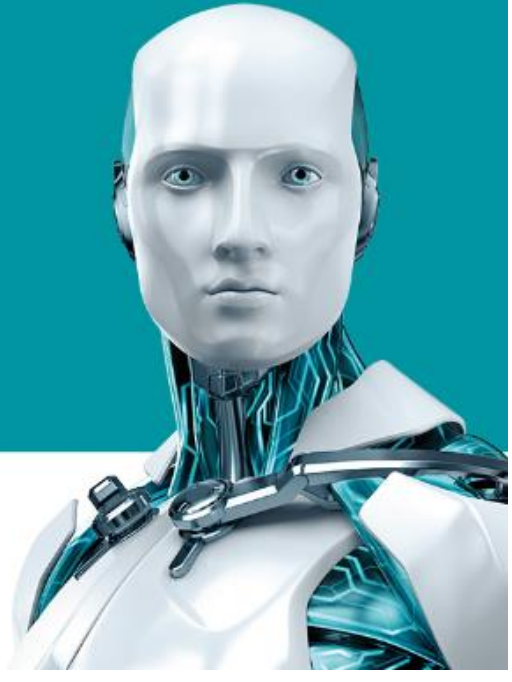
El auge del ransomware para Android

Autores
Robert Lipovský – Senior Malware Researcher
Lukáš Štefanko – Detection Engineer
Gabriel Braniša – Malware Researcher



ENJOY SAFER TECHNOLOGY™

Contenido

Resumen

El año 2016 trajo algunos desarrollos notorios al ransomware en general y también al que se enfoca en Android. Esta amenaza es uno de los problemas de seguridad más acuciantes en todas las plataformas, dado que los autores de las variedades criptográfico y de bloqueo de pantalla usaron los últimos doce meses para copiar las técnicas que resultaron efectivas en el malware para equipos de escritorio. A la vez, desarrollaron sus propios métodos sofisticados y especializados para atacar dispositivos Android.

Además de las tácticas más prevalentes para asustar a los usuarios, que los cibercriminales implementaron en el "ransomware policial", también se han puesto esfuerzos es mantener un bajo perfil, cifrando y escondiendo el payload malicioso en aplicaciones infectadas que parecen inocentes.

En 2015, ESET observó que el foco de los operadores de ransomware pasó de estar en países de Europa del Este a usuarios móviles en los Estados Unidos.

Sin embargo, durante el año pasado notamos un creciente interés de los atacantes en el mercado asiático, como evidenció el lock-screen Jisut, que empezó a usar un mensaje de rescate en chino localizado. Esta actividad en aumento también se puede ver en la prevalencia que adquirió esta amenaza, que se duplicó en los últimos doce meses.

En la primera parte del paper definimos al ransomware, observamos los datos telemétricos correspondientes a las detecciones de ESET para ver la tendencia actual de esta amenaza y cuánto se extendió, y analizamos las especificaciones del malware que se aplican al ransomware para Android. La sección principal detalla los ejemplos que más se destacaron desde 2014 y, por último, ofrecemos sugerencias para los usuarios.

El ransomware en Android

El ransomware, como lo indica su nombre, es cualquier tipo de malware que le exige al usuario infectado el pago de una suma de dinero a cambio de la promesa de "liberar" un recurso secuestrado. Existen dos tipos generales de malware que entran en esta categoría:

- Ransomware de bloqueo de pantalla
- Ransomware criptográfico

En el primero, el recurso secuestrado es el acceso al sistema comprometido; en el segundo, son los archivos del usuario.

Ambos tipos han sido un problema muy frecuente en la plataforma Windows desde 2013, año en que el ransomware comenzó a ser más popular entre los ciberdelincuentes, a pesar de que existía desde muchos años antes. Las infecciones causaron problemas tanto a individuos como a empresas.

Como una de las tendencias más notables en el malware para Android es que sus creadores han estado aplicando las técnicas que les resultaron exitosas en Windows, el surgimiento del ransomware para esta popular plataforma móvil era algo lógico y esperado.

Según ESET LiveGrid®, el número de detecciones de ransomware en Android creció más del 50% en comparaciones año a año, y tuvo su pico más alto en la primera mitad de 2016.

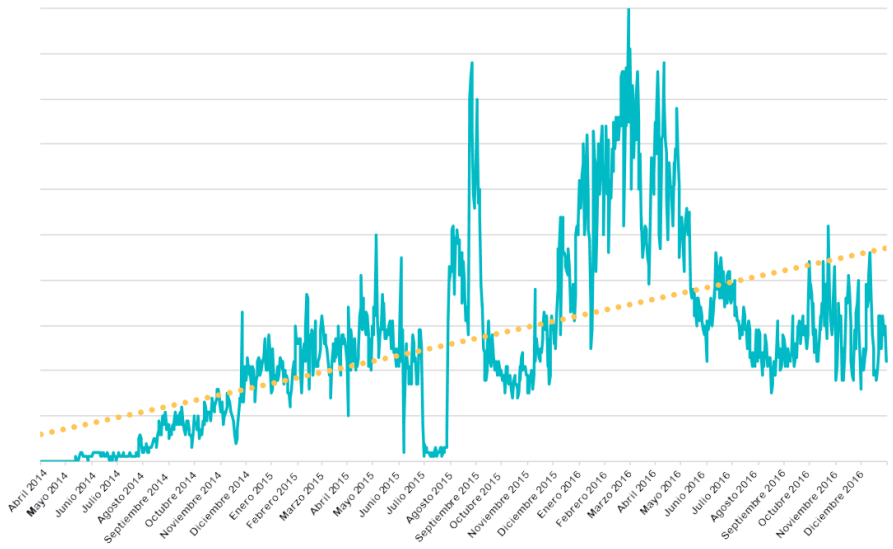


Imagen 1: Tendencia de detección de ransomware para Android, según ESET LiveGrid®

Con la creciente cantidad de usuarios que optan por el móvil en lugar de la PC a la hora de almacenar sus datos, el ransomware para Android es un atractivo cada vez mayor para los atacantes.

Vectores de infección comunes

En 2016, los expertos de ESET documentaron una tendencia emergente: el ransomware para Android que se propaga por correo electrónico. Los atacantes han estado usando Ingeniería Social para manipular víctimas y lograr que hagan clic en un enlace malicioso incluido en sus correos, con el objetivo final de redirigirlas a un APK infectado.

El malware para Android en general (ransomware incluido) se comporta como un caballo de Troya, es decir, se propaga haciéndose pasar por una aplicación legítima. Las más populares, como los juegos de moda o las apps relacionadas con la pornografía, suelen ser las elegidas para aumentar la probabilidad de que la víctima las descargue. En algunos casos, los APK maliciosos solo tienen el nombre y el ícono de la aplicación legítima, mientras que en otros, los escritores del malware toman las aplicaciones existentes y les agregan código malicioso, manteniendo la funcionalidad original. Para el malware que no se basa en una manifestación visual como el ransomware (por ejemplo, los backdoors o los troyanos SMS), el hecho de que se mantenga la funcionalidad de la aplicación aumenta la probabilidad de que el comportamiento malicioso pase desapercibido. Claro que como la modificación realizada rompe la firma digital original del paquete, tiene que volver a firmarse y a presentarse bajo una cuenta de desarrollador distinta a la original.

Ninguno de los ejemplos de ransomware descritos más adelante en este paper se encontró en la tienda oficial de Google Play. No obstante, hubo numerosos casos de malware que logró evadir con éxito las medidas de seguridad cada vez más fuertes de Google. Los investigadores de ESET encontraron y le informaron a la compañía sobre cientos de muestras de malware para Android, incluyendo scareware de falsos antivirus, spyware con phishing de credenciales, troyanos utilizados para hacer clics fraudulentos, backdoors, avisos publicitarios que muestran aplicaciones potencialmente no deseadas (PUA) y otros tipos de PUA, entre otros.

Los creadores de malware también han comenzado a usar métodos más sofisticados para propagar sus apps infectadas. Para evitar llamar la atención, comenzaron a cifrar el payload malicioso y a enterrarlo en los componentes de la aplicación, generalmente moviéndolo a la carpeta de activos usada para fotos u otros contenidos necesarios. Las apps infectadas no suelen tener una verdadera funcionalidad para el usuario, aunque funcionan como descifradores capaces de desenvolver y ejecutar el payload de ransomware escondido. Sin embargo, el uso de técnicas más avanzadas, como la infección de páginas web provocada por exploits, no es muy común en la plataforma móvil.

Comunicación del malware con su servidor de C&C

Una vez que se instalan correctamente, la mayoría de los programas maliciosos para Android le "informan" a un servidor de comando y control (C&C).

En algunos casos, el informe solo sirve para rastrear la infección y enviar información básica del dispositivo, como el modelo, el número IMEI, el idioma, etc. Pero si se establece un canal de comunicación permanente, el troyano puede recibir y ejecutar los comandos enviados por los operadores del malware. De esta forma, se crea una botnet de dispositivos Android infectados bajo el control del atacante.

A continuación mencionamos algunos ejemplos de los comandos admitidos por el ransomware para Android, más allá de su funcionalidad principal de bloquear el dispositivo y mostrar un mensaje de rescate:

- Borrar el contenido del dispositivo
- Restablecer el PIN de bloqueo de pantalla
- Abrir una URL arbitraria en el navegador del teléfono
- Enviar un SMS a un contacto cualquiera o a todos los contactos
- Bloquear o desbloquear el dispositivo
- Extraer los mensajes SMS recibidos
- Extraer los contactos
- Mostrar un mensaje de rescate diferente
- Actualizarse a una nueva versión
- Habilitar o deshabilitar los datos móviles
- Habilitar o deshabilitar el Wi-Fi
- Rastrear la ubicación del usuario por GPS

El protocolo habitual de comunicación utilizado es HTTP, aunque en algunos casos también hemos visto al malware comunicarse con su servidor de C&C a través de Google Cloud Messaging. Este servicio les permite a los desarrolladores enviar y recibir datos desde y hacia apps instaladas en el dispositivo Android. Otro protocolo similar también utilizado es Baidu Cloud Push. Algunas muestras de malware que analizamos utilizan los dominios .onion de Tor o el protocolo XMPP (Jabber).

Como alternativa, los troyanos para Android pueden recibir comandos, así como enviar datos usando la funcionalidad de SMS incorporada.

Autoprotección del malware

Infectar el dispositivo de una víctima no es una tarea trivial para los atacantes. Incluso los usuarios sin ninguna solución antimalware (como *ESET Mobile Security*) instalada cuentan con las medidas de defensa propias de Google. Naturalmente, una vez que logran superar estos obstáculos, se quieren asegurar de que su código permanecerá en el dispositivo durante el mayor tiempo posible.

Hemos visto que el malware para Android usa numerosas técnicas de autoprotección. Por ejemplo, Android/Lockerpin intenta terminar procesos pertenecientes a las aplicaciones antimalware.

Pero una de las tácticas más universales que estamos empezando a ver con mayor frecuencia es la obtención de los privilegios de Administrador de dispositivos. Cabe notar que estos no son los mismos que los privilegios de raíz, lo que sería aún más peligroso si llegaran a quedar a disposición del malware.

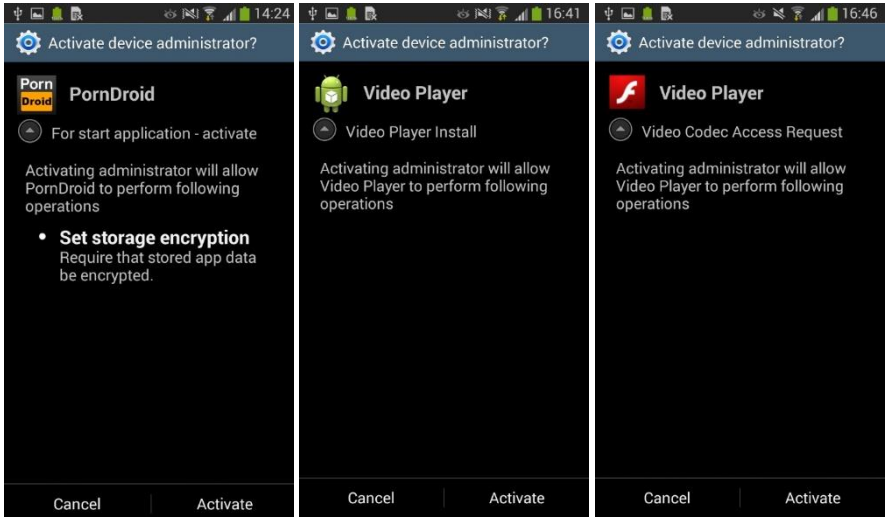


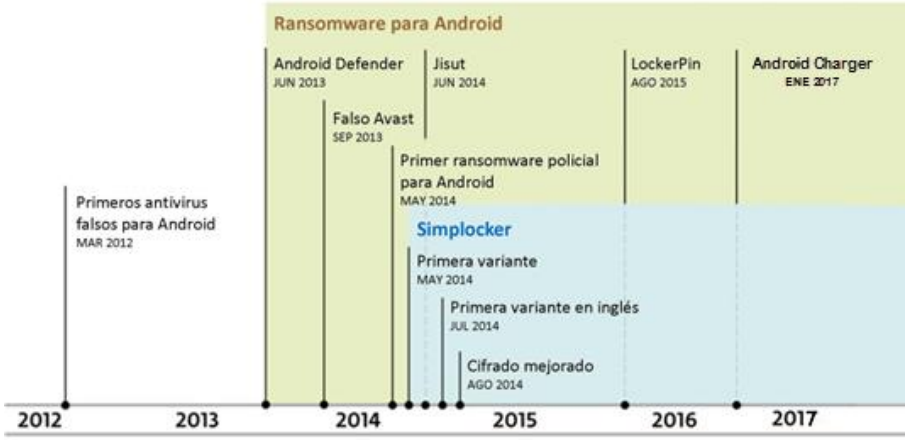
Imagen 2: Ejemplos de malware para Android solicitando privilegios de Administrador de dispositivos

Para obtenerlos, el malware la técnica de tapjacking, que crea dos capas superpuestas: una falsa que se muestra al usuario y una subyacente que activa los derechos de Administrador del dispositivo. Al hacer clic en la actividad en primer plano, la víctima hace clic sin notarlo en la pantalla de abajo, aumentando los privilegios del código malicioso.

Las aplicaciones legítimas con derechos de Administrador de dispositivos utilizan estos permisos amplios para actividades mayormente relacionadas con la seguridad. El malware, en cambio, los usa para protegerse ante la desinstalación, ya que para eliminar una aplicación es necesario revocarle sus derechos de Administrador.

Algunos programas maliciosos, como Android/Lockerpin, también utilizan los permisos adicionales que solo están disponibles para las aplicaciones del Administrador de dispositivos, por lo que son capaces de establecer o cambiar el PIN de bloqueo de pantalla.

Cronología del ransomware para Android



Las primeras apariciones de ransomware para Android fueron casos de antivirus falsos (también conocidos como *rogue*) a los que se agregó la funcionalidad de extorsión.

Los falsos antivirus son un tipo de malware que ha existido desde hace mucho tiempo: en Android desde 2012, y en plataformas de equipos de escritorio, al menos desde 2004. Como su nombre lo indica, muestran una supuesta exploración antivirus de los archivos almacenados en el dispositivo y luego tratan de convencer a los usuarios de que paguen a cambio de eliminar las amenazas que aseguran haber encontrado.

También se conocen como "scareware", dado que asustan a las víctimas haciéndoles creer que sus dispositivos están infectados para que se apresuren a pagar.

Los falsos antivirus en general no se consideran ransomware. A pesar de que intentan obtener dinero de la víctima en forma fraudulenta, se basan en métodos de persuasión en lugar de extorsión, y los usuarios engañados usualmente creen que están pagando por un producto legítimo. Sin embargo, algunos criminales decidieron hacer su software más agresivo e incorporaron la funcionalidad de bloqueo de pantalla del ransomware.

La mayoría de los casos de ransomware de bloqueo de pantalla para Windows pertenecen al ransomware policial, y esta misma tendencia se puede observar en Android. Para mejorar sus probabilidades de éxito, usa otra táctica de scareware: trata de asustar a los usuarios mostrándoles un mensaje que supuestamente fue enviado por una agencia policial como el FBI, alegando haber detectado actividades ilegales en el dispositivo.

El ransomware criptográfico que cifra archivos fue el único tipo que faltaba en la plataforma Android hasta que, en mayo de 2014, apareció una familia que ESET denominó Simplocker.

El ransomware para Android ha seguido evolucionando y se han descubierto nuevas familias en los últimos tres años. Las más notables se describen en las siguientes secciones.

Android Defender

Android Defender, descubierto por primera vez a mediados de 2013, es un ejemplo típico de un falso antivirus y probablemente sea el primer ransomware real dirigido a Android.

Como se ve en la Imagen 4, la interfaz gráfica de la aplicación fue diseñada cuidadosamente para intentar convencer a las víctimas de que están ante una aplicación de seguridad legítima. Cabe notar que, durante la exploración falsa, el troyano muestra nombres de archivos que realmente existen en la tarjeta de memoria del teléfono, lo que lo hace aún más creíble. Asimismo, los nombres de malware mostrados también son reales, con la única excepción de que el teléfono no está realmente infectado con dichos códigos maliciosos.

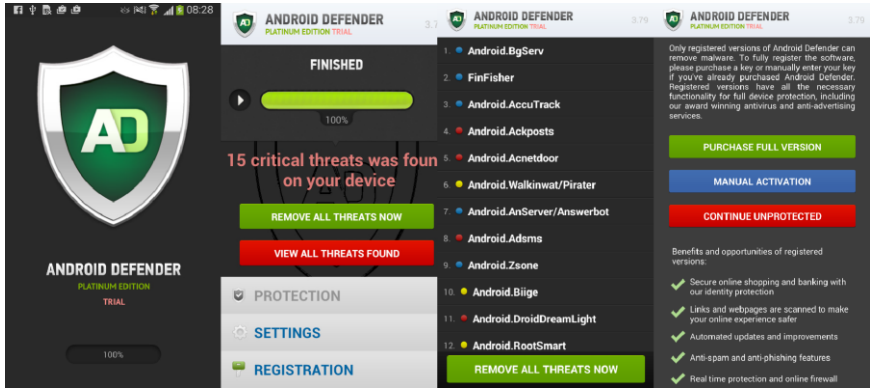
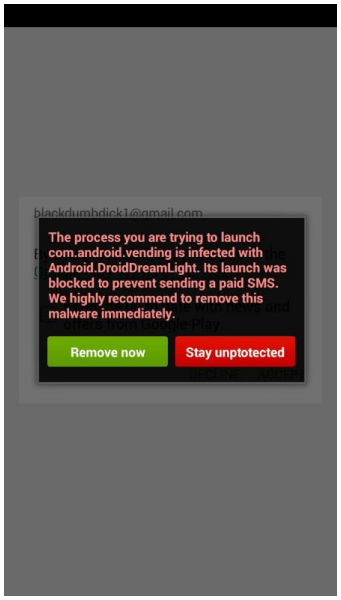
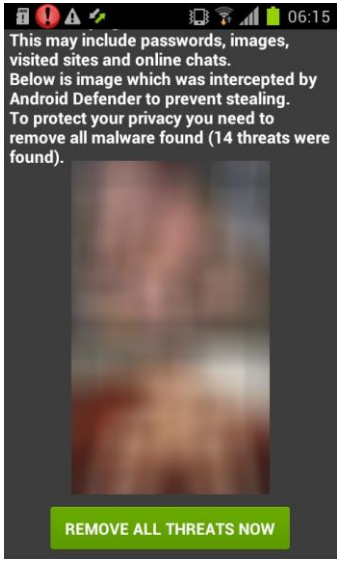


Imagen 4: Falso antivirus llamado Android Defender con una interfaz gráfica de usuario convincente



En esta etapa, el usuario todavía tiene la opción de "continuar sin protección" y cerrar la aplicación. Sin embargo, un servicio perteneciente al falso antivirus se ejecuta en segundo plano y prácticamente deja el teléfono inutilizable, ya que muestra incesantemente ventanas emergentes con advertencias sobre la existencia de malware. Al "Continuar sin protección" se desactiva la ventana emergente que se muestra en pantalla, pero se abre otra... y así sucesivamente.

Fig. 5: Incessant Android Defender popups make the infected device practically unusable



En caso de que este comportamiento no haya persuadido a las víctimas a creer que están infectadas y deben pagar por la "versión completa" del software de seguridad falso, seis horas después de su lanzamiento inicial cambia a un modo aún más agresivo. Android Defender muestra una ventana de pantalla completa con imágenes pornográficas explícitas que no se pueden cerrar.

Imagen 6: Android Defender bloquea la pantalla mostrando imágenes pornográficas

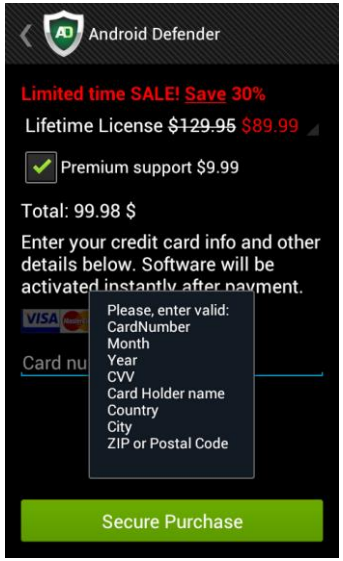


Imagen 7: Opciones de compra de Android Defender

Si el usuario infectado se rinde y decide pagar, el fraude le costará como mínimo 89,99 dólares. El mayor problema es que los datos de la tarjeta de crédito del usuario ahora están en manos de los operadores del malware (o de cualquier persona que esté escuchando en la red, dado que los datos se envían sin cifrar) y quedan disponibles para cualquier uso indebido posterior.

ESET Mobile Security detecta a Android Defender como *Android/FakeAV.B*.

Combinación del ransomware con falsos antivirus y pornografía

El segundo ejemplo de falso antivirus no aparece con un nombre inventado como Android Defender, sino que parasita el nombre de una aplicación de seguridad para Android legítima de Avast[1].

Curiosamente, el malware, detectado por ESET como *Android/FakeAV.E* también usa indebidamente otra marca conocida: se propaga haciéndose pasar por una aplicación móvil para el sitio web de videos para adultos PornHub.

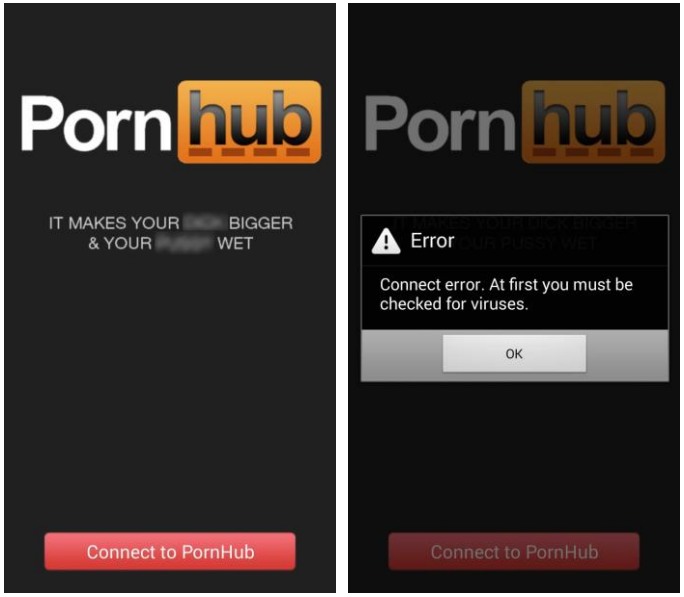


Imagen 8: Primer "disfraz" de Android/FakeAV.E: app falsa de PornHub

Cuando se inicia, en vez de mostrar videos, muestra un mensaje indicando que el dispositivo debe ser explorado en busca de virus. Tras hacer clic en Aceptar, se ejecuta una exploración fraudulenta.

1 El falso antivirus no está relacionado de ninguna manera con el software de Avast.

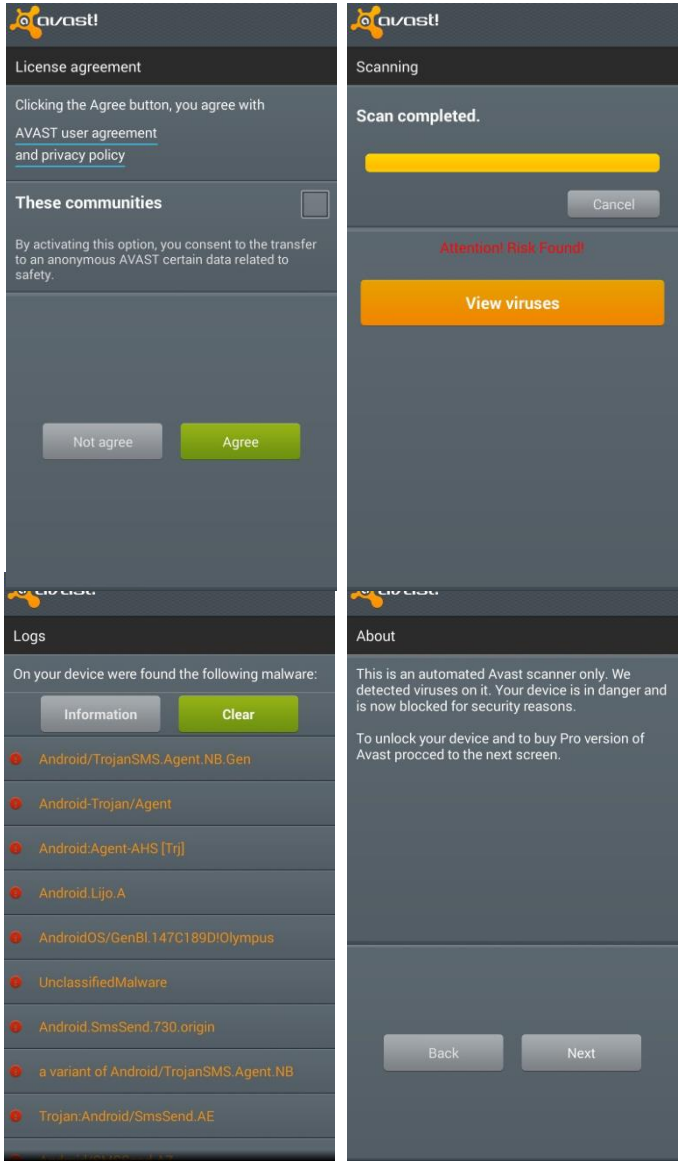


Imagen 9: Segundo disfraz de Android/FakeAV.E: falsa app de Avast

La narrativa de este fraude es bastante extraña. En primer lugar, el mensaje mostrado por la interfaz falsa de Avast indica que el "dispositivo está en peligro y se ha bloqueado por razones de seguridad", y que es necesario comprar la versión Pro del programa.

Más allá del hecho obvio de que un antivirus legítimo nunca dejaría el dispositivo inutilizable, el texto corresponde al comportamiento de un falso antivirus. Sin embargo, la molesta pantalla de rescate que aparece cuando se bloquea el equipo exige el pago de una multa de 100 dólares para evitar consecuencias legales.

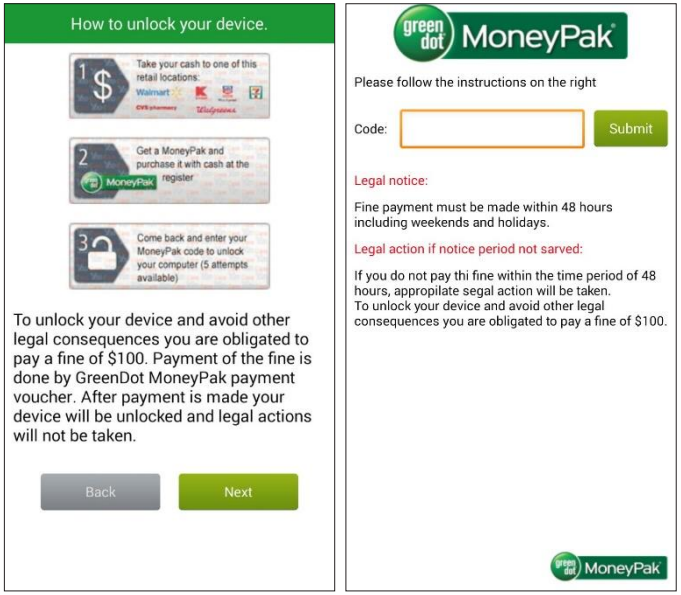


Imagen 10: Pantallas de pedido de rescate de Android/FakeAV.E

Parece que los autores de este malware tomaron las pantallas de mensajes de rescate de otro ransomware, e incluso mantuvieron los mismos errores tipográficos.

Ransomware policial

El ransomware de bloqueo de pantalla para Windows ha utilizado varias temáticas en el pasado. Algunos ejemplos incluían copias de la conocida "pantalla azul de la muerte" o un mensaje de activación de Windows. Aunque aún siguen apareciendo nuevos temas, el más recurrente en estos últimos años es el policial, y Reveton es una de las familias más conocidas de este tipo.

El ransomware policial afirma que el dispositivo fue bloqueado por una agencia local de aplicación de la ley por haber detectado contenido o actividades ilegales. Los mensajes de rescate citan algunos artículos del Código Penal, pero le dicen al usuario que puede evitar acciones legales si simplemente paga la suma indicada. A menudo se basa en la geolocalización por IP para "personalizar" la infección, utilizando banners de las agencias policiales locales.

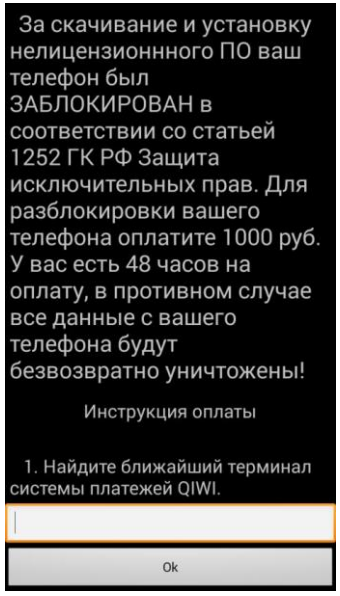


Imagen 11: Las primeras versiones de ransomware policial estaban dirigidas a usuarios de Android de habla rusa

Las primeras muestras de ransomware policial para Android aparecieron en la primera mitad de 2014 y estaban dirigidas a usuarios de habla rusa.

Poco después aparecieron las variantes que permitían la localización, así como las variantes en inglés.

Imagen 12: Variantes de Android/Locker capaces de mostrar una instantánea tomada por la cámara y personalizar la pantalla con el pedido de rescate según la ubicación del usuario

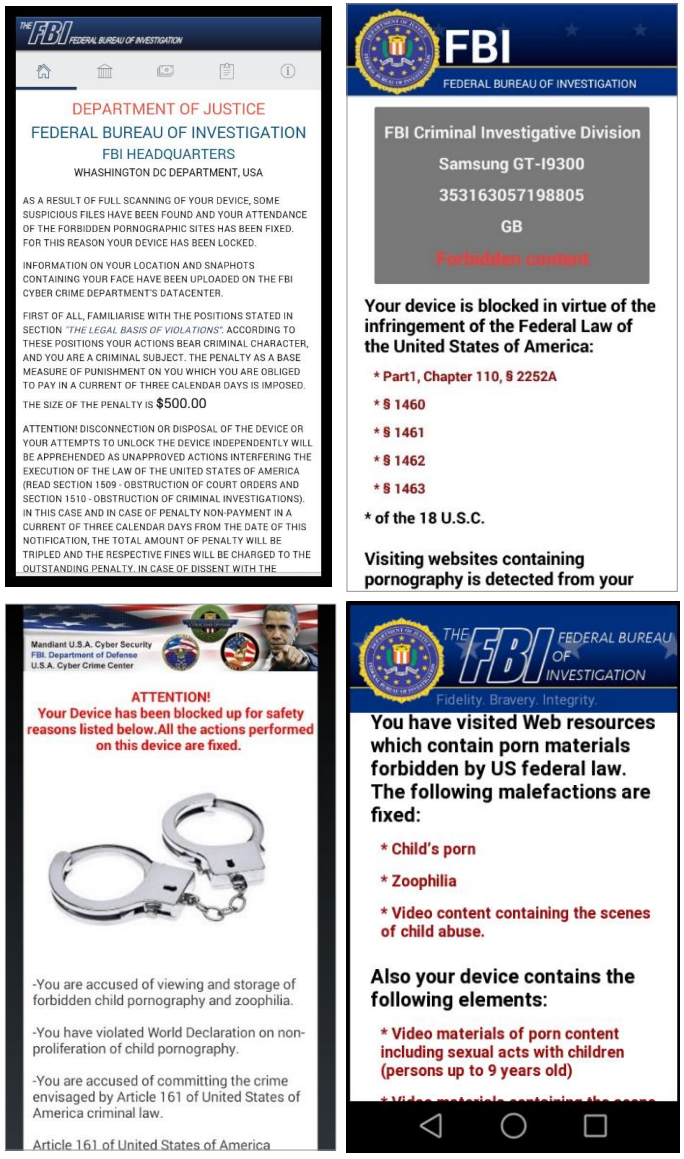


Imagen 13: Variantes de Android/Koler que comienzan a atacar a usuarios de habla inglesa

ESET detecta los ejemplos del ransomware policial mencionados arriba como variantes de *Android/Koler* o *Android/Locker*.

Simplocker

En mayo de 2014, ESET detectó al primer ransomware de cifrado de archivos para Android, una evolución esperada, ya que este tipo de malware se extendió mucho en Windows en los últimos años: Cryptolocker, Cryptowall, CTB-Locker y TorrentLocker son solo algunos de los muchos ejemplos infames.

Cuando se ejecuta, el troyano muestra un mensaje de rescate (Imagen 14) y cifra los archivos en segundo plano en un proceso separado. *Android/Simplocker.A* explora la tarjeta SD[2] en busca de archivos con cualquiera de las siguientes extensiones de imágenes, documentos o vídeos: JPEG, JPG, PNG, BMP, GIF, PDF, DOC, DOCX, TXT, AVI, MKV, 3GP, MP4; luego, los cifra con AES.

La clave de cifrado utilizada se codifica dentro del archivo binario como texto sin formato, por lo que no es difícil decodificarla, a diferencia de las familias de ransomware criptográfico para Windows más establecidas. Por esta razón, denominamos al malware Android/Simplocker y creemos que estas primeras variantes fueron o bien una prueba de concepto o una versión temprana de una amenaza más seria.

2 La amenaza también afectó los dispositivos que no tenían una tarjeta SD física. En dichos dispositivos, la memoria interna aparece como una tarjeta SD emulada.

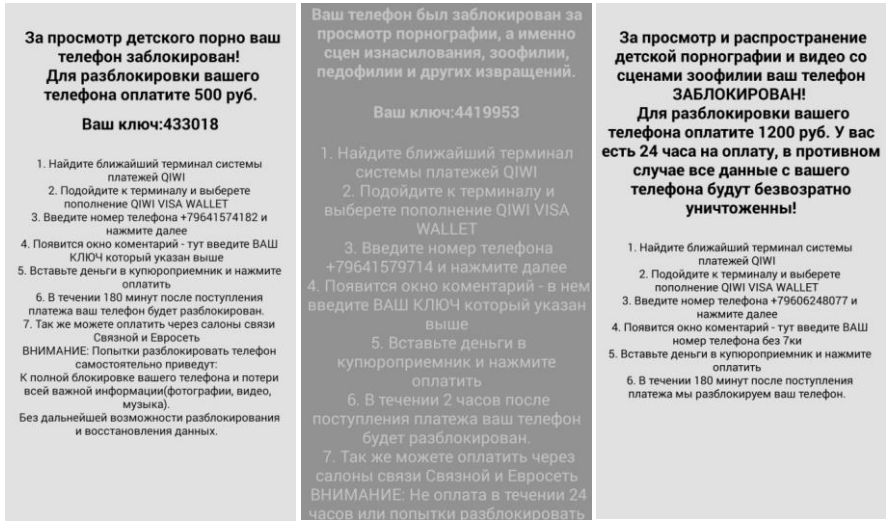


Imagen 14: Pedidos de rescate de las primeras versiones rusas de Android/Simplocker

Imagen 15: Simplocker usa las fotos tomadas por la cámara frontal del dispositivo para intimidar a la víctima

Este mensaje de rescate está escrito en ruso y pide el pago en grivnas ucranianas, por lo que podemos suponer que la amenaza está dirigida a usuarios de Android en Ucrania.

El malware le exige a la víctima que realice el pago con cupones de dinero prepagos, como MoneXy o QIWI, ya que no son tan fáciles de rastrear como las tarjetas de crédito tradicionales. Algunas variantes de Simplocker también muestran una foto de la víctima tomada con la cámara del teléfono infectado para aumentar el factor de scareware.

Vectores de propagación de Simplocker

Android/Simplocker normalmente intenta engañar al usuario haciéndose pasar por una aplicación legítima y popular. En general, la temática gira en torno a la pornografía en Internet (algunas aplicaciones móviles maliciosas se hacen pasar por videos para adultos o apps para verlos, por ejemplo), a los juegos más populares como Grand Theft Auto: San Andreas, o a aplicaciones muy comunes como Flash Player.

Sin embargo, Android/Simplocker también ha estado utilizando un mecanismo menos común: los descargadores de troyanos. Aunque son habituales en el mundo del malware para Windows, no son tan comunes en Android. Son pequeños programas cuyo único propósito (y la única razón por la que son maliciosos) es descargar otro malware.

Las razones por las cuales la estrategia tiene mayores posibilidades de evadir el radar de seguridad en el mercado de apps de Android (al igual que Bouncer para las aplicaciones oficiales de Google Play) e incluso escapar a la atención del usuario más precavido son las siguientes:

- Lo único que hace la aplicación móvil es abrir una URL fuera de la app, lo cual no es en sí mismo un comportamiento malicioso
- El descargador de troyanos prácticamente no requiere permisos que se consideren "potencialmente peligrosos"; por lo tanto, incluso aunque el usuario revise minuciosamente los permisos de las apps durante su instalación, puede aceptar la descarga

Además, en los ejemplos que analizamos, la URL incluida en la app no dirige al usuario directamente al APK malicioso de Simplocker. En cambio, el troyano se carga recién cuando el atacante lo redirige desde el servidor bajo su control.

No vimos ningún caso en que Android/Simplocker se extendiera a través de la tienda oficial de Google Play.

Simplocker en inglés

Apenas un mes después de haber descubierto las primeras variantes de Simplocker, empezamos a detectar nuevas versiones de este ransomware que presentaban algunas mejoras significativas.

El cambio más notable fue en el idioma utilizado: *Android/Simplocker.I* ahora muestra pantallas de rescate en inglés en lugar de ruso. Trata de convencer a la víctima de que el FBI bloqueó el dispositivo por haber detectado actividad ilegal, una conducta típica del ransomware policial. El rescate pedido ahora está en el rango de 200 a 500 dólares y se le exige a la víctima que lo pague con un cupón de MoneyPak.

Al igual que algunas variantes anteriores de Android/Simplocker, esta también emplea la táctica de intimidación por scareware que muestra la imagen tomada por la cámara frontal del dispositivo.

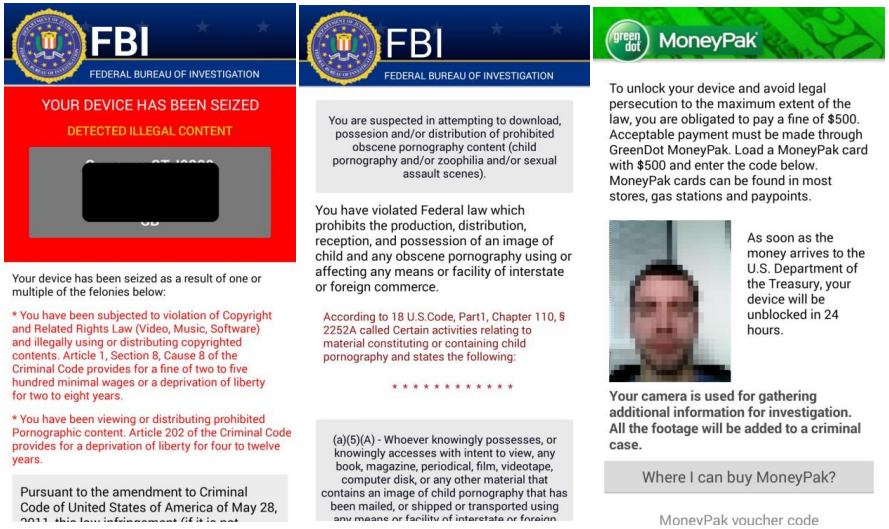


Imagen 16: Mensajes de rescate de Android/Simplocker en inglés

Las últimas variantes han cambiado ligeramente el aspecto visual del pedido de rescate. Por ejemplo, en lugar del FBI, la agencia que acusa a la víctima de "asistir" a sitios pornográficos prohibidos (sic) es la NSA y exige el pago de 500 dólares.

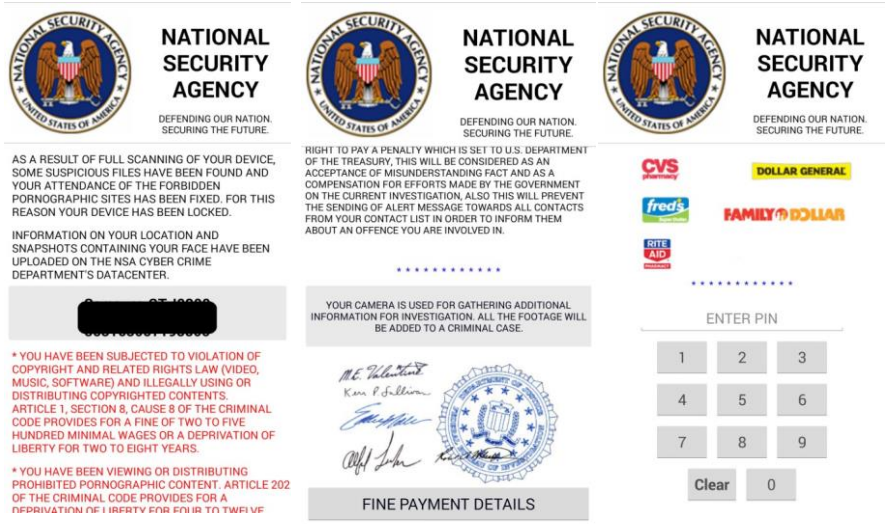


Imagen 16: Mensajes de rescate de Android/Simplocker en inglés

Además de cifrar documentos, imágenes y videos almacenados en la tarjeta SD, el troyano ahora también es capaz de cifrar los archivos comprimidos: ZIP, 7z y RAR. Esta "mejora" puede traer consecuencias muy graves, ya que muchas de las soluciones para hacer backups de archivos en Android almacenan las copias de seguridad en forma de archivos comprimidos. En caso de que el usuario se infecte con Android/Simplocker.I, estos backups también quedarán cifrados.

Las variantes de Simplocker más avanzadas también piden derechos de Administrador de dispositivos durante su instalación, lo que las hace mucho más difíciles de eliminar, sobre todo cuando el ransomware está bloqueando la pantalla.

Otro cambio notable fue que el malware comenzó a utilizar el protocolo XMPP (Extensible Messaging and Presence Protocol), también conocido como Jabber, para comunicarse con su servidor de C&C. Esto hace más difícil rastrear los servidores de C&C, en comparación a lo que sucede con HTTP. Android/Simplocker utiliza este protocolo de comunicación de mensajería instantánea para enviar información al servidor sobre el dispositivo infectado y ejecutar los comandos recibidos. Un tercer tipo de direccionamiento de C&C utilizado por algunas variantes de Android/Simplocker es el uso de dominios .onion de Tor.

El paso más importante en la evolución de Simplocker tiene que ver con las claves de cifrado utilizadas para cifrar los archivos. Unos meses después de las versiones iniciales, vimos variantes que usaban claves únicas generadas y enviadas desde el servidor de C&C. Esto marcó el final de la etapa de prueba de concepto del troyano y ya no fue posible descifrar fácilmente los archivos secuestrados.

Lockerpin

En general, troyanos de bloqueo de pantalla para Android anteriores conseguían esta funcionalidad poniendo constantemente en un primer plano la ventana de pedido de rescate en un bucle infinito. Pero no era tan difícil deshacerse del malware y desbloquear el dispositivo usando la aplicación de línea de comandos Android Debug Bridge (ADB), desactivando los derechos de administrador, o desinstalando la aplicación maliciosa en Modo Seguro.

Desafortunadamente, con *Android/Lockerpin*, que descubrimos en agosto de 2015, los escritores de malware mejoraron sus tácticas. Si un usuario se infecta, la única manera de quitar la pantalla de bloqueo por PIN es si el dispositivo fue previamente liberado o si tiene instalada una solución MDM capaz de restablecer el PIN. De lo contrario, la única opción es el restablecimiento a la configuración de fábrica, que elimina todos los datos del dispositivo.

La técnica de Lockerpin es extremadamente simple: aprovecha el mecanismo de bloqueo de pantalla por código de cuatro dígitos que ya viene incorporado en Android. Es capaz de establecer un PIN en el dispositivo, o incluso cambiarlo si ya se había configurado uno, siempre y cuando la víctima le haya concedido los privilegios de Administrador de dispositivos a la app maliciosa.

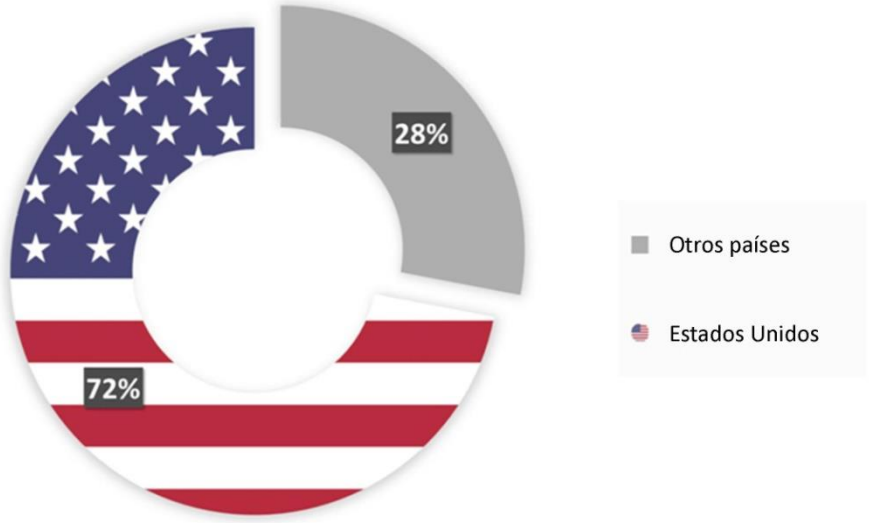


Imagen 18: Distribución geográfica de Android/Lockerpin

Según las estadísticas de LiveGrid® de ESET, la mayoría (el 72%) de los dispositivos Android infectados están en los Estados Unidos. La tendencia indica que los creadores de malware para Android están dejando de atacar mayormente a los usuarios en Rusia y en Ucrania, y están comenzando a buscar víctimas donde supuestamente pueden obtener ganancias mayores.

El malware se ha estado propagando haciéndose pasar por una aplicación para ver videos para adultos.

Las primeras versiones de la familia Android/Locker consiguen los derechos de Administrador de dispositivos de la misma manera que el resto de los troyanos para Android: se basan en la suposición de que el usuario activará voluntariamente los privilegios elevados.

En versiones más recientes, se obtienen de una forma mucho más encubierta. La ventana de activación de administración de dispositivos queda tapada por la ventana maliciosa del troyano, que se hace pasar por la "instalación de un parche de actualización". Esta técnica se basa en la posición del botón Continuar falso, que está perfectamente colocado sobre el botón Activar subyacente. Por lo tanto, cuando las víctimas hacen clic en el botón Continuar de esta instalación de aspecto inocuo, sin darse cuenta le han concedido al malware los privilegios de Administrador de dispositivos.

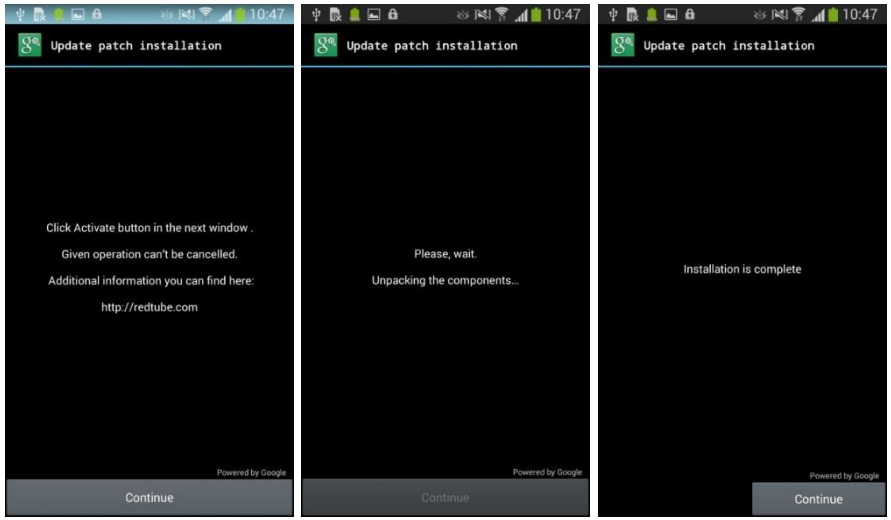
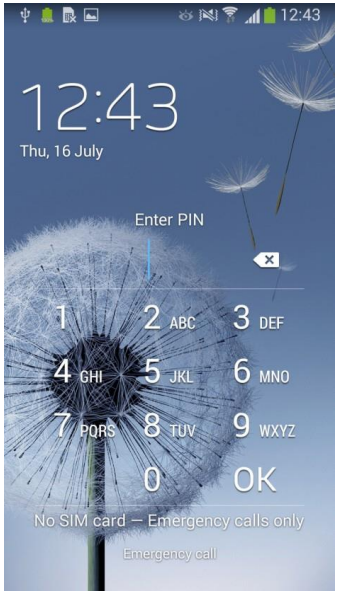


Imagen 19: Android/Lockerpin obtiene furtivamente los derechos de administrador de dispositivos mediante la superposición de dos actividades en la pantalla

Después de la instalación, aparece el típico escenario de ransomware policial. El usuario ve un mensaje falso del FBI solicitando un rescate de 500 dólares supuestamente por ver y almacenar material pornográfico prohibido.

Imagen 20: Mensaje de rescate de Android/Lockerpin

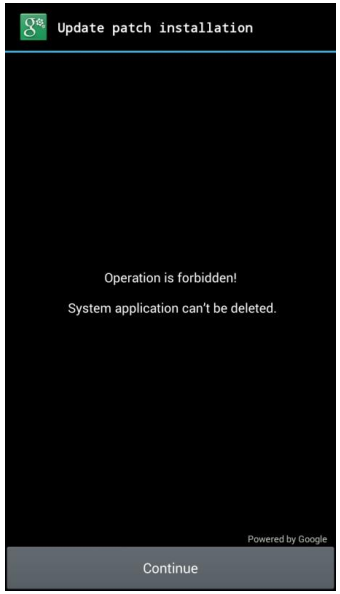


Después de un lapso de tiempo específico tras la visualización del mensaje de rescate, el malware configura un PIN (o lo cambia) en base a un número generado aleatoriamente y que no se envía al atacante. Algunas variantes de Lockerpin tienen la funcionalidad de quitar el bloqueo existente restableciéndolo al valor cero.

Imagen 21: Dispositivo bloqueado por Android/Lockerpin

Autodefensa agresiva de Lockerpin

Android/Lockerpin no solo obtiene los privilegios de Administrador de dispositivos de una forma novedosa y encubierta, sino que también utiliza un mecanismo agresivo de autodefensa para asegurarse de que nadie se los quite. Cuando los usuarios intentan desactivarlos se produce un error, dado que el troyano ya habrá registrado una función de devolución de llamada para reactivar sus privilegios inmediatamente luego de cada intento de eliminarlos.



Al igual que ocurre cuando el troyano activa por primera vez el Administrador de dispositivos, si se hace un intento de revocar dicho permiso, la ventana se vuelve a cubrir con otra ventana falsa, como se muestra en la Imagen 22. Si se hace clic en Continuar, en realidad se están reactivando los privilegios elevados.

Imagen 22: Android/Lockerpin bloquea los intentos de revocar los derechos de Administrador de dispositivos

Como capa adicional de autoprotección, el ransomware también intenta terminar los procesos antivirus activos cuando el usuario trata de desactivar sus derechos. El troyano busca tres aplicaciones antivirus móviles específicas: ESET Mobile Security y otras soluciones para Android desarrolladas por Avast y 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

Imagen 23 Android/Lockerpin intenta terminar los procesos antivirus activos

El malware no logrará cerrar ni eliminar ESET Mobile Security. Lockerpin intenta terminar el proceso `com.android.settings` para evitar la desinstalación estándar del malware a través del gestor de aplicaciones incorporado de Android.

Jisut

Esta extraña familia de ransomware que las soluciones de seguridad de ESET detectan como *Android/LockScreen.Jisut* tuvo un gran aumento de actividad en 2016, ya que sus detecciones de duplicaron respecto a 2015.

La mayoría de las variantes vistas tratan de bloquear el dispositivo para que el usuario no pueda utilizarlo, pero lo extraño es que no piden el pago de un rescate. Su única actividad visible es un cambio en el fondo de pantalla o un sonido que se reproduce de fondo, lo cual fortalece nuestra conjetura de que se creó como una broma y no con el objetivo de obtener ganancias económicas.

Sin embargo, ESET también documentó variantes que exigen un pago. Para simplificar el proceso, los atacantes añaden un código QR que permite al usuario infectado escribirles un mensaje o hacer el pago directamente. Algunas muestras incluso trataban de vender la app o su código fuente y una en particular, analizada a principios de 2017, también tenía la habilidad especial de demandar el pago de un rescate a través de un mensaje de voz. Esto la convirtió en el primer ransomware para Android "parlante" detectado in-the-wild. Tras infectar el equipo, una voz femenina felicitaba en chino a la víctima y le pedía 40 yuanes (aproximadamente 6 dólares estadounidenses) para desbloquearlo.

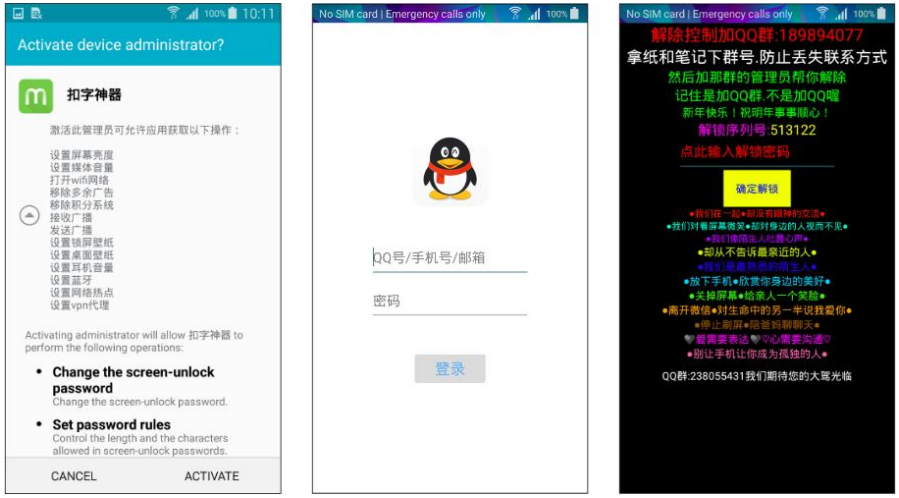


Imagen 24: Android/Jisut pide derechos de administrador, recolecta credenciales QQ y tras bloquear la pantalla demanda el pago de un rescate con un mensaje de voz

Esta variante se propagó principalmente en China y es probable que sea el trabajo de cibercriminales locales jóvenes que recién están empezando a probar creaciones maliciosas.

La mayoría de los tipos de ransomware (tanto los bloqueadores de pantalla como los criptográficos) exigen el pago de un rescate a través de cupones de dinero prepago, como MoneyPak o MoneXy, o con bitcoins, porque estos métodos de pago son prácticamente imposibles de rastrear. Sin embargo, los operadores de Jisut tomaron un enfoque totalmente diferente y no parecen preocuparse por mantener su anonimato. Las pantallas molestas de ransomware incluyen información de contacto en la red social china QQ e instan a las víctimas a ponerse en contacto directamente con los autores si desean recuperar sus archivos. Si la información de los perfiles en QQ es válida, se trata de jóvenes chinos de entre 17 y 22 años de edad.

Las primeras variantes de *Android/LockScreen.Jisut* comenzaron a aparecer durante la primera mitad de 2014. Desde entonces, hemos detectado cientos de variantes con diferencias de comportamiento o con distintos mensajes de rescate, pero que se basan en la misma plantilla de código.

La familia de malware Jisut se diferencia de todos los demás tipos de ransomware conocidos de bloqueo de pantalla. Uno de sus comportamientos es crear una "Actividad" de pantalla completa (término del desarrollador de Android para "ventana") que cubre todas las demás actividades. La pantalla completa superpuesta es simplemente un fondo negro para que el dispositivo aparezca como si estuviera bloqueado o apagado. Si el usuario abre el menú para apagar o reiniciar el dispositivo, aparecerá un mensaje de broma. Algunas muestras reproducen la icónica música de Psycho, de Alfred Hitchcock, mientras el equipo vibra en un bucle infinito.

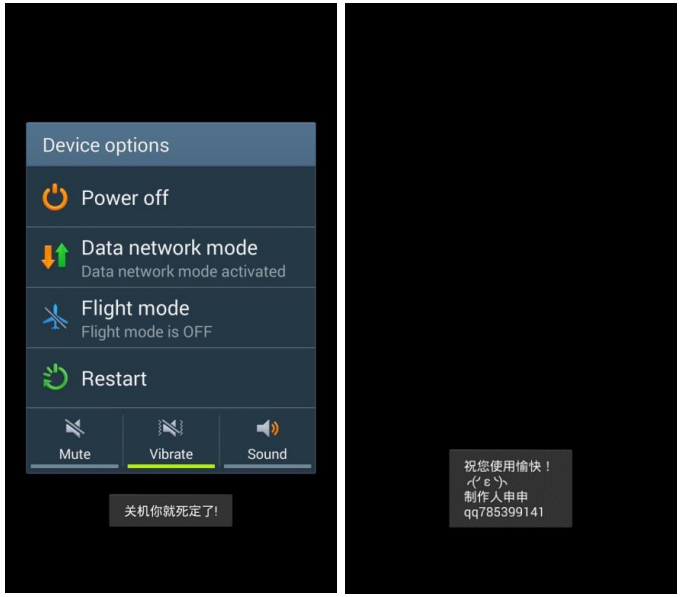


Imagen 25: Mensajes de broma de Jisut: Izquierda: "¡Fuiste: estás muerto!" Derecha: "¡Espero que te estés divirtiendo! Productor Shen"

Otra variante de Jisut le indica al usuario que haga clic en un botón que dice "Soy un idiota" 1000 veces. Sin embargo, una vez que el contador llega a 1000 no ocurre nada; solo se restablece a cero y el usuario frustrado puede continuar haciendo clic indefinidamente.

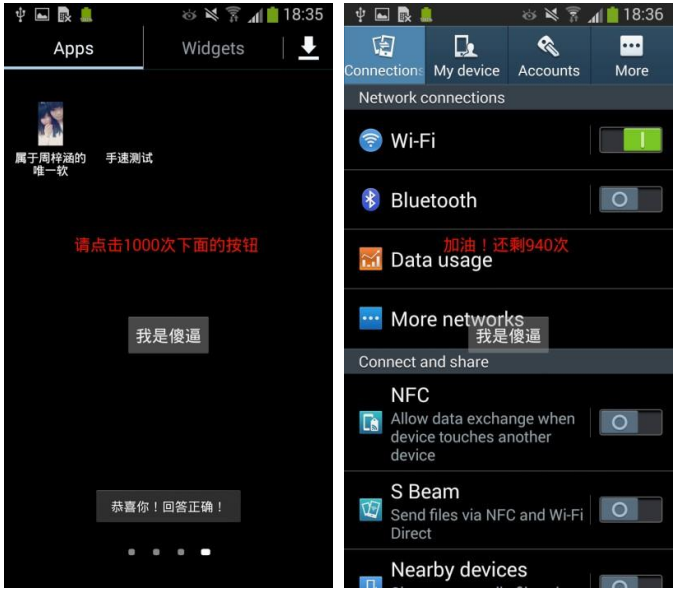


Imagen 26: Android/LockScreen.Jisut: "Haz clic en el siguiente botón 1000 veces"

Además, la mayoría de variantes de Android/LockScreen.Jisut también contienen funcionalidades dañinas. Al igual que Android/Lockerpin, son capaces de establecer o cambiar el PIN de la pantalla.

Algunas variantes no se basan en la funcionalidad legítima de bloqueo de pantalla en Android, sino que muestran su propia ventana de pantalla completa imitándola, como lo hacen las familias de ransomware policial Android/Locker y Android/Koler.

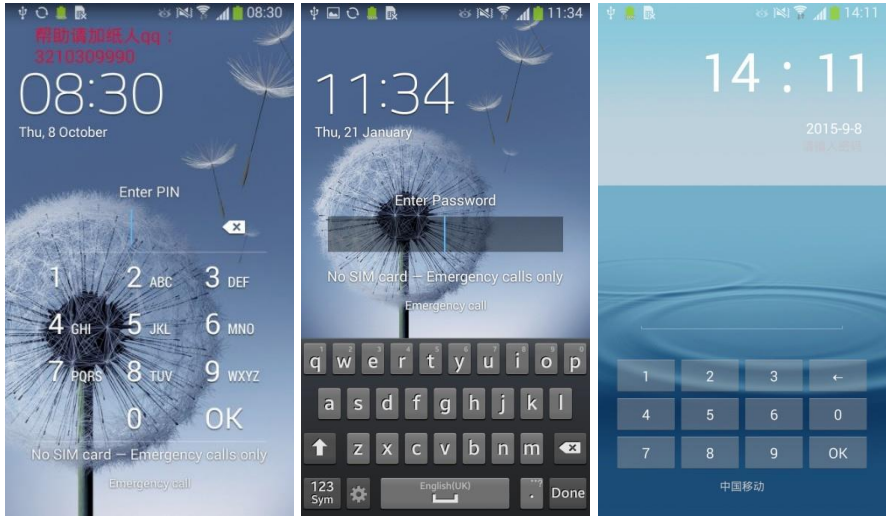


Imagen 27: Dispositivo bloqueado por Android/LockScreen.Jisut mediante el establecimiento de un PIN o una contraseña

Imagen 28: Bloqueadores de pantalla personalizados con el número de QQ del autor del malware

Además de su funcionalidad de ransomware, algunas variantes pueden propagarse enviando a todos los contactos del usuario un mensaje SMS con un enlace URL que los dirige al malware.

Charger

A principios de 2017 se descubrió en Google Play un troyano backdoor controlado remotamente con la capacidad de bloquear el dispositivo del usuario, escondido en una supuesta app para ahorro de energía llamada EnergyRescue.

El malware, llamado Charger, trataba de robar datos del usuario y tomar el control del dispositivo. Rápidamente se unió a un exclusivo club, siendo uno de los primeros ransomware de bloqueo de pantalla que pasó las revisiones de seguridad de Google Play.

El análisis de ESET mostró que podía recolectar contactos y aplicaciones instaladas; sin embargo, a pesar de tener esta funcionalidad, parece que Charger nunca envió la información a los atacantes.

En base a los comandos del cibercriminal, también era posible bloquear o desbloquear dispositivos infectados y demandar un rescate de 0,2 bitcoins. Además, podía extraer y enviar todos los mensajes de texto, incluyendo bandejas de entrada, salida y borradores, enviar una foto de la víctima, actualizarse y activar derechos de administrador. Los atacantes gestionaban estas funciones usando un protocolo HTTP.

Cómo proteger tu dispositivo Android

Lo principal es estar al tanto de las amenazas y tomar medidas preventivas. Las más importantes son evitar las tiendas de apps no oficiales y tener una aplicación de seguridad móvil instalada y siempre actualizada. Además, es imprescindible contar con un backup de todos los datos importantes.

Lo más probable es que el usuario que toma las medidas adecuadas nunca se cruce con ningún pedido de rescate. Si llega a caer víctima y sus datos terminan cifrados, el backup hará que la experiencia no sea más que una molestia.

Si se produce una infección, hay varias opciones para eliminar el malware, según su variante. Para la mayoría de las familias simples de ransomware de bloqueo de pantalla, la solución es reiniciar el dispositivo en Modo seguro (de manera que las aplicaciones de terceros, incluyendo el malware, no se carguen), con lo que el usuario podrá desinstalar fácilmente la aplicación maliciosa. En caso de que la aplicación haya conseguido privilegios de Administrador, estos deberán ser revocados desde el menú de ajustes antes de poder desinstalarla.

Si un ransomware con derechos de Administrador de dispositivos bloqueó el equipo usando la funcionalidad integrada de Android de bloqueo de pantalla por PIN o contraseña, la situación se complica. Debería ser posible restablecer el bloqueo usando el Administrador de dispositivos Android de Google o una solución MDM alternativa.

Los teléfonos Android liberados tienen aún más opciones. El restablecimiento a los valores de fábrica, que borra todos los datos, puede usarse como último recurso en caso de que no haya ninguna solución MDM disponible. Si un ransomware criptográfico como Android/Simplocker cifró los archivos del dispositivo, les aconsejamos ponerse en contacto con el soporte técnico de sus proveedores de seguridad. Dependiendo de la variante específica del ransomware, descifrar los archivos puede ser posible o no.

No recomendamos pagar el rescate por varias razones. Si bien es cierto que algunas bandas criminales establecidas devuelven a los usuarios sus archivos descifrados, este no siempre es el caso.

El ransomware de cifrado de archivos es extremadamente popular entre los creadores de malware y existen muchas familias diferentes para Windows (su nombre en inglés, filecoders, es la detección de ESET para esta categoría). Muchos ciberdelincuentes se sumaron a este negocio con la esperanza de copiar el éxito de Cryptolocker y otras amenazas similares, pero nuestro análisis demostró que pueden ser ineficientes. Para los usuarios, esto implica dos cosas: en primer lugar que, aunque paguen, sus archivos quizá no se puedan descifrar; en segundo lugar, que puede llegar a ser posible descifrarlos sin tener que pagar.

En Android encontramos unas cuantas variantes donde el código para descifrar los archivos o desinstalar la pantalla de bloqueo no existía, por lo que pagar no hubiese servido de nada. Todo se reduce a una cuestión de confianza: ¿se puede confiar en que los ciberdelincuentes mantengan su parte del trato y descifren los archivos después de haber pagado?

Obviamente, no hay garantías. E incluso si los archivos se descifran, no hay nada que les impida a esos atacantes (o a otros) volver por más. Si tenemos en cuenta la economía del ransomware (el FBI estima que sus ganancias ascendieron a 1 billón de dólares en 2016), ceder ante las demandas solo sigue alimentando el problema.

Una opción mucho más sensata es la prevención mediante la adhesión a los principios básicos de seguridad, el uso de software de seguridad y la creación de backups de datos (no solo en el propio dispositivo). Estas medidas están a disposición del usuario y además son fáciles de usar, por lo que realmente no existe razón para no aplicarlas.