¿ Qué es realmente **el ransomware?**

Guía G DATA

¿Qué tienes en tu computadora? ¿Correos electrónicos importantes, archivos secretos de la oficina o incluso fotos antiguas de sus hijos? Durante el transcurso de la vida de una computadora, se acumula en el disco duro una gran cantidad de datos que pueden ser personales, tal vez incluso relacionados con el negocio, pero en cualquier caso confidenciales. Y eso es lo que te hace vulnerable al chantaje. Si en lugar de su pantalla de inicio habitual, de repente solo aparece una calavera o una carta de chantaje en su monitor, probablemente se trate de un ransomware.

¿Qué significa "ransomware"?

“Ransomware” hace exactamente lo que dice: retiene datos o sistemas para pedir rescate. Los expertos a veces también hablan de troyanos de encriptación: el esquema de rescate se basa en el hecho de que este tipo de ransomware encripta los datos del usuario. Los otros nombres indican cómo funciona el ransomware. Se abre camino en el sistema, a menudo disfrazado como un programa legítimo, y el usuario se da cuenta con horror de que la computadora ha sido bloqueada.

¿Cómo varían los distintos tipos de ransomware entre sí?

En general, hay dos tipos diferentes de ransomware:
Bloqueadores de pantalla y Encriptadores de archivos.

Los bloqueadores de pantalla bloquean la pantalla.

Mientras que los encriptadores de archivos encriptan los datos en la computadora, tomando fotos de niños, archivos de texto y carpetas importantes como "rehenes".

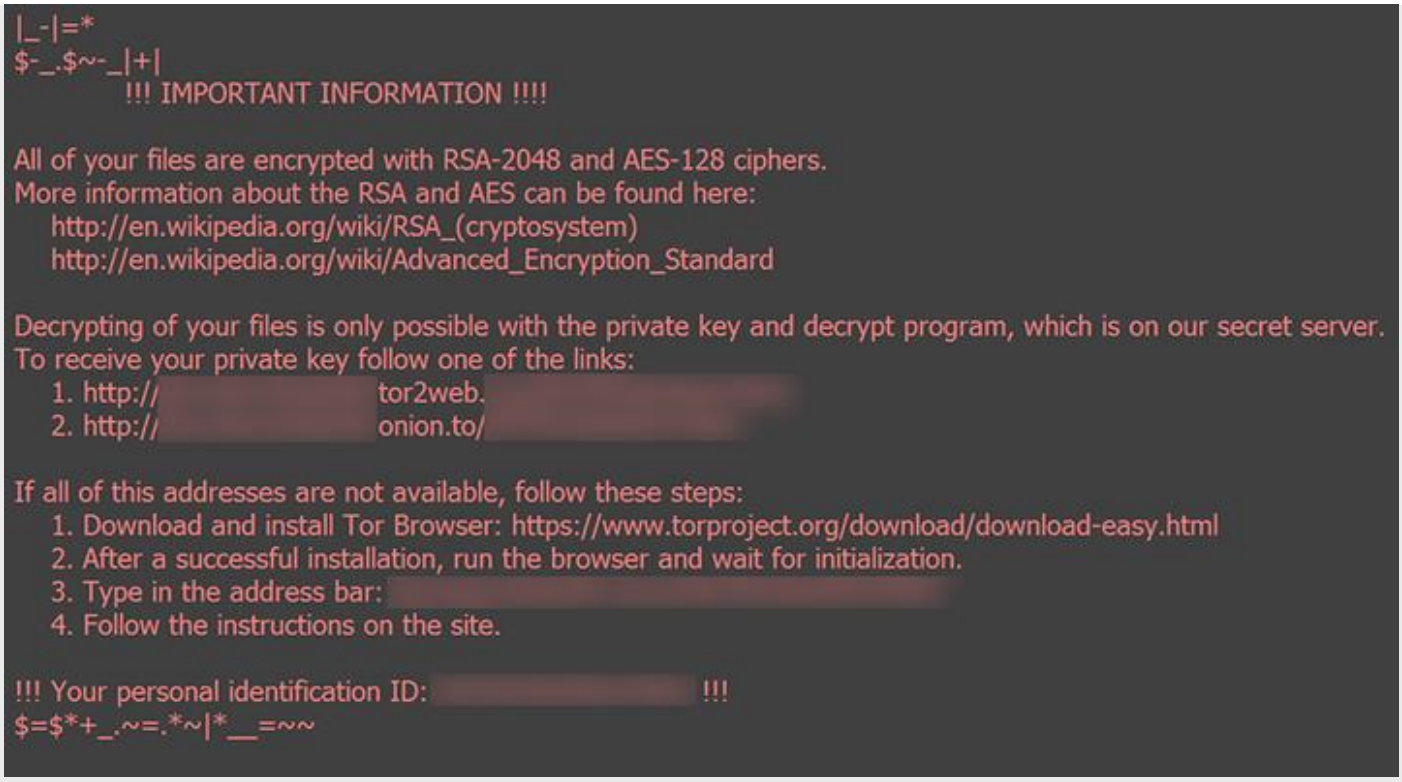
Por eso, los expertos también llaman a estos últimos "troyanos de cifrado".

¿Cómo se da a conocer el ransomware?

Generalmente, una pantalla bloqueada o una nota de rescate que no se puede eliminar es lo primero que ve el usuario del ransomware. Algunas variantes de ransomware tienen un período de incubación, lo que significa que los efectos maliciosos solo se ven cuando el usuario ya no puede recordar cuándo y dónde podría haber recogido un troyano de rescate.

Idealmente, el malware puede ser detectado por un escáner de virus y aparecer como un resultado de escaneo positivo. Sin embargo, las personas que no tengan una solución antivirus instalada solo notarán el ransomware cuando ya sea demasiado tarde. Como muchos troyanos de rescate se eliminan a sí mismos después de ejecutar su función maliciosa, es un verdadero desafío para el software de seguridad detectar el malware. Lo primero que ve el usuario de la computadora del ransomware es una ventana de información con una solicitud de pago que no se puede eliminar.

Ejemplos de ransomware



bloqueado

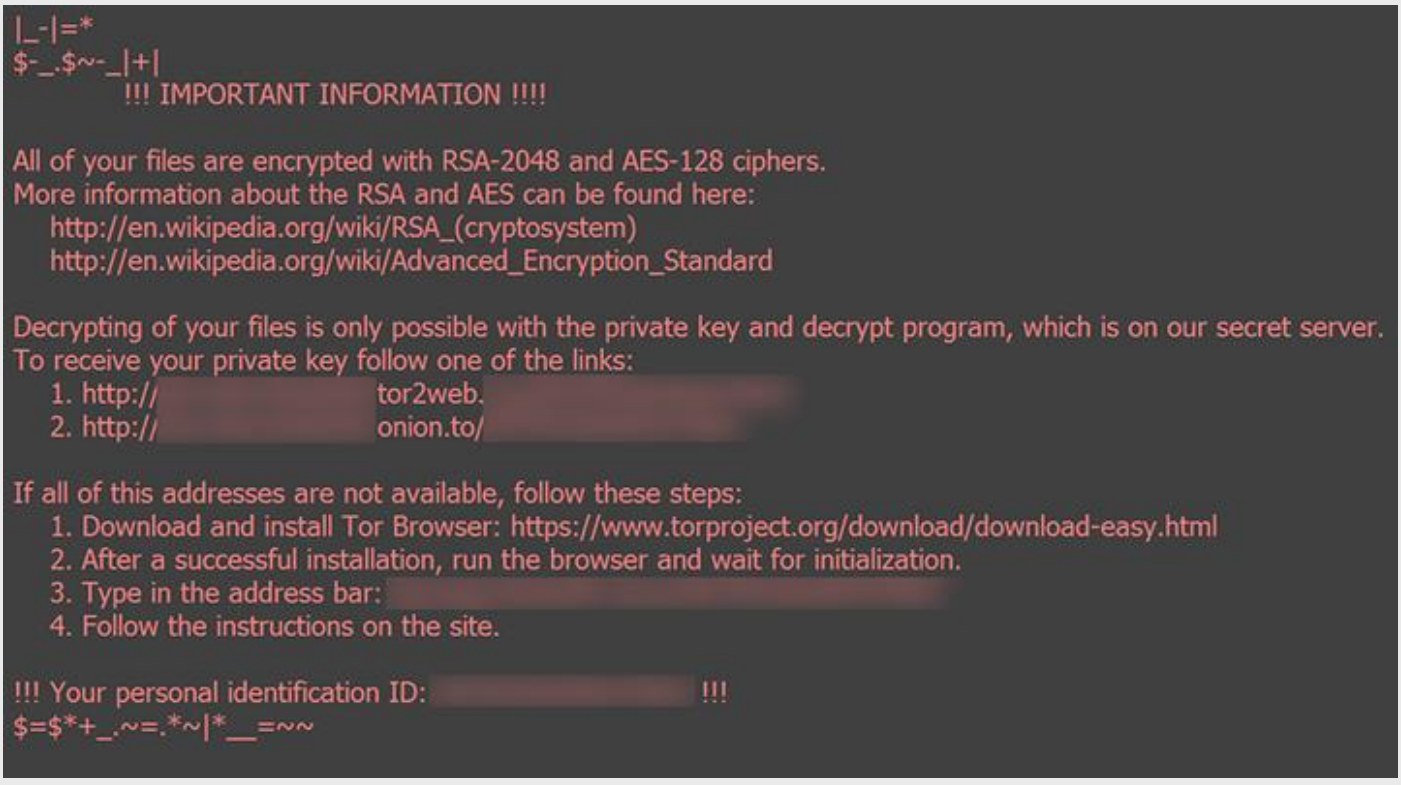
Un ejemplo bien conocido de este tipo de cifrado de archivos es Locky, que ha afectado a innumerables ordenadores Windows y Apple desde principios de febrero de 2016, principalmente en Alemania. Sin embargo, también se han encontrado casos de Locky en los Estados Unidos. Los perpetradores obtuvieron más de 15.000 euros de dos hospitales estadounidenses cuyos documentos médicos había cifrado el malware. Según los informes de los medios, los hospitales alemanes también se vieron afectados por los troyanos de rescate.

Quiero llorar

En la madrugada del 12 de mayo de 2017 se detectó una ola masiva de infección que infectó PCs y redes con la última versión de WCry/WannaCry - Ransomware. En España, un importante proveedor de telecomunicaciones se vio afectado. Se infectó un servidor interno en Telefónica, entre cuyas empresas también se encuentran los proveedores alemanes de telefonía móvil EPlus y O2. La situación se intensificó hasta el punto en que se instó a los empleados a apagar sus PC de inmediato y cortar cualquier conexión VPN para detener la propagación del malware. Según el diario español El Mundo, algunas empresas de servicios públicos también se vieron afectadas por la ola de infección. Según una fuente de datos, el número de infecciones fue mayor en Rusia.

Petia

Petya spreads when a unsuspecting user opens a dropbox file: In some cases Petya had been hidden in a dropbox file, which were supposed to contain a job application. Instead of an application of a candidate ransomware set in the dropbox. This is the most common phishing technique, that tricks users into unknowingly download Petya. When he later clicks on the downloaded file, he gets Petya started - and Petya spreads through the entire systems. So Petya is reliant on the help of the user. Unlike Locky Petya does not encrypt the files, but blocks the access to the data. Thereby, the computer does not know where the files lie and if they still exist on the hard disk.



Locky

A well-known example of such a file encrypter is Locky, which has been afflicting countless Windows and Apple computers since early February 2016, mainly in Germany. However, Locky cases have also been found in the USA. The perpetrators obtained over 15,000 Euros from two American hospitals whose medical documents the malware had encrypted. According to media reports, German hospitals were also affected by ransom Trojans.

WannaCry

En la madrugada del 12 de mayo de 2017 se detectó una ola masiva de infección que infectó PCs y redes con la última versión de WCry/WannaCry - Ransomware. En España, un importante proveedor de telecomunicaciones se vio afectado. Se infectó un servidor interno en Telefónica, entre cuyas empresas también se encuentran los proveedores alemanes de telefonía móvil EPlus y O2. La situación se intensificó hasta el punto en que se instó a los empleados a apagar sus PC de inmediato y cortar cualquier conexión VPN para detener la propagación del malware. Según el diario español El Mundo, algunas empresas de servicios públicos también se vieron afectadas por la ola de infección. Según una fuente de datos, el número de infecciones fue mayor en Rusia.

¿Qué importancia tiene el tema de la protección de datos para los usuarios?

... de todos los usuarios en todo el mundo **nunca han realizado una copia de seguridad** de su sistema.

Fuente: Día Mundial de la Copia de Seguridad

... de todos los participantes de la encuesta tienen miedo de **perder fotos y videos.**

Fuente: Encuesta Acronis

... de todos los usuarios utilizan **discos duros externos** para el almacenamiento de sus datos.

Fuente: Encuesta Kroll Ontrack

¿Cómo es posible que haya recogido ransomware?

Lo complicado del ransomware es que, como la mayoría de los troyanos, se esconde detrás de enlaces o formatos de archivo aparentemente inofensivos. El troyano de cifrado Petya, por ejemplo, se distribuye cuando los usuarios desprevenidos abren un archivo de Dropbox. El usuario descarga el malware al hacerlo. Si luego hace clic en el archivo descargado a su PC, ejecuta el archivo y Petya comienza a distribuirse por todo el sistema. Por lo tanto, Petya depende de la asistencia involuntaria del usuario, quien cree que está abriendo un archivo estándar pero en realidad está activando la instalación del ransomware.

Esto significa que sus vías de distribución apenas difieren de las de otros tipos de malware. Los archivos a menudo ingresan a la computadora a través de un sitio web manipulado, al que se accede a través de un enlace en un correo electrónico no deseado o un mensaje en una red social. A veces, los perpetradores envían sus propios correos electrónicos que contienen un supuesto recordatorio o una nota de entrega. Sin embargo, en realidad, hay malware en lugar de información importante escondida en el archivo adjunto.

¿Cuánto tiempo ha existido el ransomware?

Chantajear a los usuarios de PC de esta manera no es nada nuevo. El primer ransomware documentado, el disco troyano AIDS, circuló en 1989 y se distribuyó a través de un disquete en ese momento. El biólogo evolutivo y graduado de Harvard, Joseph L. Popp, envió 20 000 disquetes infectados con el encabezado "Información sobre el SIDA - Disquete introductorio" a los participantes de la Conferencia Internacional sobre el SIDA de la Organización Mundial de la Salud y así introdujo de contrabando el ransomware en sus computadoras. El malware reemplazó un archivo de configuración del sistema (autoexec.bat) y, después de noventa reinicios, comenzó a encriptar el disco duro. Para volver a acceder a los datos, las víctimas tenían que enviar 189 dólares estadounidenses a una empresa llamada PC Cyborg en Panamá, razón por la cual el primer ransomware también se conocía como el troyano PC Cyborg.

¿Qué sucede exactamente cuando el ransomware ingresa a la computadora?

Al hacer clic en un enlace en un correo electrónico a un sitio web o Dropbox, se activa la descarga de un instalador: así es como el troyano de cifrado Petya infectó con éxito tantas computadoras en la primavera de 2016. Petya obliga a la computadora a reiniciarse y luego reemplaza el registro de arranque maestro (MBR) con una rutina de carga maliciosa. Luego, Petya obliga a la computadora a reiniciarse nuevamente y finge al usuario que se está verificando la estructura del sistema de archivos, como es el caso, por ejemplo, después de un bloqueo del sistema. Pero Petya, de hecho, no está comprobando la eficiencia funcional del sistema. Petya no cifra los datos en sí, solo los hace inaccesibles para el usuario. La computadora ya no puede detectar los archivos y ni siquiera puede determinar si todavía están allí. Después de otro reinicio forzado, aparece la pantalla de bloqueo con las demandas de los chantajistas. Con muchos tipos de ransomware, en esta etapa es difícil descifrar los archivos sin realizar un pago. Petya, sin embargo, ahora se ha descifrado, por lo que ya nadie necesita hacer un pago de rescate para descifrar sus datos nuevamente.

¿Cómo funciona el ransomware?

Inicialmente, los programas de rescate se usaban principalmente para bloquear los escritorios de PC individuales. Hoy en día, estos ataques bastante pequeños se han vuelto bastante raros. Los programas de encriptación se encuentran mucho más a menudo que estos bloqueadores de pantalla en estos días. Con estos, los contenidos del disco duro se cifran de tal forma que el usuario ya no puede acceder a ellos. Por lo general, en la pantalla de bloqueo se muestra un sitio web o una máscara de formulario que explica las demandas y los métodos de pago. Los chantajistas prometen que volverán a descifrar los datos después de que se haya recibido el pago.

Los perpetradores más endurecidos amenazan con eliminar los datos de forma permanente si la víctima contacta a la policía. Ahora incluso hay ransomware que elimina archivos cifrados por cada hora que no se realiza el pago. Y para evitar que el usuario aproveche la amenaza apagando la PC, el software elimina mil archivos cuando se reinicia el sistema.

¿Y cómo ha cambiado la situación de las amenazas desde entonces?

El primer troyano de cifrado distribuido a través de la red fue TROJ_PGPCODER.A. Los chantajistas exigieron varios cientos de dólares para descifrarlo. Eso fue en 2005. Desde 2011, los expertos en seguridad han registrado un rápido aumento en los ataques de ransomware. La Oficina Federal Alemana para la Seguridad de la Información (BSI) advirtió: "Desde mediados de septiembre de 2015, la situación de amenaza del ransomware se ha intensificado significativamente". Especialmente en Alemania, los escáneres de virus se han encontrado cada vez más con ransomware desde principios de 2016, agregó BSI. Las soluciones de seguridad encontraron más de 10 veces más ransomware en Alemania en febrero de 2016 en comparación con octubre de 2015. Esta tendencia también se observa en el resto del mundo: globalmente, la cantidad de detecciones se ha multiplicado por 6 durante este período.

¿Cómo ganan dinero exactamente los chantajistas con esto?

El aumento en la cantidad de archivos de ransomware que circulan se debe al hecho de que ahora son tan fáciles de producir. Hay los llamados kits de crimeware en Darknet que se pueden usar para armar malware en un principio modular. También es muy fácil y económico programar ransomware, o hacer que lo programen. Los delincuentes ponen un poco de dinero para generarlo, pero pueden recuperar mucho en el mejor de los casos. Los perpetradores informan a las víctimas de las opciones de pago a través de la pantalla de bloqueo. A los ciberdelincuentes se les paga a través de tarjetas Paysafe o Ukash o con la moneda en línea Bitcoin. El rescate ronda los 400 euros en muchos casos. Sin embargo, a veces se exigen varios miles de euros para el descifrado. Depende de la importancia de los datos, como con el chantaje a los hospitales con Locky. Cuando la víctima haya hecho el pago,

¿Cómo puedo protegerme?

- **Copias de seguridad** : la mejor protección contra el ransomware es realizar copias de seguridad periódicas . Estos deben almacenarse en un medio separado del sistema. Si ejecuta una copia de seguridad en un disco duro externo, elimínelo después de la copia de seguridad y asegúrese de que este medio de almacenamiento esté fuera de línea a menos que sea necesario. Con copias de seguridad regulares, puede asegurarse de no perder ningún dato en caso de una infección real de ransomware y puede restaurar fácilmente su sistema. Al hacerlo, asegúrese de utilizar un medio seguro, como un CD, que tampoco pueda infectarse.

Una solución de software segura es vital. Idealmente, debería contener mecanismos de protección como monitoreo de comportamiento y otras tecnologías proactivas.

- **Sistema operativo** : además de esto, se deben realizar actualizaciones periódicas de su sistema operativo. De esta forma puedes cerrar agujeros de seguridad. Lo mismo se aplica a su navegador y cualquier otro software instalado en su sistema.
- **Protección del navegador** : la protección del navegador también es útil para protegerlo de secuencias de comandos peligrosas y de descargas accidentales de malware.
- **Protección de correo electrónico** : los correos electrónicos falsos y fraudulentos se pueden proteger mientras aún están en su bandeja de entrada a través de un software de seguridad especial. De esa manera, tales correos electrónicos ya no son un problema. El software antivirus también detecta malware como troyanos y lo elimina.
- **Ransomware-Cleaner** : existe una solución de software contra los bloqueadores de pantalla, que lo ayuda a eliminar la pantalla de bloqueo y la amenaza por igual.
- **Cuenta de usuario** : también se puede prevenir una infección si el usuario no inicia sesión con su cuenta de administrador en todo momento, sino que configura una cuenta de invitado en su lugar. Como esta cuenta tiene menos derechos, el ransomware no puede penetrar tan profundamente en el sistema e, idealmente, no causará ningún daño.
-

¿Los perpetradores realmente descifrarán mis datos si pago el rescate?

Siempre se recomienda precaución y escepticismo cuando se trata de delincuentes. Muchos de los delincuentes no tienen ningún interés en el juego limpio desde el principio, y algunos ni siquiera han hecho planes para una opción de descifrado. Para ellos todo se trata del dinero. Cualquiera que no haya hecho una copia de seguridad inevitablemente perderá sus archivos después de que la computadora haya sido infectada con ransomware. Por lo tanto, hay algo que aprender de las películas de acción: no negocie con los chantajistas.

La Oficina Federal Alemana para la Seguridad de la Información (BSI) desaconseja dar seguimiento a las demandas. Nadie debe esperar ser tratado justamente por los delincuentes. Además, cualquiera que pague un rescate con tarjeta de crédito está convirtiendo su cuenta en una tienda de autoservicio. Un chantajista también puede exigir repentinamente más dinero para liberar los datos, o encriptar los datos una vez más en una fecha posterior a través de una puerta trasera en el sistema y exigir más dinero, incluso si al principio parece que cumplió su promesa y liberó los datos. Por lo tanto, pagar un rescate es un riesgo en múltiples niveles.

¿Qué debo tener en cuenta si quiero pagar el rescate?

Si desea pagar el rescate a pesar de todas las advertencias, no debe eliminar de antemano ninguno de los componentes del ransomware de la PC. Dependiendo de las circunstancias, esta puede ser la cerradura en la que debe colocar la llave que puede recibir después de realizar el pago. Sin un bloqueo, el código de descifrado podría quedar inutilizable, y sus datos permanecerán cifrados irremediablemente. Además, los componentes pueden ser importantes en el caso de que las autoridades investigadoras logren devolver el golpe a los ciberdelincuentes; a menudo hay descifradores que pueden ayudar a los afectados a recuperar sus datos sin realizar un pago. La información contenida en los componentes se requeriría entonces para generar la clave de recuperación.

Si realmente recibió una clave y pudo descifrar sus archivos con ella, debe eliminar inmediatamente el ransomware de su computadora. Sin embargo, nunca debes perder de vista el hecho de que los delincuentes no se sienten obligados contigo de ninguna manera y que es posible que hayas perdido dinero y datos. También manténgase al día con las maquinaciones de los criminales. Porque si nadie les paga, la distribución de ransomware ya no valdrá la pena para los delincuentes.

¿Cómo elimino el ransomware?

Si se ha convertido en víctima de un ataque a pesar de sus mejores esfuerzos, solo una cosa ayudará: eliminar el malware de su computadora. La forma más confiable y completa de eliminar el ransomware es restablecer el sistema a la configuración de fábrica. Antes de elegir esta opción, debe tener en cuenta que todos los archivos en la computadora se perderán irremediablemente después. Alternativamente, si ha realizado copias de seguridad regulares del sistema, puede restablecer su sistema a un punto en el tiempo antes de que ocurriera la infección. Seleccione el punto de restauración más reciente. Al hacerlo, siempre debe asegurarse de que este punto sea efectivamente anterior al momento de la infección. De esta manera, puede librar su computadora del malware.

Ransomware en detalle
– Experiencia en el tema –

Troyanos de cifrado

Un troyano de encriptación o cripto-troyano encripta archivos en la computadora y requiere rescate para desencriptarlos. Algunas familias de troyanos cifran solo ciertos tipos de archivos, como imágenes, documentos o películas. Otros encriptan todos los tipos de archivos y ahorran solo unas pocas carpetas. Las familias populares son CryptoLocker (ya no está activa), CryptoWall, CTB-Locker, Locky, TeslaCrypt y TorrentLocker. Una forma bastante nueva es Petya. En lugar de cifrar archivos individuales, cifra la tabla maestra de archivos (la tabla de contenido) del disco duro. Después de lo cual los archivos ya no se pueden encontrar en el disco duro.

Bloqueo de aplicaciones

Este tipo de ransomware chantajea a los usuarios impidiendo el acceso a aplicaciones y programas. Por ejemplo, se bloquea el navegador o el acceso a la gestión del almacenamiento en red (NAS). En algunos casos, se pueden anular con herramientas estándar. Solo hay unas pocas familias de malware de este tipo, un ejemplo es Synolocker. El nombre se deriva del hecho de que la empresa de malware tiene como objetivo productos de Synology, un fabricante de soluciones NAS.

Bloqueador de pantalla

Un bloqueador de pantalla bloquea el acceso a la computadora al mostrar una pantalla de bloqueo que se mueve constantemente al primer plano y también puede terminar otros procesos. Como resultado, la computadora ya no puede ser operada. La familia más conocida en esta categoría es Reveton, también conocida como BKA-Trojans, GEZ-Trojans o FBI-Trojans.

Híbridos

También hay ransomware que combina screenlocker y encriptación. Esto hace que restaurar los datos requiera aún más tiempo. También aquí hay solo unas pocas categorías, por ejemplo, Quimera.

¿Qué puede hacer el software contra el ransomware?

- **Detección basada en firmas mediante un escáner de virus**

  Para las familias de Ransomware ya conocidas, la detección más simple y efectiva es por firma. Las firmas reconocen en el código de un archivo las secuencias de comandos que son responsables de las acciones maliciosas y son típicas de un grupo o familia particular de malware. Un signo inequívoco para la detección de ransomware es la visualización de un nombre de firma como Trojan-Ransom y el apellido como Win32.Trojan-Ransom.Petya.A. Actualmente distinguimos más de 120 familias de ransomware. Entre ellos, nombres tan destacados como Cryptowall, Locky, CTB-Locker y CryptXXX.

  Las firmas no solo pueden reconocer las acciones típicas de Ransomware. El malware a menudo se detecta mediante secuencias de código universales que son típicas para la compresión, el cifrado, las rutinas de descarga, las actividades de puerta trasera, los mecanismos de camuflaje y mucho más. Las firmas heurísticas y genéricas reconocen este tipo de secuencias de comandos generalmente válidas incluso en familias previamente desconocidas.

- **Tráfico de red**

  Muchas familias de ransomware solo se activan cuando se comunican con su servidor de control y reciben comandos. Una vez que se conocen los servidores de control, puede bloquear el acceso a ellos. Si no se puede establecer la comunicación con el servidor de control, el ransomware permanece inactivo. Además, la forma en que se establece la conexión y cómo se transmiten los datos son típicos de Ransomware y pueden detectarse y bloquearse.

- **Detección de comportamiento**

  La detección basada en el comportamiento supervisa todas las aplicaciones en ejecución en busca de actividad sospechosa. Si un programa malicioso ha conseguido entrar en el ordenador, previene posibles daños. La detección está diseñada para detectar las primeras acciones de malware. Varias familias de ransomware se propagan a través de sitios web manipulados o pancartas dañinas. Usan agujeros de seguridad (engl. to exploit), para secuestrar las computadoras cuando visitan el sitio web.

La forma en que se producen estos ataques muestra acciones típicas en el sistema que son detectadas por métodos especiales de protección basados en el comportamiento. Si los indicadores individuales no son suficientes, también se utilizan combinaciones y secuencias de diferentes áreas para la evaluación.

- **Comportamiento de instalación**

Cuando el ransomware ha infectado un sistema, se llevan a cabo procesos característicos mediante los cuales se puede detectar el malware. A menudo, la infección ocurre sin una ventana visible. En muchos casos, el sistema se examina en el primer paso antes de cargar más software. Se crean archivos de configuración típicos y/o entradas de registro, por nombrar solo algunos ejemplos.

- **Persistencia**

Para volver a activarse después de reiniciar la computadora, el Ransomware debe usar uno de los muchos mecanismos de inicio automático. Este procedimiento sigue patrones típicos. Estos pueden ser reconocidos por ciertas actividades del sistema y terminados. Se considera altamente sospechoso cuando se cifran muchos archivos individuales. Si se agregan más características, como un proceso desconocido o una ventana no visible, la acción finaliza.

- **Ataques desde la Web**

En muchos casos, el ransomware se distribuye a través de sitios web u otros servicios de Internet. La nube de URL de G DATA se actualiza constantemente con las URL actuales que se sabe que distribuyen malware. Si se sabe que un sitio es dañino, nuestro software bloquea el acceso. Además, todos los datos que ingresan al navegador se verifican en busca de malware, ya sean descargas de archivos o scripts activos en el sitio web.

- **Protección contra el spam**

Los correos electrónicos también se utilizan a menudo para distribuir ransomware. Antes de que los demás mecanismos de protección, como la protección web y los escáneres de virus, comprueben el contenido del correo, el correo debe entregarse en el buzón. Nuestra excelente protección contra correo no deseado con tecnología OutbreakShield detecta correos electrónicos maliciosos mientras están en tránsito, en función de cómo se propagan. El correo electrónico con contenido dañino a menudo no se entrega o se elimina del buzón.

- **Foco en Ransomware en los sistemas de análisis de SecurityLabs**

En G DATA SecurityLabs se analizan diariamente cientos de miles de archivos. Los procedimientos de búsqueda en los sistemas de análisis automático están diseñados para identificar tanto malware como sea posible. También podemos utilizar métodos que los clientes no suelen utilizar porque, por ejemplo, son demasiado intensivos desde el punto de vista computacional. Cuando los resultados son claros, los mecanismos de protección, como las URL y las listas negras de archivos en la nube, se actualizan automáticamente y se crean firmas para los detectores de virus.

Las muestras sospechosas que todavía son dudosas son evaluadas por los analistas de malware. En estos procesos comunes, hemos incluido métodos de detección especiales con los que Ransomware se detecta inmediatamente y luego se procesa con alta prioridad. Además, se analiza con especial intensidad la metodología Ransomware. Estos análisis son la base para las firmas heurísticas, para los filtros de URL de los nombres de dominio recién generados o para la adición de reglas para la detección basada en el comportamiento.