



RASOMWARE

—

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

Qué es Ransomware

De la misma forma que existe el secuestro de personas con fines económicos, en el mundo IT el **ransomware se ha convertido en un ataque secuestrador de datos** ya que este ataque básicamente accede a nuestro equipo, encripta toda la información y exige una determinada suma de dinero para su recuperación, así de sencillo.

El origen del nombre "Ransomware" viene de la combinación de dos palabras:

- Ransom (Secuestro)
- ware (Software)

Este ataque, también conocido como rogueware o scareware, ha estado afectando usuarios desde el año 2005. Aunque ha ido evolucionando apareciendo diferentes tipos, perfeccionando y encontrando debilidades donde poder propagarse con facilidad. Os dejamos un vídeo que os lo explica de forma excepcional para entenderlo a todos los niveles.

Cómo funciona Ransomware

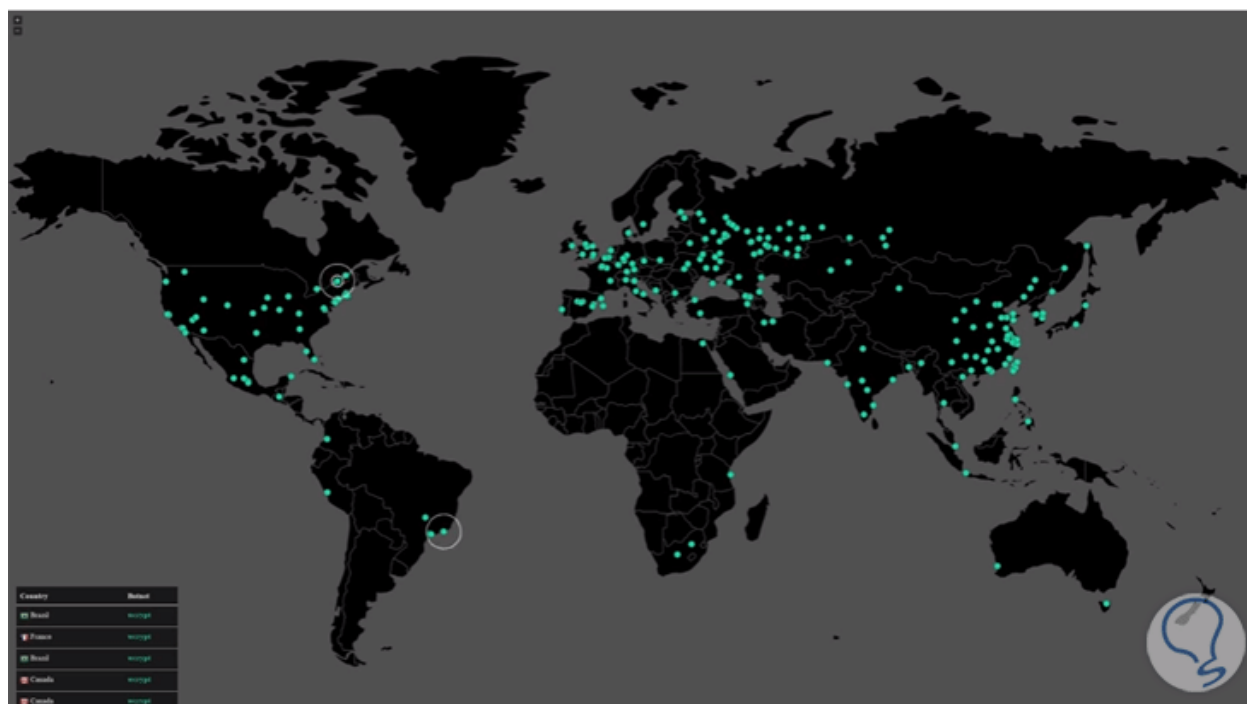
Ransomware hace uso de una serie de pasos donde lamentablemente el primero lo da la víctima al ejecutarlo, estos pasos son:

- Exploración del sistema a través de unidades USB, correos fraudulentos, etc.
- Instalación en el sistema al ejecutarse el archivo infectado.
- Selección de archivos a cifrar.
- Cifrado de los datos seleccionados usando actualmente RSA de 2048 bits.
- Mensajes a la víctima usando diversas alternativas desde correos hasta mensajes de voz
- Espera del pago usando medios como bitcoins, MoneyPak, Ukash y cashU, entre otros.
- Envío de las claves de cifrado a la víctima, pero esto no es 100% seguro. (Podemos decir que NO os lo van a enviar, no recomendamos pagar).

Como podemos observar, es una cadena que nosotros mismos podemos romper desde el principio. En el mundo de internet y digital debería serle enseñado a la gente que es mucho mejor siempre pensar mal y acertarás. Desconfía y no seas de los que abre alegremente cualquier adjunto recibido, o entrar en cualquier web e instalar sin dudar ni un momento cualquier programa.

Ransomware WannaCry


Este es el **Ransomware últimamente más conocido** porque ha realizado ataques a muchos equipos de compañías y personas a nivel mundial. Es un Ransomware Criptográfico pero merece la pena catalogarlo al margen, ya que ha salido como sabéis en las noticias a nivel mundial, por ataques realizados en muchos países diferentes. Es importante comentar que esto no es nuevo como mucha gente piensa, ya que lleva tiempo cocinándose en muchos equipos. Podéis ver en la siguiente imagen donde se están realizando.



Hay muchos virus y ataques peligrosos en Internet, pero **Ransomware WannaCry es uno de los peores.**

Básicamente, podemos decir que lo consideramos de los peores porque te realiza un cifrado limpio de múltiples archivos de mucha importancia con un algoritmo y clave potentes, lo que hace muy difícil volverlos a tener. Además es importante señalar la facilidad de ejecución que posee para transmitirlo y ejecutarlo en todas las unidades de red.

Ransomware criptográfico



Este tipo de ataque hace uso de algoritmos de nivel avanzado y su función principal consiste en bloquear archivos del sistema donde para acceder a ellos debemos pagar una suma, en ocasiones alta, de dinero.

Dentro de este tipo encontramos CryptoLocker, Locky, TorrentLocker, también WannaCry etc.

Ransomware de MBR

Sabemos que el MBR (Master Boot Record) gestiona el arranque del sistema operativo y este tipo de ataque se encarga de modificar los valores de los sectores de arranque con el fin de evitar que el usuario pueda iniciar su sistema operativo de forma normal.

Winlocker

Este ataque está basado en SMS, mensajes de texto, mediante el cual exige el envío de un mensaje de texto a un sitio de pago con un código asignado con el fin de desbloquear los archivos.

Jigsaw

Este ataque se encarga de eliminar periódicamente archivos con la finalidad que la víctima sienta la presión de pagar el rescate para no perder más información valiosa.

Con este ataque cada hora se va eliminando un archivo del equipo hasta que el pago sea realizado, y, como detalle adicional pero no alentador, jigsaw elimina hasta mil archivos del sistema cada vez que el equipo se reinicia y accede al sistema operativo.

Kimcilware

Con este ataque estamos siendo víctimas del cifrado de datos en nuestros servidores web y para ello hace uso de las vulnerabilidades del servidor y así cifra bases de datos y archivos allí alojados estableciendo la no actividad del sitio web.

Maktub

Este es un ataque que se propaga a través de correos fraudulentos y comprime los archivos afectados antes de cifrarlos.

Su apariencia es de un archivo PDF o de texto, pero cuando es ejecutado, en segundo plano sin que estemos enterados se instala en el equipo y por lo general se exigen altas sumas de dinero por la recuperación de los datos.

SimpleLocker, Linux.Encoder.1 y KeRanger

Estos ataques cumplen su rol básicamente en dispositivos móviles y de PC con el fin de bloquear su contenido. Con SimpleLocker se afecta la tarjeta SD de los dispositivos Android cifrando archivos. Linux.Encoder.1 y KeRanger se encargan de cifrar datos en sistemas operativos Linux y Mac OS.

Cerber

Puede ser uno de los que más miedo de a los usuarios, sobre todo de sistemas Windows, ya que este ataque accede al audio del sistema operativo para emitir mensajes, y no propiamente de motivación o de las últimas novedades de Microsoft.

Este ataque genera un archivo VBS llamado “# DECRYPT MY FILES # .vbs” el cual está en 12 idiomas diferentes y emite mensajes amenazantes y solicitando pago por la recuperación de los datos.

Como veis, encontramos diversos **tipos de ataques ransomware** (Tener en cuenta que hay y habrá muchos más tipos) lo cual lo convierten en una amenaza latente y si aún no lo creemos veamos estos datos, seguirán subiendo de forma muy rápida:

- En el mundo existen alrededor de 500.000 víctimas del ataque Cryptolocker.
- Una organización en Sudamérica pago alrededor de USD 2500 para recuperar sus datos.
- El 1.44% de los usuarios victimas de TorrentLocker ha pagado el rescate.
- Se están produciendo ataques a nivel mundial con el tipo WannaCry donde lo recaudado hasta ahora dicen que está entre unos USD 7.500-25.000. (No pagues).

Cómo dijimos al principio, **no recomendamos pagar este rescate por la clave de cifrado utilizada**. No está 100% verificado que os la vayan a dar y al hacerlo tener en cuenta que estaréis fomentando que aparezcan más ciberdelincuentes al ver que hay "negocio" suculento para ellos. Además tener en cuenta que pueden existir ciertas soluciones más practicas que os explicamos en los siguientes apartados.

Hemos hablado del avance de la tecnología, pero ransomware también ha evolucionado, ya que hoy en día está el ataque **PHP Ransomware o WannaCry Ransomware**, los cuales cifran todos los datos importantes y en algunos casos sin pedir rescate o pago por los datos cifrados entre los cuales están los archivos con las siguientes extensiones:

zip, rar, r00 ,r01 ,r02 ,r03, 7z, tar, gz, xlsx, doc, docx, pdf, pptx, mp3, iso entre otras más que detallamos en los siguientes apartados.

Tener en cuenta que irán incrementándose o variando, y por ello no es bueno pensar que un determinado tipo de archivo está libre de ser "secuestrado".

Objetivo de Ransomware

Aunque muchos ataques de ransomware ocurren a nivel organizativo donde la información es mucho más delicada y confidencial, los atacantes que crean estos virus no ponen límite, también son un punto débil los usuarios de hogar por razones como:

- Pocos o nulos conocimientos de seguridad informática.
- No contar con aplicaciones de antivirus en sus sistemas operativos.
- Contar con redes abiertas e inseguras.
- No crear respaldos constantes de la información.
- No actualizar el sistema operativo y las aplicaciones de seguridad de forma periódica.
- Por el uso indebido de los servicios de internet.

Quizás no tengamos información valiosa, pero si somos **víctimas del cifrado de nuestra información** sin lugar a dudas seremos víctimas donde nos afectará para poder seguir de forma normal nuestras operaciones diarias como a nivel educativo, personal o empresarial.

De las empresas tampoco se han olvidado los creadores de ransomware, es más, son el objetivo número 1, ya que con ellas obtienen las siguientes ventajas:

- Son donde más daño pueden hacer, con jugoso potencial económico para que paguen rescate.
- Mayor desestabilidad al cifrar datos delicados de nómina, finanzas, RRHH, etc.
- Posibilidad de afectar un mayor número de equipos y servicios.
- Vulnerabilidades presentadas en los servidores o equipos cliente.
- Desestabilizar puntos importantes de países, y sino creéis esto, mirar las últimas noticias donde han sido afectados Hospitales de Londres, empresas como Telefónica en España etc.
-

Podemos certificar que este es el **nuevo formato de Guerra Mundial**, no es disparando bombas pero puede ser igual o más doloroso de lo que imaginamos.

Técnicas para propagar Ransomware

Como hemos visto anteriormente existen diversos tipos de ataque ransomware y algunas de las técnicas empleadas para su propagación son:

- Envío de correos electrónicos fraudulentos.
- Direccionamiento web a sitios falsos.
- Mensajes de texto.
- Vulnerabilidades encontradas a nivel de seguridad en servidores o equipos cliente.
- Campañas de publicidad maliciosa.
- Sitios web legales que poseen códigos maliciosos en su contenido.
- Auto propagación entre dispositivos.


3. Recomendaciones para protegernos contra malware Ransomware

En vista que ransomware está tomando tanta fuerza y es muy sencillo ser victimas, existen una serie de opciones que nos ayudarán a estar atentos ante este tipo de ataques y evitar ser una víctima más. Algunos consejos son:

Realizar copias de seguridad

Podemos decir que es lo más importante de ser realizado tanto en organizaciones, como a nivel personal. Tener copia de seguridad, nos salva de problemas no sólo de malware, virus y ataques, también nos protege de errores físicos del hardware que pueden ocurrir en discos, equipos, servidores etc. Por lo que **copia de seguridad (backup) es necesaria y vital**.

Es una solución a implementar de forma contante y de ser posible en discos y unidades externas, o bien tienes la opción (a nivel personal) de hacerlo en ubicaciones como la nube, Dropbox, OneDrive, etc, pero lo que más recomendamos son servidores o discos externos ya que así **tendremos siempre la disponibilidad e integridad de los archivos**.



Es importante comentaros que se debe tener en cuenta que este malware (gusano) Ransomware perfectamente ataca y cifra también en las unidades que tengas conectadas en ese momento, incluidas las de la nube, por ello recuerda desconectar esa conexión y no tenerlo siempre conectado si no lo estás usando.

Hemos visto como este ataque de **Ransomware WannaCry** (y otras versiones anteriores) realizarán un cifrado de conexiones en la nube de los ordenadores que fueron infectados. Se replicaron en las cuentas Dropbox, Google Drive o OneDrive, porque al estar conectadas como unidad de red perfectamente podía ver también estos archivos y por ende, ser cifrados y eliminados también. La parte buena es que dentro de estos sistemas tienes la posibilidad de recuperar también los datos, ya que una vez cifraron tus datos en la nube también eliminaron los archivos originales, por lo que si te han infectado en la nube, no te preocupes, es posible recuperarlos siguiendo este tutorial.