Guía de prevención y respuesta frente a ataques de ransomware

Anexo II. Familias de ransomware

Carlos Alberto Crego Sánchez
Master en Ciberseguridad y Privacidad
Privacidad

Albert Jové Canela
Cristina Pérez Sola

28 de diciembre del 2021

Índice

Lista de figuras

Anexo II. Familias de ransomware

Aunque los expertos en ciberseguridad prefieren clasificar el ransomware en familias de acuerdo con la firma del código, en este anexo se abordarán las familias de ransomware más destacadas desde 2016 y profundizaremos un poco en sus particularidades.

1. Ryuk

Apareció por primera vez en agosto de 2018, se trata de un ransomware de cifrado especializado en ataques dirigidos contra grandes empresas ya que el coste del rescate promedio exigido se encuentra entre 15 BTC y 50 BTC.

Tras analizar el código fuente de Ryuk, los investigadores descubrieron que comparte muchas similitudes con el ransomware Hermes1 ya que ambos emplean un algoritmo de cifrado similar y se distribuye mediante campañas de spam y exploit kits [1].

En los primeros 2 meses, Ryuk había ingresado 640.000$ de empresas de todo el mundo y 3 meses después, el número había aumentado a 3.7 millones de dólares en Bitcoin. Los autores de Ryuk usaron una dirección de Bitcoin única para cada víctima y dividieron el dinero del rescate recibido entre varias cuentas de Bitcoin para hacer que el rastreo sea casi imposible.

Como se ha mencionado anteriormente, Ryuk se utiliza para ataques dirigidos lo que significa que los atacantes necesitan recopilar información técnica sobre la infraestructura de IT de la empresa objetivo antes de lanzar el ataque.

En la mayoría de los ataques reportados, la infección fue llevada a cabo explotando el protocolo de escritorio remoto (RDP) o mediante spear phising.

Una vez que infecta un dispositivo, se comporta como un gusano, creando 3 copias de sí mismo en la carpeta donde se encuentra alojado, cada copia, se ejecuta con distintos parámetros para detectar otros equipos en la red e intentar infectarlos. Los archivos cifrados por Ryuk tienen la extensión *.ryk.

Ryuk cifra los archivos utilizando el algoritmo AES256 con una clave generada aleatoriamente que a su vez es cifrada con la clave pública RSA que se encuentra dentro del malware, la clave cifrada se guarda dentro del archivo cifrado. A medida que Ryuk va cifrando los archivos, crea la nota de rescate en la misma carpeta donde se encuentra alojado el archivo.

Una vez ejecutado en el dispositivo de la víctima, elimina todos los puntos de restauración de Windows haciendo imposible la recuperación.

Ryuk ha sido uno de los ransomware con mayor actividad desde que comenzó la pandemia del COVID-19. Uno de los ataques que generó gran impacto en España fue el que se realizó sobre el servicio público de empleo estatal (SEPE) en marzo del 2021.

2. WannaCry

Se trata de un ransomware de cifrado diseñado para infectar dispositivos con sistema operativo Windows que tiene las características de un gusano.

El rescate inicialmente exigido era de 300$ en Bitcoin, sin embargo, se duplicaba si no se pagaba al cabo de 3 días y en caso de no proceder con el pago, al cabo de una semana, WannaCry procedía a la destrucción permanente de los archivos cifrados.

Imagen 1. Nota de rescate de WannaCry.

WannaCry se propagó por medio de la vulnerabilidad de Windows conocida como MS17-010, que los hackers pudieron aprovechar gracias al uso de EternalBlue, un exploit desarrollado por la NSA que fue filtrado por el grupo de hackers The Shadow Brokers.

Microsoft acabó entrando en conocimiento de la existencia del exploit EternalBlue y publicó un parche para corregir la vulnerabilidad:

https://technet.microsoft.com/en-us/library/security/MS17-010

Sin embargo, aquellos que no aplicaron el parche continuaron siendo vulnerables a EternalBlue. WannaCry ataca las redes usando SMBv1, un protocolo de uso compartido de archivos que permite a los equipos informáticos comunicarse con dispositivos conectados a la misma red.

WannaCry se comporta como un gusano, lo que significa que se propaga a través de las redes. Una vez que WannaCry se instala en un equipo, es capaz de analizar la red para encontrar más dispositivos vulnerables.

WannaCry se cuela utilizando el exploit EternalBlue y, a continuación, utiliza una herramienta de puerta trasera (backdoor) llamada DoublePulsar para instalarse y ejecutarse, de este modo, es capaz de propagarse automáticamente sin interacción humana y sin necesidad de archivos o programas anfitriones, lo que lo convierte en un gusano, más que en un virus.

El ataque de WannaCry comenzó el 12 de mayo de 2017 y la primera infección se produjo en Asia. Debido a su naturaleza de gusano, WannaCry se extendió como la pólvora. Infectaba 10 000 equipos cada hora y mantuvo esta velocidad hasta que pudo ser detenido, cuatro días más tarde.

WannaCry provocó un caos inmediato, especialmente en hospitales, el servicio sanitario nacional británico quedó incapacitado por el ataque y muchos hospitales se vieron obligados a apagar por completo sus sistemas informáticos, lo que afectó al cuidado de los pacientes e incluso a cirugías y otras operaciones esenciales.

El ataque, que hoy en día se considera uno de los más devastadores hasta la fecha, afectó a 230.000 dispositivos en 150 países y costo casi 4.000 millones de dólares.

WannaCry usa el puerto 445 para instalarse e infectar nuevos dispositivos, el servidor C&C se encuentra en la red TOR. Cuando WannaCry infecta un dispositivo, agrega la extensión *.wncry a todos los archivos infectados, elimina los puntos de restauración de Windows y deshabilita la recuperación de inicio de Windows.

En cada carpeta donde existan archivos cifrados, WannaCry deja los siguientes archivos para que la víctima sepa cómo proceder con el rescate:

- Please_Read_Me@.txt
- @WanaDecryptor@.exe.lnk
- !WannaDecryptor!.exe.lnk
- !Please Readme Me!.txt

3. Cerber

Se trata de un ransomware de cifrado diseñado para infectar dispositivos con sistema operativo Windows, el caso de Cerber, es particular dado que emplea el modelo ransomware como servicio (RaaS) como método de distribución.

Usando el modelo RaaS, los creadores de Cerber vendieron licencias del ransomware a otros ciberdelincuentes a cambio del 40% de las ganancias que generasen sus ataques.

Para infectar los dispositivos de las víctimas, Cerber emplea diversos vectores de ataque, aunque principalmente emplea archivos de Microsoft Office con macros maliciosas que se distribuyen a través de archivos adjuntos de email, redes P2P, actualizaciones falsas de software y troyanos.

Cerber utiliza tácticas de ingeniería social para persuadir a las víctimas a que habiliten las macros de Microsoft Office, una vez que se habilitan las macros, Cerber comienza a cifrar los archivos utilizando los algoritmos RC4 y RSA y cambia las extensiones de los archivos cifrados por *.cerber.

Cuando Cerber ha infectado un dispositivo, coloca una nota de rescate como fondo de escritorio (ver imagen 2) que instruye a las víctimas a pagar el rescate en Bitcoin a través del navegador Tor, además de cambiar el fondo de pantalla, Cerber crea 3 notas de rescate que contienen instrucciones paso a paso con extensiones *.txt, *.html y *.vbs.

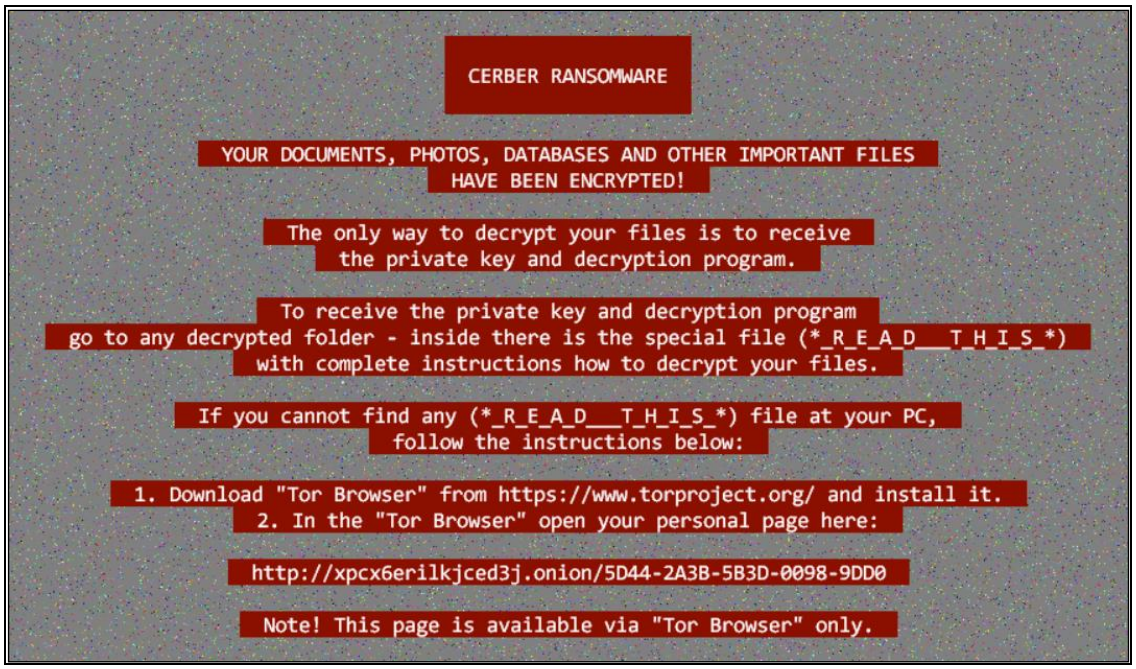

Imagen 2. Nota de rescate del ransomware Cerber.

Las notas de rescate aseguran a los usuarios de que solo podrán desencriptar los archivos si usan un programa llamado 'Cerber Decryptor' que pueden descargar si pagan 1.24 Bitcoins, si no se paga el rescate al cabo de 7 días, el importe se duplica hasta los 2.48 Bitcoins.

Cerber está diseñado para cifrar más de 300 tipos de archivos y tiene capacidad para trabajar sin conexión, lo que significa que desconectar el dispositivo infectado de Internet no detendrá el procedimiento de cifrado, lo que lo convierte en un ransomware muy peligroso.

Actualmente, existen más de seis variantes de Cerber, tras su primer lanzamiento en julio de 2016, más de 150.000 dispositivos con sistema operativo Windows se infectaron en todo el mundo, a finales de 2016, los autores de Cerber habían obtenido 2.3 millones de dólares en pagos de rescate.

A diferencia de otros tipos de ransomware, los desarrolladores de Cerber lanzaron varias actualizaciones que introducían características para evadir la detección por parte de antivirus.

4. Locky

Se trata de un ransomware de cifrado diseñado para infectar dispositivos con sistema operativo Windows. Tiene capacidad para cifrar hasta 160 tipos de archivos distintos, incluyendo archivos de código fuente y bases de datos, lo que representa una amenaza para todo tipo de empresas.

Locky apareció por primera vez en febrero del 2016 y emplea criptografía de clave pública, concretamente, usa RSA de 2048 bits combinado con AES de 128 bits, el par de claves de cifrado (pública y privada) se generan en el servidor de C&C donde se almacena la clave privada de cada víctima.

El vector de ataque más extendido empleado por Locky es el correo electrónico y macros maliciosas de Office en combinación con técnicas de ingeniería social.

La táctica más común, es el envío de un correo electrónico que contiene un documento Word con una macro maliciosa que introduce el ransomware, estos correos electrónicos suelen hacerse pasar por facturas sin pagar para persuadir a las víctimas a que abran el archivo adjunto que resulta ser un documento Word intencionadamente incomprensible.

Tras abrir el documento adjunto, se solicita a la víctima que habilite las macros de Word para que el contenido pueda mostrarse adecuadamente, en ese momento, el código de la macro, que no es más que un *Downloader* descarga el código del ransomware y lo almacena en la carpeta %Temp% del usuario antes de ejecutarlo.

Al ejecutarse el código del ransomware, se contacta con los servidores de C&C donde se generan las claves RSA necesarias para iniciar el cifrado de los archivos, si se detecta una cartera de Bitcoin en el equipo de la víctima, también se procederá a cifrarla, una vez terminado el proceso de cifrado, muestra una nota de rescate en el idioma de la zona horaria de la víctima solicitando entre 0.5 y 1 Bitcoin a cambio de la clave de descifrado.

Sin embargo, el daño efectuado por Locky no termina aquí, ya que infecta todos los dispositivos que son accesibles por el dispositivo de la víctima, ya sean Windows, Linux o macOS.

Durante el cifrado, Locky cambia las extensiones de los archivos infectados a *.locky, *.zepto, *.thor, *.asasin y otras extensiones según la variante.

Al igual que WannaCry, Locky también elimina los puntos de restauración de Windows para evitar la recuperación de los archivos.

Actualmente, se han detectado más de 10 variantes distintas de Locky, cada variante, usa un método de ofuscación distinto y diferentes tipos de archivos para encapsular el código que descarga el ransomware.

Una variante de Locky se propagó a través de la aplicación de mensajería de Facebook, la infección se produjo mediante el uso de un archivo de imagen SVG que ocultaba un código Javascript, una vez que la víctima hacía clic en la imagen, se le dirigía a un sitio web malicioso que solicitaba la instalación de una extensión de Chrome para poder visualizar la imagen, al proceder con la instalación, se otorgaban permisos para alterar los datos de los usuarios en relación con los sitios web visitados [2].

Existe una alta probabilidad de que el grupo de ciberdelincuentes que se encuentra detrás de Locky provenga de Rusia, ya que se sabe que el código malicioso no se ejecuta en dispositivos ubicados en Rusia.

5. Petya

Se trata de un ransomware de cifrado diseñado para el sistema operativo Windows que apareció por primera vez en 2016.

Petya infecta el MBR (master boot record), que es el sector del disco duro responsable de suministrar información del sistema de archivos y de las particiones durante la carga del sistema operativo. Una vez infectado el MBR, Petya sobrescribe el componente encargado de cargar el sistema operativo en memoria (boot loader) con uno malicioso tras lo cual reinicia el dispositivo.

Después del reinicio, empieza a cifrar la MFT (master file table) del sistema de archivos NTFS, lo que hace que Windows no pueda localizar los archivos almacenados. En el próximo reinicio, Petya evita que Windows se inicie y muestra una nota de rescate en su lugar, que instruye a la víctima a abrir una URL mediante el navegador TOR, donde se solicitan 300$ en Bitcoin para recuperar el acceso al dispositivo.

Petya se propaga principalmente a través de campañas de spam, aunque también se ofrece como modelo RaaS.

La primera versión de Petya, requiere acceso de administrador al dispositivo de la víctima, sin embargo, hay variantes de Petya que instalan el ransomware Mischa en caso de que no se consiga obtener acceso de administrador.

El ransomware Mischa cifra todos los archivos del dispositivo de la víctima, incluyendo archivos ejecutables y en cada carpeta que contenga archivos cifrados crea 2 notas de rescate exigiendo 1.93 Bitcoins.

En 2017, apareció una variante de Petya que paso a llamarse NotPetya y que se trata de la más peligrosa ya que tiene efectos irreversibles y puede propagarse automáticamente sin intervención humana, las claves de cifrado de NotPetya se generan aleatoriamente y se destruyen automáticamente lo que hace imposible la recuperación de datos.

NotPetya se propagó gracias a los exploits EternalBlue y EternalRomance que se encontraban en el repositorio de herramientas y exploits de la NSA que filtró el grupo de piratería Shadow Brokers, su primer ataque tuvo lugar en junio de 2017 y se lanzó contra las principales empresas de Rusia y Ucrania, sin embargo, la mayor parte del daño tuvo lugar en Ucrania lo que hizo pensar a los expertos en ciberseguridad que el ataque fue llevado a cabo por Rusia.

Después de analizar el código fuente, los expertos en ciberseguridad descubrieron que su objetivo final era destruir datos, lo que contribuyó a que se clasificara como “arma cibernética”.

6. SamSam

Se trata de un ransomware de cifrado que se utiliza para llevar a cabo ataques dirigidos, por tanto, su uso está condicionado a una investigación previa de la infraestructura de IT de la organización objetivo.

El ataque comienza con la intrusión en un dispositivo de la organización, mediante el uso de herramientas de piratería, exploit kits y ataques de fuerza bruta contra el protocolo RDP.

Cuando se ha ganado acceso a un servidor de la organización, se elabora un mapa de la red corporativa mediante el uso de herramientas de administración de redes, análisis de vulnerabilidades de red y recopilación de credenciales.

Una vez que se dispone de un mapa de la red, de sus vulnerabilidades y de las credenciales de inicio de sesión de varios dispositivos, SamSam se instala en uno de ellos para propagarlo por la red.

Los primeros ataques registrados por SamSam tuvieron lugar en 2016 y continuaron hasta 2018 alcanzando principalmente empresas estadounidenses y grandes organizaciones del sector público.

Uno de los ciberataques más mediáticos fue el de Atlanta en 2018 donde muchos servicios de la ciudad se vieron afectados lo que obligó a los funcionarios a tramitar muchos procedimientos administrativos mediante formularios en papel.

Una característica de SamSam que impide su análisis en profundidad es que el payload viene cifrado con una clave que sólo conoce el atacante.

A diferencia de la mayoría de las familias de ransomware, SamSam no utiliza tácticas de ingeniería social ni campañas de spam y phising para propagarse, en su lugar, se centra en la explotación de vulnerabilidades en servidores y en ataques de fuerza bruta para obtener contraseñas de cuentas del protocolo de escritorio remoto (RDP).

SamSam requiere el uso de técnicas de piratería sofisticadas ya que los ataques deben llevarse a cabo manualmente, además, si la víctima decide pagar el rescate, debe ejecutar manualmente el programa suministrado por el atacante para restaurar los archivos a su estado original.

Una vez instalado en el dispositivo de la víctima, SamSam comienza a buscar todas las copias de seguridad y borra los puntos de restauración existentes.

El algoritmo de cifrado empleado es RSA-2048, los rescates se pagan a través de Bitcoin y el margen de tiempo para pagarlo es de 7 días, transcurrido dicho periodo de tiempo, el rescate aumenta.

Una de las particularidades de SamSam que lo diferencia del resto de familias de ransomware se encuentra en que sus creadores han invertido parte de los ingresos obtenidos en la implementación de técnicas más sofisticadas que facilitan su propagación, así como en el perfeccionamiento de las técnicas de evasión y detección por parte de antivirus e IDS.

Se estima que los creadores de SamSam llegaron a recaudar casi 6 millones de dólares.

7. CryptXXX

Se trata de otro ransomware de cifrado diseñado para atacar el sistema operativo Windows, apareció por primera vez en abril de 2016.

CryptXXX se distribuye a través de páginas web que utilizan el exploit kit Angler, que se aprovecha de vulnerabilidades para infectar los equipos con Bedep, un malware encargado de descargar el ransomware.

El proceso de infección es el siguiente:

1) El usuario ingresa en una página que integra el exploit kit Angler.

2) Angler lanza un análisis de vulnerabilidades en el dispositivo, si se detecta que el dispositivo es vulnerable, se infecta con el malware Bedep.

3) Bedep descarga CryptXXX como un archivo DLL con ejecución retardada que esperará 62 minutos antes de iniciar la rutina de cifrado.

4) Una vez que se han cifrado los archivos, se les cambia la extensión por *.crypt y se sustituye el fondo de escritorio de la víctima por una nota de rescate.

CryptXXX tiene capacidades de evasión frente a herramientas de análisis de malware para evitar que su comportamiento sea estudiado.

La versión 1.0 de CryptXXX cifraba los archivos de las víctimas utilizando el algoritmo RSA-4096 y agregaba la extensión *.crypt al nombre del archivo, mientras que las versiones más modernas adoptan diferentes comportamientos con respecto a la asignación de nombres.

La versión 2.0 de CryptXXX se comporta como un ransomware de bloqueo ya que no permite el acceso al dispositivo de la víctima mediante el bloqueo de la pantalla con la nota de rescate.

A partir de la versión 3.0, CryptXXX descarga una DLL llamada StillerX diseñada para robar credenciales de usuario y Bitcoins de monederos virtuales, esta DLL funciona como un plugin, pero también puede ser usada de forma independiente sin el ransomware.

StillerX extrae las credenciales, tanto cifradas como en texto plano, de los programas compatibles y las envía automáticamente al servidor de C&C, donde se almacenan para procesarlas más adelante.

En la versión 3.100, los desarrolladores de CryptXXX cambiaron el exploit kit Angler por el exploit kit Neutrino que incluye más capacidades de análisis de redes para buscar y cifrar archivos compartidos en el directorio activo de Windows, además, el portal empleado para el pago de los rescates también se actualizó para conectar directamente con un sitio web alojado en la red TOR.

8. CryptoWall

Se trata de un ransomware de cifrado diseñado para atacar el sistema operativo Windows.

Hasta la fecha se le conocen 6 variantes, la primera apareció en noviembre de 2013 y fue un clon del ransomware CryptoLocker ya que empleaba la misma interfaz de usuario y las mismas notas de rescate.

La segunda variante, denominada CryptoDefense, apareció en febrero del 2014, sin embargo, contenía un error en la implementación del algoritmo de cifrado que hacía posible la restauración de los archivos comprometidos.

En marzo del 2014, los autores de CryptoWall liberaron su primera versión, se trataba de una versión moderna y parcheada de CryptoDefense, sin embargo, contenía un fallo de diseño que hacía posible la recuperación de los archivos de restauración mediante el uso de software de recuperación de archivos.

En cada nueva versión, los autores de CryptoWall fueron agregando nueva funcionalidad y fueron arreglando los fallos de diseño y los errores detectados en la versión anterior.

El principal método de distribución fue el envío de correos electrónicos que incluían un archivo adjunto o un link que al abrirlo ejecutaba el downloader Upatre responsable de descargar el archivo binario del ransomware.

En junio del 2014, los creadores de CryptoWall lanzaron una agresiva campaña de spam en la que utilizaron la técnica de ingeniería social “Missed fax”, que consistía en persuadir a las víctimas a descargar el archivo adjunto o hacer clic en un enlace malicioso que descargaba un ZIP que a su vez contenía el downloader haciéndoles pensar que habían recibido un fax.

Antes de la campaña de spam de junio del 2014, se detectó que CryptoWall se estaba distribuyendo mediante el uso del exploit kit Angler.

El binario de CryptoWall era comprimido y ofuscado con un montón de instrucciones y trucos que se añadían deliberadamente para evitar ser detectado por los antivirus cuando llegaba al disco duro de la víctima.

Cuando CryptoWall se ejecutaba, se desempaquetaba en memoria e inyectaba el código malicioso en los procesos que creaba, lo que dificultaba la detección por parte de los antivirus.

Entre los procesos que creaba, ejecutaba uno que se encargaba de eliminar las instantáneas y puntos de restauración existentes en el dispositivo infectado, lo que evitaba que se pudieran recuperar los archivos cifrados.

Para establecer la persistencia entre reinicios, se creaban una serie de claves en el registro en Windows y una copia del malware en las siguientes carpetas:

- %AppData%
- %UserProfile%\Start Menu\Programs\Startup

CryptoWall utilizaba servidores de C&C con los que se comunicaba directamente, a finales de julio del 2014, empezó a desplegar los servidores C&C en la red TOR. Los servidores de C&C eran los responsables de generar la clave pública RSA de 2048 bits con la que se cifraban los archivos y de recibir las notificaciones de infección.

CryptoWall estaba diseñado para cifrar tanto los archivos del disco duro, como los archivos encontrados en medios extraíbles (USB) y unidades de almacenamiento compartidas en la red.

A parte de Bitcoin, CrytpoWall ofrecía a las víctimas otras opciones de pago y a diferencia de otras familias de ransomware, el coste del rescate fluctuaba sin que se estableciera un patrón exacto que determinase el precio a pagar por cada víctima.

Los datos extraídos del servidor de pagos revelaron que CryptoWall infecto a 625.000 dispositivos, de los cuales solo 1.683 víctimas pagaron el rescate, el total de ingresos generado fue de 1.101.900 dólares.

Referencias

[1]. [10/2021]. Checkpoint. Ryuk Ransomware: A Targeted Campaign Break-Down

[2]. [10/2021]. Mundowin. Locky ransomware se propaga en Facebook

Bibliografía

Nihad A. Hassan
Ransomware Revealed
Apress, 2019

[10/2021]. WeliveSecurity. Ransomware Ryuk análisis principales características

[10/2021]. CybersecurityNews. Ryuk, la última amenaza del ransomware

[10/2021]. Kaspersky. Ransomware WannaCry

[10/2021]. Avast. ¿Qué es WannaCry?

[10/2021]. PcRisk. Cerber Ransomware

[10/2021]. Varonis. Cerber Ransomware, what you need to know

[10/2021]. Avast. ¿Qué es el ransomware Locky?

[10/2021]. Checkpoint. Locky ransomware

[10/2021]. Avast. Ransomware Petya

[10/2021]. ElConfidencial. De WannaCry a Petya

[10/2021]. Wikipedia. Ciberataque de Atlanta de 2018

[10/2021]. Infobae. Como opera SamSam el ransomware de los 6 millones de dólares

[10/2021]. Unaaldia. El ransomware SamSam ataca a entidades financieras peruanas

[10/2021]. ComputerHoy. CryptXXX el ransomware que roba contraseñas y bitcoins

[10/2021]. Cyberseguridad.net. CryptXXX un ransomware en crecimiento

[10/2021]. Gobierno de paraguay. CryptXXX ahora también roba tus contraseñas

[10/2021]. WeliveSecurity. CryptoWall 3.0 aprovecha una vulnerabilidad en Flash

[10/2021]. SecureWorks. Cryptowall ransomware

[10/2021]. Sophos. The current state of ransomware cryptowall