Ransomware Wannacry

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
WannaCry	Es un ransomware de cifrado, esta cifra los archivos valiosos para que no puedas acceder a ellos	Este ransomware posee una función que comprueba la disponibilidad de un dominio web, y si está disponible, este infecta toda la red.	Algoritmo de cifrado AES, la clave aleatoria es generada con la función de Windows "CryptGenRandom". Esta se guarda con una clave cifrada de RSA pública, el descifrado de los archivos solo es posible por la clave privada RSA que se está utilizando durante el ataque.	Los atacantes exigieron un rescate en bitcoins por valor de 300 dólares y, posteriormente, aumentaron el rescate en bitcoins a un valor de 600 dólares. A las víctimas del ataque de ransomware WannaCry se les comunicó que, si no pagaban el rescate en un plazo de tres días, sus archivos se eliminarán de forma permanente.	Mayo de 2017

Ransomware Locky

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Locky	Locky es un tipo de malware que puede cifrar archivos importantes en su equipo y exigir el pago de un rescate para recuperarlos. Aprenda cómo funciona el ransomware Locky, qué puede hacer para que no infecte su equipo y cómo detectar y bloquear los ataques de ransomware mediante un potente software antimalware.	El vector de infección más usado por los ciberdelincuentes es el correo electrónico. Usan mensajes fraudulentos relacionados a cobros de bancos o deudas, usando ingeniería social siembran incertidumbre en la posible víctima. Si esta última cae y abre el correo encontrará que tiene que descargar un archivo adjunto en Word el cual al momento de visualizarse solicita la activación de macros de Word. Este es el método como Locky se instala en el equipo y cifra los archivos.	Locky usa el algoritmo AES-128. Advanced Encryption Standard. Algoritmo de cifrado simétrico. Su nombre original es Rijndael. AES es una especificación para cifrado de datos establecido por el instituto nacional de estándares y tecnología de América 2001. El instituto seleccionó 3 sistemas de cifrado de 128 bits de la familia Rijndael para el estándar AES. Esta última se utiliza ampliamente en diversas aplicaciones de negocios. Sin embargo, crypto-malware ha descubierto una manera de tomar ventaja de ella y usarla contra los usuarios de PC. Al ser infectado por Locky utiliza los métodos de AES y cifra archivos que coincidan con las siguientes extensiones: .medio, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .gpg, .aes, .ARCO, .PAQ, .tar.bz2, .Tbk, .detrás, .toma, .tgz, .rar, .cremallera, .DJV, .djvu, .svg, .bmp, .png, .gif, .prima, .cgm, .jpeg, .jpg, .tif, .pelea, .NEF, .psd, .cmd, .murciélago, .clase, .tarro, .Java, .áspid, .brda, .SCH, .DCH, .inmersión, .vbs, .pers, .no, .cpp, .php, .LDF, .mdf, .EII, .VENDIDO, .MYD, .frm, .odb, .dbf, .CIS, .sql, .SQLITEDB, .sqlite3, .asc, .lay6, .laico, .MS11 (copia de seguridad), .sldm, .sldx, .PPSM, .PPSX, .PDMA, .docb, .MML, .sxm, .OTG, .respuesta, .uop, .Potx, .senderos, .pptx, .pptm, .std, .sxd, .maceta, .pps, .STI, .ella, .OTP, .Responder, .semanas, .xltx, .XLTM, .xlsx, .xlsm, .xlsb, .ch, .xlw, .XLT, .XLM, .xlc, .dif, .STC, .sxc, .ots, .párrafo, .pliegue, .dotm, .DOTX, .docm, .docx, .PUNTO, .max, .xml, .txt, .CSV, .UOT, .RTF, .pdf, .XLS, .PPT, .STW, .sxw, .hay, .odt, .DOC, .pem, .RSE, .crt, .clave, wallet.dat. Estos archivos se renombran y cambian sus extensiones a, por ejemplo: aesir,. odin, osiris,. thor o .locky etc.	Al ser infectado Locky muestra la nota de rescate en el idioma de la zona correspondiente. Pedirá instalar el navegador Tor y solicita transferir bitcoins a cambio de una clave de cifrado. Los rescates varían según los deseos de los atacantes y quien sea el afectado. Si el afectado tiene en su equipo una cartera de Bitcoins puede llegar a cifrarla.	Locky apareció en 2016 y se extendió rápidamente por muchas regiones del mundo, incluidas Norteamérica, Europa y Asia. Uno de los primeros ataques importantes afectó a un hospital de Los Ángeles, que se vio obligado a pagar un rescate de más de 17.000 USD. A lo largo del año siguió con una serie de ataques dirigidos contra otras instituciones sanitarias.

Ransomware Bad Rabbit

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Bad Rabbit	Ransomware de cifrado.	Se hace pasar por un instalador de Adobe Flash, se descarga desde páginas infectadas con tan solo visitar un sitio web. El malware se integra a las páginas mediante JavaScript inyectándose en el HTML de la página. Bad Rabbit se propaga a través de una falsa actualización de Adobe Flash Player. Sin embargo, tales virus se distribuyen probablemente a través de correos basura (adjuntos infecciosos), fuentes de descarga de software no oficiales (redes P2P, sitios web de descarga de software gratuito, sitios web de alojamiento de archivos, etc.) y troyanos. Los correos basura vienen a menudo con documentos de ofimática adjuntos, códigos JavaScript o archivos maliciosos que, cuando se abren, descargan e instalan malware. Las fuentes de descarga no oficiales presentan a menudo ejecutables maliciosos como software legítimo, por lo que engañan a las víctimas para que descarguen e instalen software malicioso. Los troyanos son los más simples; solo abren "puertas traseras" para que entren otros programas maliciosos en el sistema.	Bad Rabbit se sirve de criptografía AES (simétrica) y RSA-2048 (asimétrica). Los archivos se cifran con un algoritmo AES que genera una clave única usada para encriptar y desencriptar los archivos. La clave generada se encripta luego a través de criptografía RSA-2048 (para ver más información sobre los algoritmos de cifrado y claves, haga clic aquí). El precio de la clave es 0,05 Bitcoins (actualmente, equivalente a ~$280). Tras pagar el rescate, las víctimas recibirán supuestamente la clave de desencriptación. No obstante, los usuarios nunca deberían fiarse de los ciberdelincuentes. Los estudios demuestran que estos individuos suelen ignorar a las víctimas una vez que realizan el pago. Por este motivo, el pago no garantizará que esos archivos sean recuperados. Es más que probable que las víctimas resulten estafadas. Por tanto, le recomendamos que haga caso omiso a las peticiones de pago. Por desgracia, no hay herramientas capaces de restaurar los archivos encriptados por Bad Rabbit. Por tanto, la única solución es restaurar el sistema desde una copia de respaldo.	En la pantalla del infectado aparece un archivo readme.txt el cual lanza un mensaje en pantalla el cual informa a las víctimas que sus archivos fueron cifrados y anima a pagar un rescate por ellos. La manera de pago es generalmente en Bitcoins.	Surgió en Julio 2017 y es similar a Wanna Cry y Petya.

Ransomware Ryuk

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Ryuk	Es un ransomware de cifrado	La metodología del ataque se llama triple amenaza. El primer paso es un correo electrónico con phishing, este correo tiene un documento de Microsoft office con un código en su interior. Este ejecuta un comando en PowerShell donde descargara el troyano EMOTET sin utilizar archivos de script, es de esta manera como comienza el cifrado de RYUK.	RYUK es un algoritmo de cifrado RSA y AES son irrompibles con tres claves, su modelo de cifrado base es CTA que utiliza un clave RSA global privada, la segunda RSA se entrega al sistema a través de la carga útil principal y se cifra con la clave RSA global privada de la CTA. Ryuk escanea los sistemas infectados y cifra casi todos los archivos, directorios, unidades, recursos compartidos y recursos de red.	Es día de pago para los hackers. La cantidad del rescate se basa en el tamaño y el valor de la organización objetivo. El rescate puede variar, pero en general, la cantidad es bastante elevada.	2018

Ransomware Shade / Troldesh

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Shade/Troldesh	Ransomware de cifrado.	Este Ransomware se divulga a través de mensajes de correo electrónico en el apartado de SPAM, este contiene archivos tipo zip que son presentados como el receptor. El zip extraído es un JavaScript que descarga el malware, una vez la víctima le da apertura al mensaje con malware, este inicia el cifrado de archivos del usuario utilizando la extensión XBTL. Una vez terminado el proceso de cifrado, la víctima ve un mensaje de rescate que dice "LÉAME". Los atacantes buscan la comunicación directa con la víctima.	El algoritmo que utilizan es AES 246 en modo CBC. Para cada archivo que cifran utilizan dos claves AES de 246 bits aleatorias, una de ellas cifra el contenido del archivo, mientras que la otra cifra el nombre del archivo. Troldesh busca extensiones en unidades fijas, extraíbles y remotas como pueden ser: 1cd, .3ds, .3fr, .3g2, .3gp, .7z, .accda, .accdb, accdc, accde, accdt, accdw, adb, .adp, .ai3, .ai4, .ai5, .ai6, .ai7, .ai8, anim, arw, as, asa, .asc, .ascx, .asm, .asmx, .asp, .aspx, asr, asx, avi, .avs, .backup, .bak, .bay, .bd, .bin, .bmp, .bz2, .c, .cdr, .cer, .cf, .cfc, .cfm, .cfml,.cfu, .chm, .cin, .class, .clx, .config, .cpp, .cr2, .crt, .crw, .cs, .css, .csv, .cub, .dae, .dat, .db,dbf .dbx, .dc3, .dcm, .dcr, .der, .dib, .dic, .dif, .divx, .djvu, .dng, .doc, .docm, .docx, .dot. . dotm,. dotx, .dpx, .dqy, .dsn, .dt, .dtd, .dwg, .dwt, .dx, .dxf, .edml, .efd, .elf, .emf, .emz, .epf, .eps, .epsf, .epsp, .erf, .exr, .f4v, .fido, .flm, .flv, .frm, .fxg, .geo, .gif, .grs, .gz, .h, .hdr, .hpp .hta, .htc, .htm, .html, .icb, .ics, .iff, .inc, .indd, .ini, .iqy, .j2c, .j2k, .java, .jp2, .jpc,. jpe,.jpeg,, .jpf, .jpg.	Este ransomware conocido como TROLDESH cifra documentos, fotos y archivos de oficina. Este solicita a las víctimas un pago a cambio del descifrado, este rescate por lo general lo cobran en 118 Euros y hacen la transferencia por QIWI.	Existió desde el 2014 pero en el 2015 se registró su primer ataque con un total de 311. En el 2016 fue su pico más alto con 9039 ataques a usuarios registrados y en el 2020 los responsables abandonaron el proyecto publicando las 750000 claves para descifrar los archivos. Este apareció en Rusia.

Ransomware Jigsaw

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Jigsaw	Ransomware de encriptación	También conocido como BitcoinBlackmailer.exe. Es conocido por mostrar la marioneta de la película Saw en la pantalla al hacer la infección. Cuenta con más de 240 extensiones. El vector de infección más usado son los correos maliciosos. El malware se activa en cuanto el usuario lo descarga y cifra todos los archivos y el MBR el cual es el sistema de arranque. Jigsaw se hace pasar por DROPBOX o FIREFOX como fue escrito en .NET framework se puede realizar ingeniería inversa para eliminar el cifrado. Usando actualizaciones falsas de software, troyanos, e-mails maliciosos y redes P2P como Torrent	El algoritmo de cifrado es AES el cual afecta a los tipos de archivos: .jpg, .jpeg, .raw, .tif, .gif, .png, .bmp , .3dm, .max, .accdb, .db, .dbf, .mdb, .pdb, .sql, .dwg, .dxf, .c, .cpp, .cs, .h, .php, .asp, .rb, .java, .jar, .class, .py, .js, .aaf, .aep, .aepx, .plb, .prel, .prproj, .aet, .ppj, .psd, .indd, .indl, .indt, .indb, .inx, .idml, .pmd, .xqx, .xqx, .ai, .eps, .ps, .svg, .swf, .fla, .as3, .as, .txt, .doc, .dot, .docx, .docm, .dotx, .dotm, .docb, .rtf, .wpd, .wps, .msg, .pdf, .xls, .xlt, .xlm, .xlsx, .xlsm, .xltx, .xltm, .xlsb, .xla, .xlam, .xll, .xlw, .ppt, .pot, .pps, .pptx, .pptm, .potx, .potm, .ppam, .ppsx, .ppsm, .sldx, .sldm, .wav, .mp3, .aif, .iff, .m3u, .m4u, .mid, .mpa, .wma, .ra, .avi, .mov, .mp4, .3gp, .mpeg, .3g2, .asf, .asx, .flv, .mpg, .wmv, .vob, .m3u8, .dat, .csv, .efx, .sdf, .vcf, .xml, .ses, .Qbw, .QBB, .QBM, .QBI, .QBR , .Cnt, .Des, .v30, .Qbo, .Ini, .Lgb, .Qwc, .Qbp, .Aif, .Qba, .Tlg, .Qbx, .Qby , .1pa, .Qpd, .Txt, .Set, .Iif , .Nd, .Rtp, .Tlg, .Wav, .Qsm, .Qss, .Qst, .Fx0, .Fx1, .Mx0, .FPx, .Fxr, .Fim, .ptb, .Ai, .Pfb, .Cgn, .Vsd, .Cdr, .Cmx, .Cpt, .Csl, .Cur, .Des, .Dsf, .Ds4, , .Drw, .Dwg.Eps, .Ps, .Prn, .Gif, .Pcd, .Pct, .Pcx, .Plt, .Rif, .Svg, .Swf, .Tga, .Tiff, .Psp, .Ttf, .Wpd, .Wpg, .Wi, .Raw, .Wmf, .Txt, .Cal, .Cpx, .Shw, .Clk, .Cdx, .Cdt, .Fpx, .Fmv, .Img, .Gem, .Xcf, .Pic, .Mac, .Met, .PP4, .Pp5, .Ppf, .Xls, .Xlsx, .Xlsm, .Ppt, .Nap, .Pat, .Ps, .Prn, .Sct, .Vsd, .wk3, .wk4, .XPM, .zip, .rar. Método usado para descifrar jigsaw: **1:** Haga clic en el icono de la batería en la bandeja del sistema (al lado del reloj digital) en Windows y luego haga clic en Más opciones de energía. **2:** Opciones de poder Aparecerá el menú. En el plan de energía, haga clic en Cambiar la configuración del plan. **3:** En la configuración de su plan asegúrese de que establece "Apagar la pantalla" y "Poner equipo de dormir" a "Nunca" Del menú desplegable minutos. **4:** Haga clic en "Cambiar la configuración avanzada del Plan" y haga clic para expandir la opción "disco duro" en la lista que hay. **5:** Desde allí, configurar los ajustes de potencia (En la batería y encendido) "Nunca".	Solicitan rescate en Bitcoins 150 dólares durante la primera hora de infección, aparece un reloj en cuenta atrás el cual muestra exactamente una hora si el tiempo termina proceden a borrar archivos. Si el pago no se realiza en el tiempo enviado se empiezan a borrar archivos progresivamente hasta terminar borrando todos en 72 horas. cada vez que el usuario intente reiniciar el equipo se eliminan 1000 archivos.	2016

Ransomware CryptoLocker

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
CryptoLocker	Es un ransomware que cifra los archivos de Windows.	Este ransomware para infectar a sus víctimas utilizaron la red de robots o más conocida como botnet denominada Gameover ZeuS. Esta se trata de una red de equipos infectada anteriormente con un malware cuyo operador podría controlar la máquina de forma remota, sin el consentimiento de sus propietarios. De esta manera propagaron CryptoLocker a una infinidad de usuarios.	Este utiliza un método de cifrado asimétrico, este sistema utiliza dos claves vinculadas, una pública RSA de 2048 bits para el cifrado de extensiones de documentos, fotos e información del usuario y la otra es privada para el descifrado. El atacante utiliza conexiones anónimas a través de TOR para solicitar el pago del rescate.	El ransomware CryptoLocker ha obtenido de sus víctimas millones de dólares en bitcoins.	Surgió en septiembre del 2013 y su ataque se prolongó hasta el 2014

Ransomware Petya

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
Petya	Ransomware de cifrado bloquea discos duros enteros e intenta impedir que el equipo no pueda arrancar.	Diseminado mediante archivos adjuntos maliciosos de correo electrónico. Cuando dichos archivos se descargan y abren, el malware cae sobre el equipo de la víctima. El ataque pudo haber sido iniciado como tradicionalmente hacen los cibercriminales con el ransomware: mediante phishing. Aunque las pruebas de que esto fuese así cada vez son más débiles. La hipótesis de este vector de ataque se sustenta en una posible propagación de documentos de MS Office que explotaría una vulnerabilidad de esa plataforma ofimática como vía de entrada a un equipo de la red y luego, de forma que detallaremos más adelante, se propagara en la red local de los equipos infectados mediante ese primer vector. Se habla de que podría tratarse de un falso currículo alojado en Dropbox. Este documento sería enlazado desde un email fraudulento, aunque no disponemos de evidencias certeras.	El ransomware Petya cifra la tabla maestra de archivos (MFT). Esta tabla es una guía de referencia rápida de todos y cada uno de los archivos que contiene un equipo. Sin acceso a la tabla, un equipo no puede encontrar ninguno de sus archivos, por lo que no es capaz siquiera de arrancar, y mucho menos funcionar con normalidad. Cuando la víctima instala inadvertidamente Petya en un equipo Windows, el malware infecta el registro de arranque maestro (MBR). El MBR es la parte de la programación de un equipo responsable de cargar el sistema operativo cada vez que el equipo se enciende. Una vez dentro del MBR, Petya fuerza el reinicio del equipo y, a continuación, comienza a cifrar la MFT mientras muestra la nota de rescate.	La pantalla de solicitud de rescate de Petya indica el identificador de una cartera de Bitcoins en la que deben ingresar el equivalente a 300 dólares. A continuación, los cibercriminales solicitan que se les envíe un email en el que se especifique el identificador de la cartera desde la que se ha hecho la transferencia y un número de identificación de la computadora.	Apareció en 2016, fue el 27 de junio de 2017 cuando explotó mundialmente con una nueva versión llamada NOT PETYA afectando a empresas ucranianas y luego se extendió a Francia, Alemania, Italia, Polonia, Reino unido y Estados Unidos.

Ransomware GandCrab 5.2

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
GandCrab 5.2	Es un Ransomware de cifrado que cifra los datos almacenados y los mantiene encriptados.	Este tipo de ransomware se distribuye por lo general a través de campañas de correos basura (Spam), herramientas falsas y programas infectados por malware. Los archivos adjuntos que vienen en los correos por lo general son documentos de Microsoft Office, ficheros PDF, archivos (ZIP), juegos descargados por TORRENT. Si se ejecutan estos archivos se descargan e instalan en la computadora de la víctima.	Actualmente no se sabe si es simétrico o asimétrico, pero usa el cifrado en este caso.	Para hacer el pago, las víctimas tienen que usar criptomoneda DASH o Bitcoin y transferirla haciendo clic en un enlace que apunta a una dirección de monedero de criptomonedas. El sitio web tiene un tiempo limitado que, si no se cumple, hará que el precio se duplique. El precio que te daban primero por la clave de descifrado es de $1200, después de un tiempo determinado se incrementará hasta los $2400.	Este apareció en enero del 2018.

Ransomware GoldenEye

Nombre	Tipo de Ransomware	Metodología de infección (Vector de Transmisión)	Algoritmo de cifrado que está utilizando	Cuál es el rescate que está pidiendo	Fecha en la que apareció el primer ataque
GoldenEye	Ransomware de cifrado. Cifra todos los documentos del ordenador a los cuales les añadirá una extensión de 8 números al azar. A partir de este momento la víctima perderá control de todo y cada vez que intente realizar alguna actividad le saldrá un mensaje de texto en formato TXT.	Es una variante de Petya. Su vector de infección son correos electrónicos camuflados como solicitudes de empleo o spam los cuales tienen dos archivos adjuntos, el primero es un archivo pdf que contiene una carta de presentación; su finalidad es la credibilidad. El segundo es un documento en formato xls que contiene macros maliciosos y solicita validarlos para poderse ejecutar.	Usa el mismo método de Petya Mischa. Golden Eye encripta primero los archivos de la computadora y luego intenta instalar el MBR (Máster Boot Record). A continuación, añade una extensión aleatoria de 8 caracteres a cada archivo al que se dirige. Después de eso, modifica el proceso de arranque del sistema, haciendo que el ordenador sea inútil al restringir el acceso de los usuarios.	Solicitan pago por rescate en bitcoins.	2017