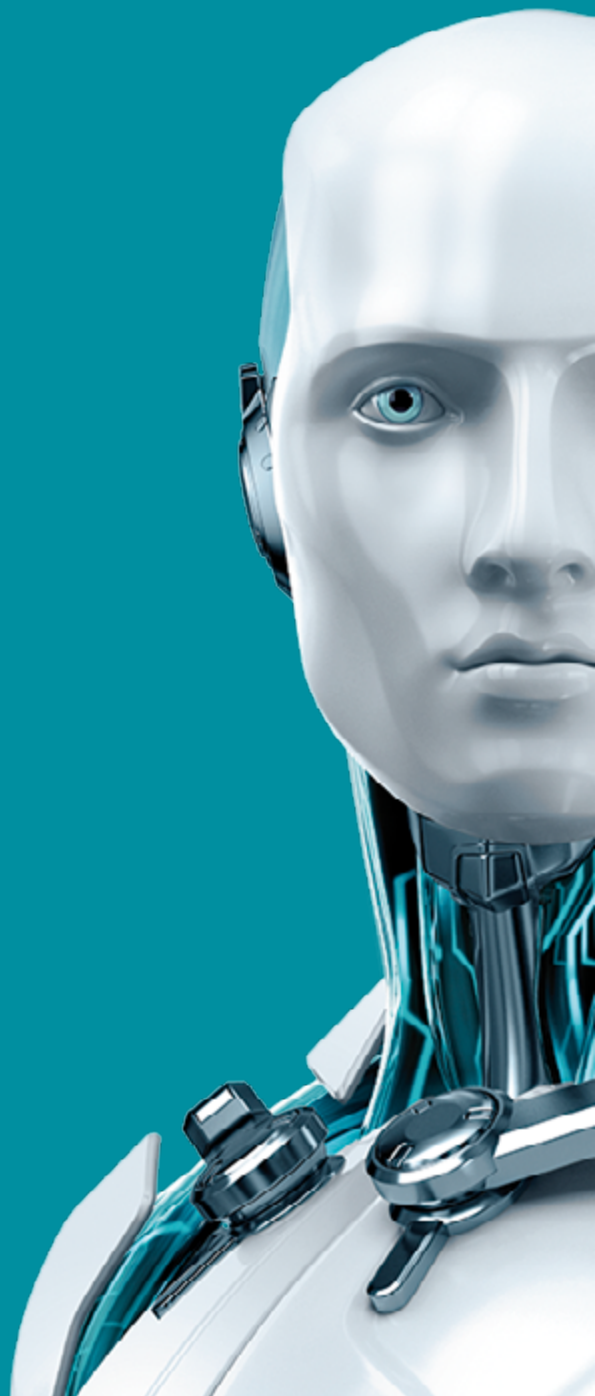
ENJOY SAFER TECHNOLOGY™

RANSOMWARE

Cómo proteger a su empresa del malware de extorsión



Contenido

Resumen ejecutivo

El ransomware es un tipo de malware que bloquea los dispositivos o cifra su contenido con el fin de extorsionar al propietario para devolverle el acceso a dichos recursos a cambio de dinero. En ciertos casos, incluye un temporizador que indica el plazo de pago: si el usuario no lo cumple, aumenta el importe que deberá pagar para descifrar los datos y el hardware. En última instancia, la información y el dispositivo quedan bloqueados permanentemente.

Entre los ejemplos más conocidos de ransomware dirigido a equipos de escritorio se encuentran Reveton, CryptoLocker, CryptoWall y TeslaCrypt, y para plataformas móviles, Simplocker y LockerPin.

Los análisis llevados a cabo por ESET indican que el ransomware se ha convertido en una opción muy popular entre los cibercriminales y que su uso se ha extendido ampliamente durante los últimos años, atacando tanto los dispositivos privados como los corporativos. Aunque actualmente Windows y Android son los sistemas operativos que se ven más afectados, investigaciones recientes demuestran que Linux y OS X no son inmunes al ransomware.

El objetivo del presente *white paper* es ayudar a las empresas a mitigar los riesgos de infección por ransomware. Para ello, suministramos información sobre los vectores de ataque empleados con mayor frecuencia, indicamos qué pueden hacer las empresas para proteger eficazmente los dispositivos corporativos y su contenido, y finalmente describimos las opciones disponibles en caso de que los dispositivos o archivos ya estén infectados.

Además, se explica la postura de ESET con respecto a la pregunta más apremiante que las víctimas de ataques de ransomware necesitan responder: "¿Debo pagar lo que exigen los ciberdelincuentes?"

Ransomware prevention

Para las empresas, es mucho lo que está en juego. En comparación con los usuarios privados, si una empresa pierde el acceso a sus recursos cruciales, podría llevar a graves pérdidas financieras o al daño de su reputación. Como demostró una *encuesta reciente* de casi 3.000 profesionales de TI y de seguridad cibernética en todo el mundo, una de cada cinco organizaciones ya han experimentado un incidente relacionado con este tipo de amenaza.

Hoy en día, el nivel de cifrado que utilizan los atacantes es tan fuerte como el que usan los bancos para proteger los pagos de sus clientes, por lo que la recuperación de los archivos y dispositivos se complica bastante y, en el peor de los casos, es incluso imposible.

En consecuencia, resulta más barato enfocarse en la prevención que pagar las consecuencias. Si los dispositivos de la empresa no están protegidos y los empleados carecen de la capacitación adecuada, existe un alto riesgo de que, ante una infección de ransomware, los datos valiosos almacenados en los dispositivos de la empresa y, posteriormente, en los discos conectados a ellos a través de redes, se pierdan para siempre.

A. Use la última versión de su software de seguridad

Instale la versión más reciente de su software de seguridad, ya que muchas infecciones se deben al uso de soluciones obsoletas. Si tiene una licencia valida de ESET, actualizar a la última versión no le costará nada.

Si aún está utilizando las versiones 3 o 4 de ESET Endpoint Security, le recomendamos firmemente actualizar a la versión más reciente: la sexta generación de nuestros productos comerciales, que incluye tecnologías de última generación especialmente diseñadas para mejorar la protección de los clientes ante los tipos de malware que utilizan la ofuscación y el cifrado para evadir la detección.

Algunos ejemplos de estas tecnologías incluyen la Exploración avanzada de memoria, que busca conductas sospechosas una vez que el malware se muestra en memoria, y el Bloqueo de exploits, que refuerza la protección contra ataques dirigidos y ataques que aprovechan nuevas vulnerabilidades, también conocidos como ataques *0-day*.

B. Mantenga actualizada la base de datos de virus de su software de seguridad

Las nuevas versiones de ransomware aparecen con frecuencia, por lo que es importante que los equipos y otros dispositivos de la empresa reciban actualizaciones periódicas de la base de datos de virus. Junto con otras medidas, esto ayuda a garantizar que los dispositivos no sean vulnerables a la infección por ransomware. Los productos de ESET comprueban si hay nuevas actualizaciones a cada hora, siempre y cuando la licencia sea válida y haya una conexión a Internet.

C. Habilite el sistema de protección en la nube ESET LiveGrid®

Las aplicaciones desconocidas y potencialmente maliciosas, así como otras posibles amenazas, se monitorean y se envían a la nube de ESET a través del sistema de recopilación de datos ESET LiveGrid. Las muestras recopiladas se verifican automáticamente en el modo sandbox y se someten al análisis de su comportamiento. En caso de confirmar sus características maliciosas, se crean nuevas firmas automatizadas.

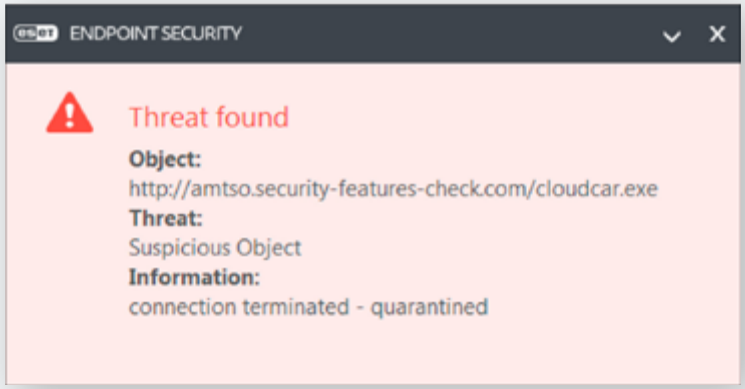
A los clientes de ESET les llegan estas nuevas detecciones automatizadas en cuestión de minutos a través del Sistema de reputación de archivos ESET LiveGrid, sin necesidad de esperar a la próxima actualización de la base de firmas. Si se considera que un proceso determinado es inseguro (como borrar un backup), se bloquea de inmediato. Es importante señalar que ESET LiveGrid solo usa hashes de archivos sospechosos, nunca sus contenidos, respetando así la privacidad de los clientes de ESET.

NOTA IMPORTANTE

Es posible que el firewall de su empresa bloquee las comunicaciones de ESET LiveGrid, por lo que debe comprobar que esté funcionando correctamente. Para ello, visite la siguiente página Web de la reconocida organización evaluadora AMTSO, de la cual ESET es miembro:

http://www.amtso.org/feature-settings-check-cloud-lookups/

Haga clic en el enlace "Download the CloudCar Testfile" (Descargar el archivo de prueba CloudCar) y descargue el archivo de prueba "cloudcar.exe". Si ESET LiveGrid funciona correctamente, el archivo se abrirá en los servidores de ESET y, tras obtener la información necesaria, lo bloqueará. El archivo no se descargará en su equipo y se mostrará el siguiente mensaje:



Cómo mantener sus equipos de escritorio corporativos a salvo

Para mitigar el riesgo de pérdida de datos y daños a los dispositivos como consecuencia de ataques de ransomware, les recomendamos a todas las empresas que sigan estos once pasos.

11 PASOS PARA EVITAR LA PÉRDIDA DE DATOS

1. Realice backups de los datos importantes en forma periódica
2. Instale los parches y actualice su software automática mente
3. No descuide la capacitación de sus empleados en materia de seguridad
4. Configure el equipo para que muestre las extensiones ocultas de los archivos
5. Filtre los archivos adjuntos ejecutables en los mensajes de correo electrónico
6. Deshabilite los archivos que se ejecutan desde las carpetas AppData y LocalAppData
7. Trate de no compartir carpetas
8. Deshabilite el protocolo RDP
9. Use un paquete de seguridad confiable
10. Use la Restauración del sistema para volver a un estado previo conocido sin infecciones
11. Use una cuenta estándar en lugar de una con privilegios de administrador

1. Realice backups de los datos importantes en forma periódica

La mejor medida para derrotar al ransomware incluso antes de que comience su actividad maliciosa es sin duda tener un backup actualizado en forma periódica. Recuerde que el malware también cifra los archivos en unidades de dominio asignadas, es decir, que tengan una letra de unidad asignada, y en ocasiones incluso puede afectar las unidades que están sin asignar.

Esto incluye todos los discos externos como las memorias USB, así como los espacios de almacenamiento en la red o en la nube. Por lo tanto, es esencial establecer un régimen de creación de backups, lo ideal es usar un dispositivo externo y offline para almacenar los archivos de backup.

2. Instale los parches y actualice su software automáticamente

Los creadores de malware con frecuencia se basan en que las personas usan software desactualizado con vulnerabilidades conocidas sin re-parar, lo que les permite usar un exploit e ingresar en forma inadvertida a los dispositivos y sistemas corporativos. Si las empresas se hicieran la costumbre de actualizar el software corporativo con frecuencia, reducirían significativamente la posibilidad de convertirse en víctimas del ransomware.

Algunos fabricantes de software lanzan actualizaciones de seguridad periódicamente. Sin embargo, muchas veces también se emiten actualizaciones no programadas en casos de emergencia. Siempre que sea posible, habilite las actualizaciones automáticas, o vaya directamente al sitio Web del fabricante.

3. No descuide la capacitación de sus empleados en materia de seguridad

Uno de los vectores de infección más comunes es el uso de la ingeniería social, es decir, métodos que se basan en engañar a los usuarios para convencerlos de que abran archivos ejecutables. Mediante el envío de correos electrónicos que se hacen pasar por notificaciones de seguimiento de paquetes de una empresa de logística (como FedEx o UPS), mensajes del banco, o avisos internos de la misma empresa, como New_Wages.pdf.exe (nuevos_salarios.pdf.exe), los atacantes intentan engañar a los empleados para lograr sus objetivos maliciosos. Para evitar que esto ocurra, es necesario capacitar a los empleados de modo que no abran archivos adjuntos ni vínculos de correos electrónicos desconocidos o sospechosos.

4. Configure el equipo para que muestre las extensiones ocultas de los archivos

El ransomware suele llegar en el archivo adjunto de un correo electrónico con la extensión ".PDF.EXE". Esta táctica aprovecha la configuración predeterminada de Windows de ocultar las extensiones de archivo para tipos de archivo conocidos. Al desactivar la opción de ocultar las extensiones, podrá ver la extensión completa de cada archivo y será más fácil detectar archivos sospechosos.

5. Filtre los archivos adjuntos ejecutables en los mensajes de correo electrónico

Si su sistema de exploración para la puerta de enlace de correo electrónico permite filtrar archivos por extensión, puede configurarlo para bloquear los correos con archivos adjuntos ".EXE" o con doble extensión, donde la última extensión sea la del ejecutable (para ello, cuando configure el filtro, seleccione los archivos "*.*.EXE"). También recomendamos filtrar los archivos con las siguientes extensiones: *.BAT, *.CMD, *.SCR y *.JS.

6. Deshabilite los archivos que se ejecutan desde las carpetas AppData y LocalAppData

Una de las conductas típicas de la mayoría de variantes de ransomware es que ejecutan sus archivos ejecutables desde la carpeta AppData o LocalAppData. En consecuencia, es conveniente crear reglas en Windows o mediante el software de prevención de intrusiones para impedir que se ejecuten archivos desde estas carpetas. Si por alguna razón hay algún software legítimo que esté configurado para ejecutarse desde AppData en vez de hacerlo desde Archivos de programa, será necesario crear una excepción para esta regla.

7. Trate de no compartir carpetas

Recuerde que si un dispositivo corporativo se infecta con ransomware, puede provocar el cifrado de todos los archivos guardados en las carpetas compartidas donde tenga permiso de escritura. Por esta razón, los empleados deben tener cuidado con los archivos valiosos y confidenciales que almacenan en discos compartidos, ya que el malware podrá cifrar sus datos en estas ubicaciones, a pesar de que su equipo no esté infectado directamente.

8. Deshabilite el protocolo RDP

El ransomware en general accede a las máquinas de destino mediante el Protocolo de escritorio remoto (RDP), una utilidad de Windows que le permite a un tercero obtener acceso a un equipo de escritorio en forma remota. Además se sabe que los cibercriminales usan sesiones de RDP para entrar a un sistema y deshabilitar el software de seguridad. Una buena práctica es deshabilitar el RDP a menos que sea realmente necesario en el entorno específico. Para deshabilitarlo, consulte los artículos correspondientes de Microsoft Knowledge Base.

9. Use a reputable security suite

Los creadores de malware con frecuencia lanzan nuevas variantes de sus códigos maliciosos como estrategia para evadir la detección, por lo que es importante contar con múltiples capas de protección. Incluso después de que el malware se instala en el sistema, la mayoría necesita recibir instrucciones remotas para llevar a cabo daños graves.

Si aparece una variante de ransomware tan nueva que logra pasar el software antimalware sin ser detectada, es posible que se bloquee cuando intente conectarse con su servidor de Comando y Control (C&C) para recibir instrucciones sobre el cifrado de los archivos. La última suite de seguridad de ESET proporciona un módulo mejorado de Protección ante botnets que bloquea el tráfico malicioso cuando intenta comunicarse con un servidor de C&C.

10. Use la Restauración del sistema para volver a un estado previo conocido sin infecciones

Si la funcionalidad de Restauración del sistema está habilitada en el equipo Windows infectado, es posible llevar el sistema a un estado previo conocido sin infecciones y restaurar algunos de los archivos cifrados desde los archivos de respaldo creados por la Restauración del sistema. Pero es necesario ser más astuto que el malware y actuar con rapidez.

La razón es que algunas de las variantes más nuevas de ransomware también tienen la capacidad de eliminar estos archivos de respaldo. Comenzarán a eliminarlos cada vez que se ejecute el archivo ejecutable, y posiblemente usted ni siquiera se entere de lo que ocurre, dado que estos archivos pueden funcionar sin que el usuario los vea, como parte de las actividades normales de Windows.

11. Use una cuenta estándar en lugar de una con privilegios de administrador

Siempre es un riesgo de seguridad usar una cuenta con privilegios de administrador del sistema, ya que le permite al malware ejecutarse con permisos elevados y así puede infectar el sistema con facilidad. Asegúrese de que los usuarios utilicen siempre una cuenta de usuario limitada para las tareas diarias regulares, y la cuenta de administrador del sistema solo cuando sea absolutamente necesario. No deshabilite el Control de acceso de usuarios (UAC).

CÓMO OPERA EL RANSOMWARE

El Ransomware es un tipo de software malicioso capaz de bloquear el dispositivo y secuestrar los archivos que pueden llegar a tener algún valor personal o profesional para el usuario.

El Malware se suele propagar a través de correos electrónicos o al visitar sitios Web infectados. Tras hacer su trabajo malicioso, el Ransomware genera un mensaje emergente con el pedidode rescate.

Qué hacer si uno de los equipos de escritorio de su empresa ya está infectado.

Desconecte el dispositivo

Si usted o alguno de sus empleados ejecuta un archivo sospechoso y luego encuentra dificultades para abrir algunos de los archivos almacenados, desconecte de inmediato el dispositivo de Internet y de la red corporativa y, si es posible, también de la red eléctrica. De esta forma se puede impedir la comunicación entre el software malicioso y su servidor de C&C antes de que finalice el cifrado de los datos almacenados en dicho dispositivo y en todas las unidades asignadas.

Aunque esta técnica no es infalible, al menos le da a su empresa una oportunidad de salvar algunos de los archivos importantes antes de que se terminen de cifrar. Recomendamos apagar el hardware, dado que el ransomware puede haber sido programado para sobrevivir el apagado del software y seguir causando más daños.

Póngase en contacto con el soporte técnico de ESET

Si el ransomware ya ha completado sus tareas maliciosas y la empresa no cuenta con una copia de seguridad funcional, póngase en contacto con el soporte técnico de ESET. No se olvide de adjuntar el registro obtenido del Recopilador de registros de ESET y algunas muestras de los archivos cifrados (si es posible, envíe aproximadamente cinco archivos de MS Word o MS Excel).

Si su licencia de ESET abarca 100 equipos o más, deberá emitir un ticket a través de nuestro sistema online. A continuación, nuestros especialistas se comunicarán con usted y le pedirán más información sobre la infección. Junto con el Laboratorio de ESET de investigación de malware, nuestros especialistas intentarán descifrar y recuperar los archivos afectados.

No obstante, recuerde que los creadores del código malicioso han hecho todo lo posible para que el ransomware sea efectivo, y el cifrado que usan es cada vez más fuerte y avanzado. Por lo tanto, en general es imposible lograr descifrar todo, o hacerlo rápidamente.

Hoy en día, el cifrado constituye un estándar tecnológico para la protección de transferencias bancarias y financieras, transacciones en tiendas de comercio electrónico y muchos otros servicios online, y las últimas versiones disponibles son prácticamente impenetrables. Por esta razón, ningún fabricante puede garantizarle que va a recuperar sus archivos.

Los expertos de ESET intentarán encontrar fallas en el ransomware que permitan reparar los daños causados a los discos y dispositivos afectados. Si tienen éxito, le proporcionarán una herramienta de descifrado hecha a medida para su negocio.

Basándonos en nuestra propia experiencia, podemos decir que este resultado se da en uno de cada cinco casos de infecciones de ransomware. El proceso de descifrado puede tardar hasta varias semanas, según las habilidades de los autores del malware. También es posible que el intento resulte infructuoso. Si ha optado por el soporte Premium de ESET, nuestros especialistas estarán disponibles para responder a sus inquietudes las 24 horas, los 365 días del año.

No se olvide de los dispositivos Android de la empresa

Como ya hemos mencionado, los ciberdelincuentes no atacan exclusivamente a sistemas Windows. En los últimos años, el foco de su atención ha pasado al *sistema operativo móvil dominante, Android*, que es utilizado por muchos smartphones y tabletas corporativos.

ESET ya encontró varias familias de ransomware para Android diseñadas específicamente para atacar dispositivos móviles. Los atacantes utilizan diversas técnicas, haciéndose pasar por un software antivirus o por una agencia policial local que bloquea el dispositivo hasta que el usuario pague lo que exige (un ejemplo de este tipo de ransomware es *Reveton*).

En 2014, nuestros investigadores encontraron el primer ransomware que intentaba *cifrar los datos de dispositivos móviles Android*. Desde entonces, los atacantes han diseñado más de 50 variantes, cada una más peligrosa y avanzada que la anterior. Tan solo un año más tarde, apareció *el primer ransomware que bloqueaba el acceso a un dispositivo* mediante la generación de una secuencia de cuatro dígitos aleatorios para bloquear la pantalla.

Hay que recordar que todos estos códigos maliciosos lograron bloquear en forma efectiva el acceso a recursos vitales para las actividades laborales diarias, y les exigían a las víctimas y a sus empresas el pago de cientos de dólares para restaurar el acceso.

CÓMO MANTENER LOS DISPOSITIVOS ANDROID A SALVO

A. Capacite a sus empleados

Es importante que los empleados que usan dispositivos Android estén al tanto de las amenazas de ransomware y que tomen medidas preventivas. Por consiguiente, es una medida de prevención fundamental.

- Entre las cosas principales a tener en cuenta, es importante evitar las tiendas de aplicaciones móviles no oficiales o de terceros.
- Antes de que los empleados descarguen algo de la tienda oficial, deben leer los comentarios de otros usuarios. Los usuarios en seguida identifican las conductas maliciosas de los programas y publican comentarios al respecto directamente en la página de la aplicación.
- Los empleados siempre deben comprobar si los permisos solicitados por la aplicación son necesarios para su correcto funcionamiento.
- Si es posible, cree una lista blanca de las aplicaciones móviles permitidas para los dispositivos Android de la empresa.

B. Use un software de seguridad

Instale una aplicación móvil de seguridad en todos los dispositivos Android de la empresa y manténgala siempre actualizada. Si usted es un cliente de ESET, puede instalar ESET Endpoint Security para Android como parte de los siguientes paquetes de seguridad para empresas:

- ESET Endpoint Protection Standard
- ESET Endpoint Protection Advanced
- ESET Secure Business
- ESET Secure Enterprise

C. Haga backups de todos los datos importantes

Además, es importante tener backups funcionales de todos los datos importantes de cada dispositivo Android. Lo más probable es que los usuarios que toman las medidas adecuadas contra el ransomware nunca se vean afectados por ningún pedido de rescate. Incluso si llegan a ser víctimas y, en el peor de los casos, sus datos terminan cifrados, si tienen una copia de seguridad, la experiencia no será nada más que una molestia.

Qué hacer si uno de los dispositivos Android de su empresa ya está infectado

Si su dispositivo o el dispositivo de un empelado se infecta con ransomware, tiene varias opciones para eliminarlo, según la variante específica de malware.

1. Arranque el dispositivo en modo seguro

Para la mayoría de las familias simples de ransomware de bloqueo de pantalla, la solución es reiniciar el dispositivo en modo seguro (para que las aplicaciones de terceros, incluyendo el malware, no se carguen), con lo que el usuario podrá desinstalar fácilmente la aplicación maliciosa. Los pasos para arrancar el dispositivo en modo seguro pueden variar según el modelo. Para conocer cuáles corresponden a su dispositivo, consulte el manual o búsquelos en Google.

2. Revoque los privilegios de administrador para el malware

En el caso de que la aplicación haya conseguido privilegios de administrador de dispositivos (lo que suele ser el caso con las nuevas variantes de ransomware, cada vez más agresivas), éstos deberán ser revocados desde el menú de ajustes antes de poder desinstalar la aplicación.

3. Restablezca la contraseña desde Mobile Device Management (Administración de Dispositivos Móviles)

Si un ransomware con derechos de administrador de dispositivos bloqueó el dispositivo 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 de MDM (Administración de Dispositivos Móviles) alternativa. Los teléfonos Android liberados tienen aún más opciones.

4. Póngase en contacto con el soporte técnico

Si un ransomware criptográfico como Android/Simplocker cifró los archivos del dispositivo, les aconsejamos a los usuarios que se pongan 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.

5. Restablecimiento a los valores de fábrica

El restablecimiento a los valores de fábrica, que borra todos los datos del dispositivo, puede usarse como último recurso en caso de que las soluciones anteriores no estén disponibles.

Y por último pero no menos importante: ¿Debo pagar el rescate?

ESET les recomienda a sus clientes corporativos (así como a todos los demás usuarios) que **nunca paguen los rescates**.

En primer lugar, los atacantes no están actuando legalmente, por lo que no tienen ninguna obligación de cumplir con su parte del trato. Nada garantiza que descifren los datos afectados o desbloqueen el dispositivo a cambio del pago.

Por otro lado, el pago de los rescates también ayuda a los ciberdelincuentes a financiar sus actividades maliciosas en curso.

Además, aunque los autores del malware efectivamente le proporcionen la clave de descifrado, no hay ninguna garantía de que funcione. ESET ha visto muchos casos en los que la herramienta enviada por los atacantes no logró descifrar los archivos, o solo lo hizo de manera parcial. En algunos casos de ransomware para Android, el código PIN generado aleatoriamente para bloquear la pantalla del dispositivo no fue enviado al cibercriminal y, por tanto, no hay ninguna forma de desbloquearlo.

Por último, si usted les paga a los delincuentes, ¿cómo sabe que no van a volver por más? Si tuvieron éxito al atacar su empresa, es posible que la consideren débil y traten de volver a aprovecharse.