выкуп через ту платежную систему, транзакцию в которой невозможно отследить. Злоумышленники выбирают такие системы как MoneyPak, MoneXy или Bitcoin. Тем не менее, авторы Jisut взяли на вооружение иной подход, который не предполагает анонимности. Текст экрана блокировки вымогателя содержит контактную информацию злоумышленника для китайской социальной сети QQ. Сообщение призывает пользователя связаться с злоумышленником для получения своих файлов обратно. Если информация в профилях QQ верна, то возраст злоумышленников варьируется от 16 до 21 года.

Первые варианты Android/LockScreen.Jisut начали появляться в первой половине 2014 г. С тех пор, мы обнаруживали сотни модификаций этой вредоносной программы, которые ведут себя немного иначе или отображают различный текст в экране блокировки, но все они основаны на одной кодовой базе. Все семейство вымогателей Jisut отличается от других известных вымогателей типа LockScreen.

Одна из модификаций Jisut специализируется на создании полноэкранного окна (Activity), которое перекрывает все остальные окна. При этом это окно представляет из себя черный фон, так что для пользователя это выглядит так, как будто устройство заблокировано или выключено. В случае, если пользователь вызывает меню Android для выключения или перезагрузки устройства, ему отображается сообщение в шутливой форме. Некоторые модификации вымогателя также проигрывают музыку из фильма Psycho известного кинорежиссера Альфреда Хичкока, вызывая вибрацию устройства в бесконечном цикле.

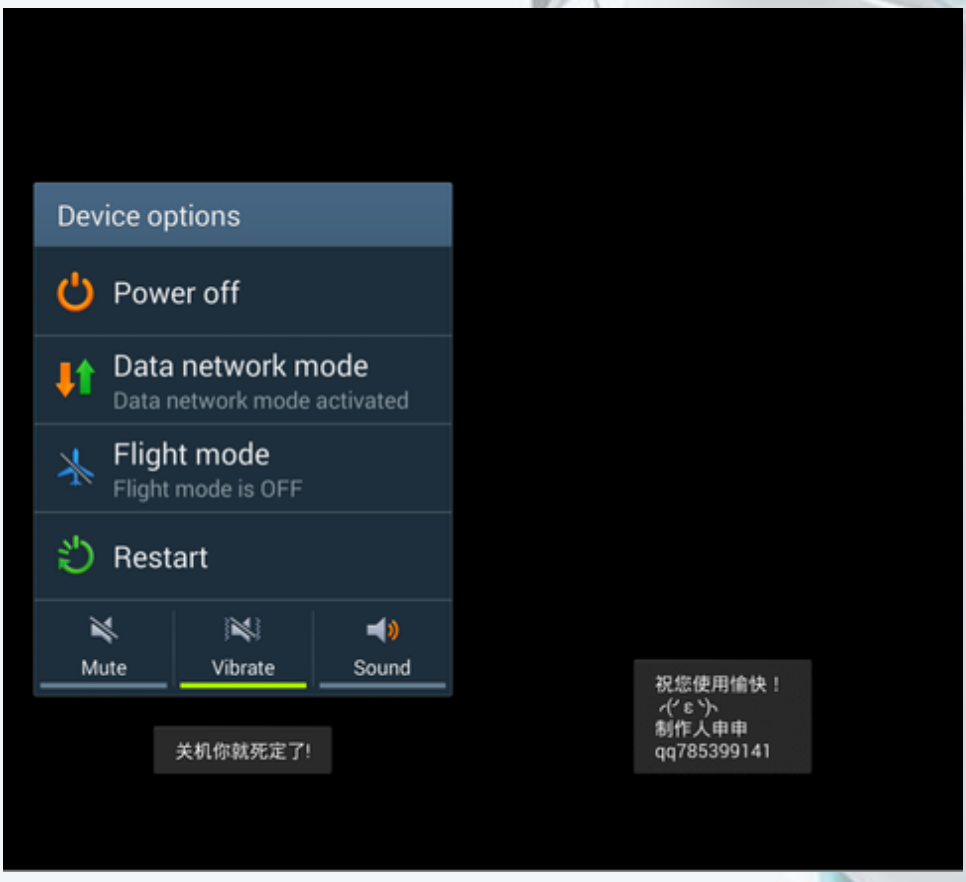


Рис. Шутливые сообщения Jisut на китайском: слева: «Выключить, ты мертв!», справа: «Я надеюсь тебе весело! Продюсер Shen Shen».

Еще одна модификация Jisut просит пользователя нажать на кнопку с надписью: «Я идиот» тысячу раз. В случае выполнения операции, вымогатель не осуществляет никаких действий, при этом сбрасывая счетчик нажатий до нуля.

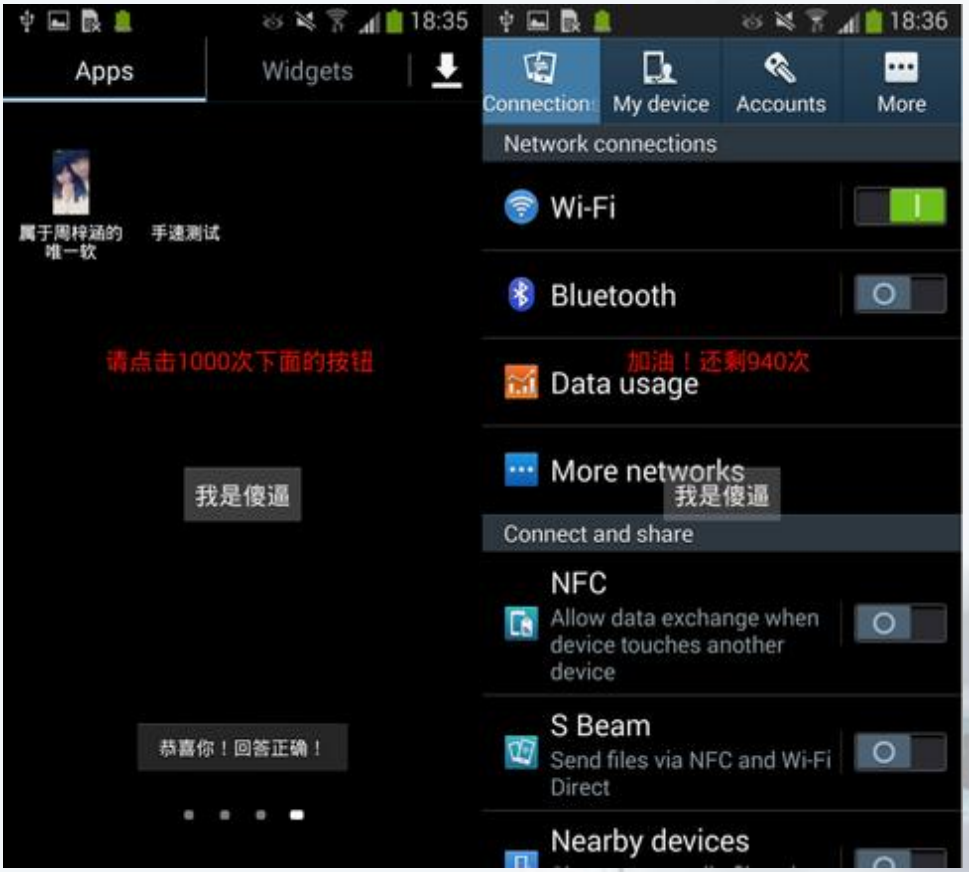


Рис. Сообщение с надписью: «Пожалуйста нажмите кнопку внизу тысячу раз».

В дополнение к упомянутому выше глупому поведению вымогателя по розыгрышу жертвы, некоторые его модификации содержат вредоносные функции. Одной из таких функций является возможность смены PIN-кода или пароля пользователя аналогично тому, как это сделано в Android/Lockerpin. Jisut может отображать пользователю и фальшивый экран блокировки, который имитирует легитимный экран блокировки. Эта последняя функция также встречалась в семействах вымогателей Android/Locker и Android/Koler.

Рис. Устройство заблокировано со сменой PIN-кода или пароля вымогателем Android/LockScreen.Jisut.

Рис. Другие примеры экрана блокировки вымогателя.

Мы наблюдали варианты Jisut, которые также специализировались на отправке SMS-сообщений с URL-ссылками в тексте контактам пользователя.

Как защитить устройство под управлением Android

Для пользователей мобильной ОС Android важно быть в курсе информации о той угрозе, которую представляют из себя вымогатели, а также о соответствующих профилактических мерах для предотвращения заражения. В целях защиты от вредоносного ПО следует избегать установки приложений из неофициальных магазинов, установить у себя на устройстве антивирусное ПО и регулярно обновлять ОС и приложения. Кроме этого, пользователю следует регулярно делать резервную копию важных данных устройства.

Соблюдающие указанные правила пользователи вряд ли столкнуться с угрозой установки вредоносных программ или потери своих данных. Даже в том случае, если по каким-либо причинам, устройство будет заблокировано вымогателем, актуальную копию зашифрованных данных можно всегда восстановить из резервной копии. Кроме этого, можно воспользоваться следующими полезными способами для борьбы с ними.

Для большинства простых семейств вымогателей, которые специализируются на блокировании экрана пользователя, загрузка устройства в безопасном режиме является простым способом удаления вредоносного приложения. Поскольку загрузка в таком режиме блокирует запуск сторонних приложений, вредоносное ПО также лишиться возможности своего запуска. Способы загрузки устройства в безопасном режиме могут отличаться в разных моделях. В случае использования вымогателем прав администратора в системе, они должны быть отозваны перед удалением вредоносного приложения.

В том случае, если вымогатель с правами администратора устройства заблокировал устройство с использованием PIN-кода Android или пароля, ситуация с его разблокировкой существенно усложняется. Разблокировать устройство в таком случае возможно с использованием менеджера устройства Google Android Device Manager или альтернативного решения MDM (Mobile Device Management). Устройства с активированной функцией root имеют в таком случае больше возможностей восстановления. В качестве крайней меры можно использовать заводской сброс устройства, который удалит на нем все данные.

При заражении вымогателем с функцией шифрования файлов, таким как Android/Simplocker, мы рекомендуем пользователю связаться с технической поддержкой поставщика, используемого им решения безопасности. В зависимости от конкретной модификации вымогателя, расшифровка файлов может быть, как возможна, так и нет.

Мы советуем пользователям не попадаться на удочку злоумышленников и не платить требуемую сумму выкупа по следующим причинам. В то время, как некоторые киберпреступные группы вышли на высокий уровень профессионализма и действительно расшифровывают файлы пользователя после оплаты выкупа, такая ситуация происходит не всегда. Например, авторы вымогателей-шифровальщиков для Android пытаются копировать многие приемы аналогичных семейств для Windows (Filecoder), причем делают это весьма плохо. Для пользователя из этого вытекает два следствия: во-первых, даже в случае оплаты выкупа, он не сможет расшифровать файлы. Во-вторых, в некоторых случаях, файлы можно будет расшифровать и без оплаты выкупа.

Некоторые варианты вымогателей для Android, которые мы анализировали, не содержали в себе код расшифровки файлов и удаления экрана блокировки, поэтому оплата выкупа в таком случае также ничем не сможет помочь.

Восприятие ситуации заражения вымогателем для одного пользователя или же корпоративной единицы сводится к вопросу доверия. Можно ли доверять киберпреступникам и действительно ли они возвратят устройство и файлы на нем в состояние, предшествующее заражению? Очевидно, что никто не может предоставить таких гарантий. Даже в том случае, если выкуп будет оплачен, а данные возвращены, не существует гарантий его повторной компрометации. Таким образом, идя на поводу у злоумышленников жертва лишь играет в предложенную киберпреступниками игру, в которую все равно проиграет.

Как уже упоминалось выше, соблюдение профилактических мер на основе базовых правил безопасности, которые заключаются в использовании обновленного антивирусного и прочего ПО на Android, а также резервное копирование данных является наилучшей мерой безопасности. Поскольку в этих правилах безопасности нет ничего сложного, мы не видим причин, по которым их можно не выполнять.