Por: Grupo de Seguridad de la Información de la Dirección de Telemática

Abril 2016

¿Qué es un Ransomware?

Es un tipo de malware que infecta a sistemas o equipos informáticos (PC, servidores, dispositivos móviles, etc.), restringiendo su acceso a los usuarios de los sistemas una vez infectados a cambio de un rescate (de ahí viene su nombre en inglés por "*ransom*" - rescate, y "*ware*" - software).

- Algunas variantes de ransomware por lo general tratan de extorsionar a las víctimas mediante la visualización de una alerta en pantalla.
- Frecuentemente estas alertas afirman que los sistemas de los usuarios se han bloqueado, o bien que los archivos del usuario han sido cifrados.
- En ocasiones solamente la información valiosa del usuario es cifrada (como documentos, fotos, vídeos, etc.), aunque algunos tipos de ransomware pueden cifran incluso los archivos del sistema operativo, inutilizando completamente el equipo afectado y coaccionando al usuario a pagar el rescate solicitado.
- El ransomware notifica a los usuarios afectados que de no pagarse el rescate, el acceso a su equipo no será restaurado o su información se perderá de forma permanente.
- El monto del rescate exigido es variable, pero normalmente oscila entre los 200 y 400 dólares.
- La forma de pago más común usada por el ransomware es la moneda virtual como el Bitcoin, en algunos casos solicitan el pago por vale pre-pago anónimo como MoneyPak, o incluso en raros casos por SMS.

¿Cómo se propaga?

1. Por correos electrónicos de phishing que contienen datos maliciosos.
2. Por medio de algún recurso externo infectado que se conecte al equipo, como una unidad de red, o algún dispositivo USB.
3. Un sitio web infectado que facilita la descarga de un malware en el equipo, sin el conocimiento del usuario.
4. Mediante un instalador o una actualización de un sistema o software legítimo previamente instalado (Adobe, Windows, etc.), pero descargando dicho instalador desde un sitio web no autorizado.

¿Por qué es tan eficaz?

La ingeniería social aplicada en los ransomware es diseñada para infundir miedo entre sus víctimas, facilitando la disposición de la persona afectada para acceder a los recursos que el ransomware le brinda para pagar un rescate, a cambio de su información. Algunos mensajes intimidatorios son similares a los siguientes:

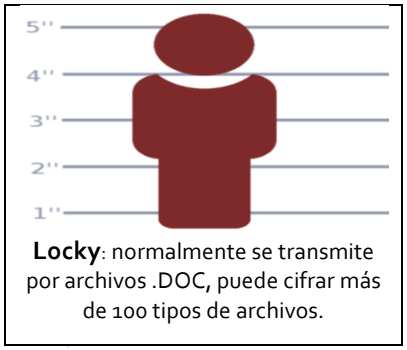
- "Su equipo ha sido infectado con un virus. Haga click aquí para resolver el problema".
- "Su computadora ha sido utilizada para visitar sitios web con contenido ilegal. Para desbloquear el equipo deberá pagar una multa de $100 USD".
- "Todos los archivos de su equipo han sido cifrados. Para recobrar el acceso a su información deberá pagar este rescate dentro de las próximas 72 horas".

¿Cuál es su impacto?

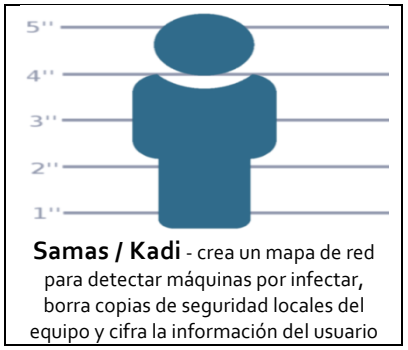
El ransomware no sólo se enfoca en usuarios domésticos, las empresas también pueden infectarse y enfrentar consecuencias negativas, como las siguientes:

- Pérdida temporal o permanente de información confidencial o propietaria.
- Interrupción de las operaciones regulares.
- Pérdidas financieras derivadas de las acciones tomadas para restaurar sistemas y archivos.
- Daño potencial a la reputación de una organización o empresa.

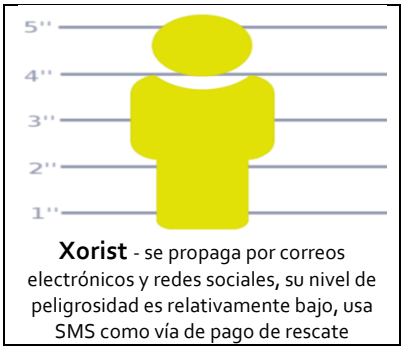
Algunas variantes de ransomware:



Locky: normalmente se transmite por archivos .DOC, puede cifrar más de 100 tipos de archivos.

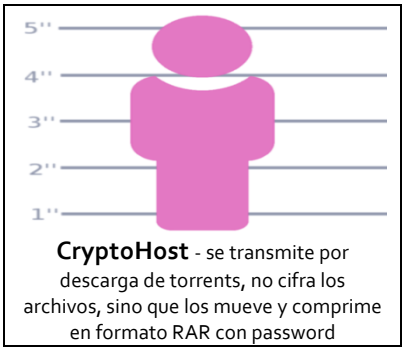


Samas / Kadi - crea un mapa de red para detectar máquinas por infectar, borra copias de seguridad locales del equipo y cifra la información del usuario



Xorist - se propaga por correos electrónicos y redes sociales, su nivel de peligrosidad es relativamente bajo, usa SMS como vía de pago de rescate

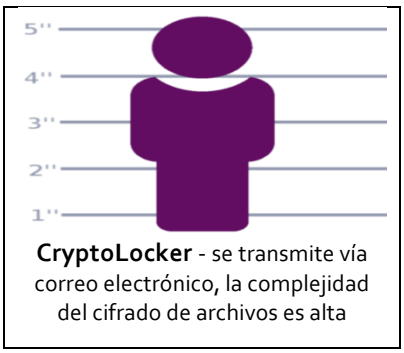
CryptorBit - cifra los archivos pero no los libera, a pesar de que el usuario realice el pago por una clave



CryptoHost - se transmite por descarga de torrents, no cifra los archivos, sino que los mueve y comprime en formato RAR con password

KeRanger - se transmite por descarga de torrents, afecta a equipos Mac

CryptoWall - uno de los más activos, tiene muchas variantes, la versión 4 puede incluso cifrar los nombres de archivos



CryptoLocker - se transmite vía correo electrónico, la complejidad del cifrado de archivos es alta

¿Cómo prevenir un ransomware?

1. Realice periódicamente respaldos de su información, y guarde sus respaldos en lugares externos a su equipo.
2. No ejecute o abra archivos que vienen atados a correos electrónicos, sin antes asegurarse que el correo es legítimo, o que fue enviado por quien dice ser (un contacto válido para usted).
3. Mantenga actualizado el sistema operativo.
4. Mantenga actualizado su sistema anti-virus.
5. Instale software anti-spyware, anti-malware y realice revisiones periódicas en su equipo para prevenir y/o eliminar spyware, malware.
6. Evite navegar por páginas no seguras o con contenido no verificado.
7. Evite compartir discos o mantener mapeo a discos externos en red.

¿Qué hacer en caso de ser infectado?

- Si ya es víctima de un ransomware, POR NINGÚN MOTIVO realice el pago solicitado por la clave o llave privada para descifrar los archivos, pues de acuerdo a los reportes, en la mayoría de los casos no envían la clave, o dicha clave no funciona; además de que al hacerlo estaría brindando a desconocidos información personal o financiera.
- En caso de ser víctima de un ransomware, contacte a su soporte técnico, en CICESE a través de la **Mesa de Servicios de Telemática**, o marcando la extensión **611**.

Referencias:

- Alert TA16-091A - Ransomware and Recent Variants (https://www.us-cert.gov/ncas/alerts/TA16-091A)
- Wikipedia - Ransomware (https://es.wikipedia.org/wiki/Ransomware)
- Blog SATINFO - Solucionado el descifrado del ransomware Cryptohost (http://www.satinfo.es/blog/2016/solucionado-el-descifrado-del-ransomware-cryptohost)
- RedesZone - CryptorBit, un malware que cifra los datos de tu disco y no los libera (http://www.redeszone.net/2014/01/28/cryptorbit-un-malware-que-cifra-los-datos-de-tu-disco-y-no-los-libera/#sthash.CUI28fsg.dpuf)
- RedesZone - KeRanger, el ransomware para Mac OS X, es una copia de Linux Encoder (http://www.redeszone.net/2016/03/10/keranger-ransomware-mac-os-x-una-copia-linux-encoder)