BOLETÍN DE ALERTA

Boletín Nro.: 2015-12
Fecha de publicación: 06/11/2015
Tema: Ransomware: CryptoWall, CTB-Locker, SimpleLocker y otras amenazas

Descripción:

¿Qué es el Ransomware?

Ransomware es un tipo de software malicioso (malware) que infecta un dispositivo y restringe el acceso al mismo, o a una parte del mismo, en la mayoría de los casos, encriptando documentos personales hasta que la víctima pague un "rescate" exigido por el malware para desbloquearlo. Normalmente intenta extorsionar a las víctimas mediante la visualización de una alerta en pantalla. Estas alertas a menudo afirman que su ordenador ha sido bloqueado o que todos sus archivos se han cifrado, y se exige que se pague un rescate para restaurar el acceso. Dependiendo de la variante, este rescate puede ir desde los US$ 50 hasta US$ 2000 dólares, y en algunas ocasiones se exige en moneda virtual, como Bitcoin.

Existen muchas variantes, que afectan a diversos tipos de sistemas operativos, cada una de las cuales tiene características y comportamientos particulares.

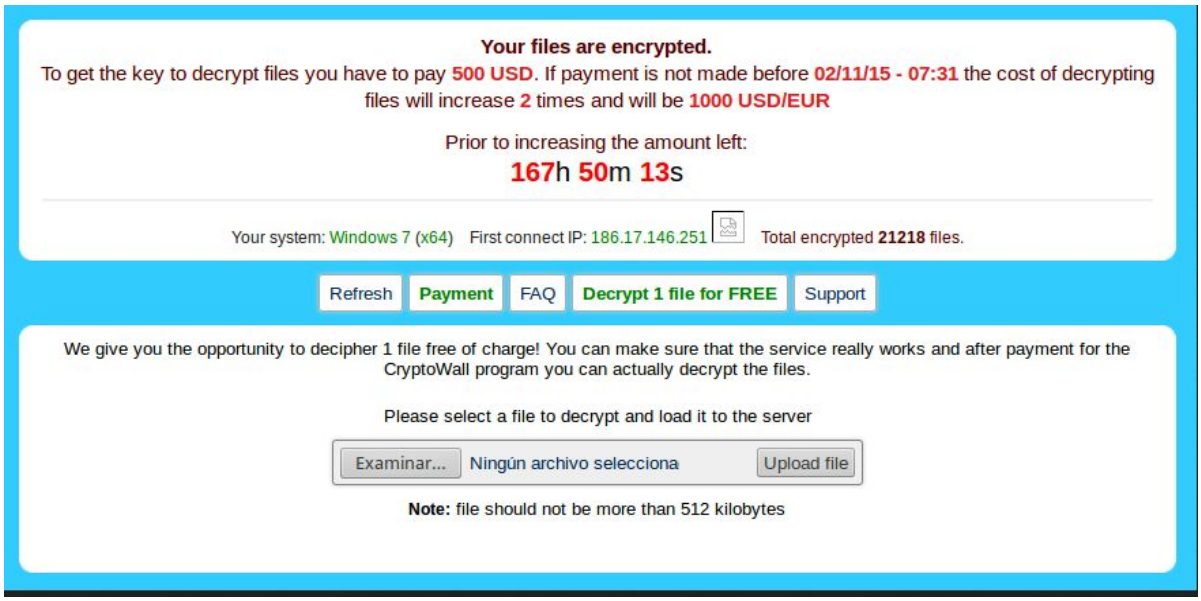

Figura 1: Ejemplo de una variante de Ransomware (CryptoWall 3.0)

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Los autores del ransomware tratan de infundir miedo y pánico en sus víctimas, haciendo que accedan al pago de un rescate o que hagan click en otro enlace que los infecta con malware adicional. Normalmente utilizan mensajes como:

- "El equipo ha sido infectado con un virus. Haga clic aquí para resolver el problema ".
- "Se utilizó el ordenador para visitar sitios web con contenido ilegal. Para desbloquear el equipo, deberá pagar una multa de US$ 100 ".
- "Todos los archivos de su equipo se han cifrado. Usted debe pagar este rescate dentro de las 72 horas para recuperar el acceso a sus datos ".

Para aumentar la presión a la víctima, muchas variantes establecen un tiempo límite en el que esperan recibir el pago.

¿Qué sistemas operativos afecta?

Se han detectado numerosas variantes que afectan a varias versiones de Windows: CryptoLocker, CryptoWall, CBT-Locker, Virus de la Policía (Reveton), POSHCoder, entre otros.
Sin embargo se ha detectado también variantes que afectan a dispositivos móviles, como por ejemplo SimpleLocker que afecta a Android o el ataque de Oleg Pliss que afectó a iOS.

¿Cómo se transmite?

El Ransomware se transmite de diversas formas:

- Correos electrónicos de phishing que contienen archivos adjuntos maliciosos o enlaces maliciosos.
- Drive-by-Download: la descarga del malware se realiza de forma automática cuando un usuario visita un sitio web infectado, sin que lo sepa, y se instala automáticamente explotando alguna vulnerabilidad.
- Redes sociales: mensajes, noticias o videos falsos que redirigen a sitios infectados.
- Aplicaciones de mensajería instantánea basada en la web.

Impacto:

El ransomware busca restringir o bloquear el acceso al sistema operativo y/o a los archivos del mismo cifrándolos. Algunas variantes cifran ciertos tipos de archivos (por ejemplo, todos los documentos e imágenes); otras variantes restringen el acceso a recursos del sistema operativo, impidiendo que el usuario salga de la pantalla de advertencia.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Las campañas de distribución de Ransomware no sólo están dirigidas a usuarios domésticos, sino también a las empresas, en las que el impacto a veces es mayor. La mayoría de las variantes de ransomware generan consecuencias, entre ellas:

- Pérdida temporal o permanente de información confidencial o de propiedad;
- La interrupción de las operaciones regulares, principalmente en los negocios o empresas;
- Las pérdidas financieras contraídas para restaurar los sistemas y archivos; y
- Daño potencial a la reputación de una organización.

Pagar el rescate no puede garantizar que los archivos cifrados serán recuperados; además, desencriptar los archivos no significa que la infección de malware en sí se ha eliminado.

Mitigación y Prevención:

Debido a que por lo general el ransomware utiliza mecanismos de encriptación no reversibles, la mayoría de las veces no existen mecanismos para desencriptar los archivos sin la clave que está en poder de los atacantes.

Es por esto que las acciones preventivas son fundamentales:

- Realizar copias de seguridad (backup) de toda la información crítica para limitar el impacto de la pérdida de datos o del sistema y para facilitar el proceso de recuperación. Idealmente, estos datos se debe mantener en un dispositivo independiente, y las copias de seguridad se deben almacenar offline.
- Contar con soluciones de antivirus y mantenerlo actualizado, de modo a prevenir la infección.
- Mantener su sistema operativo y el software siempre actualizado, con los últimos parches.
- No ingresar a enlaces dudosos que le son enviados a través de correo electrónico, servicios de mensajería, redes sociales, etc.
- Evitar abrir correos sospechosos,tanto si vienen de usuarios conocidos como desconocidos. Asegurarse siempre de que la persona que le ha enviado el correo realmente le quería remitir ese adjunto.
- Tener cuidado con todos los archivos adjuntos, especialmente aquellos que vienen comprimidos en formato zip. Incluso los archivos aparentemente inofensivos, como los documentos de Microsoft Word o Excel, pueden contener un virus, por lo que es mejor ser precavido.
- La mayoría de los clientes de correo electrónico ofrecen la posibilidad de hacer visible todas las extensiones de los archivos adjuntos recibidos. Aconsejamos habilitar esta función para saber exactamente qué tipo de archivo se nos envía.
- No acceder a ningún pago u acción exigida por el atacante.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Uno de los vectores de infección más frecuentes es la explotación de plugins vulnerables del navegador (Adobe Flash Player, Java, etc.) mediante drive-by-download. Algunas recomendaciones específicas para evitarlo son:

- Evitar la ejecución automática de plugins como Adobe Flash Player, Java, etc. La mayoría de los navegadores modernos permiten configurarlo de modo a que se solicite permiso al usuario cada vez que un sitio web intente ejecutar un plugin. Para ello puede ir a la Configuración o Opciones de su navegador.
    - En Google Chrome, escribir "chrome://settings/content/" en la barra de navegación y en la sección "Complementos", seleccionar "Permitirme decidir cuándo ejecutar contenido de plugins".
    - En Mozilla Firefox, escribir "about:addons" en la barra de navegación y en cada plugin deseado, seleccionar la opción "Preguntar para activar".
- Contar con mecanismos de protección contra la publicidad invasiva, muy ligada al malvertising (anuncios maliciosos embebidos en la web). Existen complementos muy útiles como AdBlock Plus, disponible para varios sistemas operativos y navegadores: https://adblockplus.org/es/

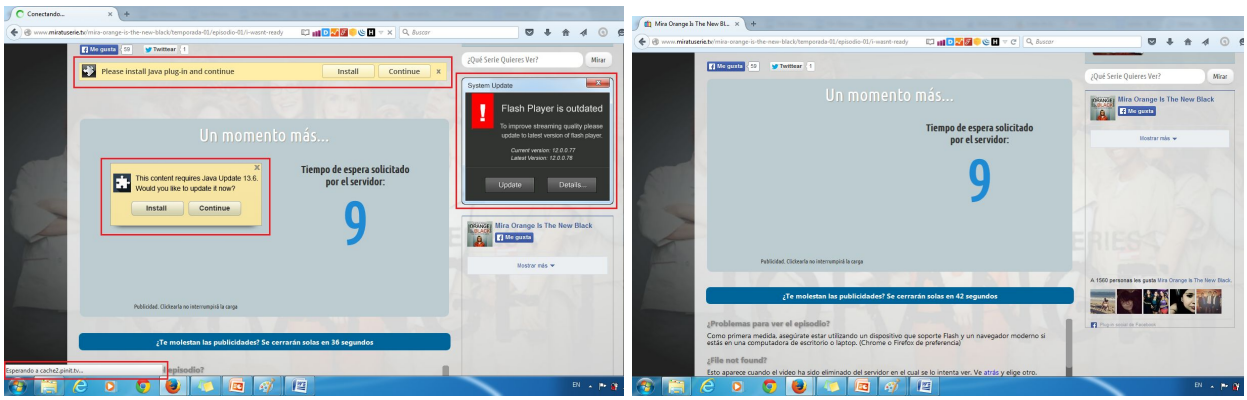

Figura 2: Ejemplo de filtrado de publicidad maliciosa con AdBlock Plus

- Evitar la ejecución automática de Javascript. Existen complementos como No-Script y ScriptSafe que deshabilitan por defecto la ejecución de Javascript, permitiendo al usuario habilitarlo sólo en las páginas en las que confía.
  https://addons.mozilla.org/es/firefox/addon/noscript/
  https://chrome.google.com/webstore/detail/scriptsafe/oiigbmnaadbkfbmpbfijlflahbdbdgdf

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Para más información sobre la técnica de drive-by-download, lea nuestro boletin: http://www.cert.gov.py/index.php/download_file/view/392/188

En algunos casos, algunas variantes de ransomware pueden ser eliminadas y los archivos recuperados sin necesidad de pagar, tal como SimpleLocker o TorLocker, los cuales tenían vulnerabilidades que han podido ser utilizadas para que se desarrollen herramientas para desencriptar los archivos. Sin embargo, para la gran mayoría de los casos no existe una manera de desencriptar los archivos.

Cuando un equipo fue infectado por un ransomware, es importante no modificarlo: no se debe eliminar archivos ni reinstalar el sistema operativo, hasta tanto se haya realizado un análisis detallado de la infección, que debe ser llevado a cabo por expertos en la materia. En caso de víctima de ransomware se recomienda realizar la denuncia a los organismos correspondientes; puede reportarlo al Centro de respuestas ante Incidentes Cibernéticos (CERT-PY).

Información adicional:

http://www.welivesecurity.com/la-es/2014/06/10/todo-sobre-ransomware-guia-basica-preguntas-frecuentes/
http://blogs.protegerse.com/laboratorio/2015/01/20/siguen-proliferando-las-infecciones-por-ramsonware-algunos-consejos-utiles/
http://www.welivesecurity.com/la-es/2015/06/30/cryptowall-3-vulnerabilidad-flash-player/
http://www.welivesecurity.com/la-es/2015/03/16/teslacrypt-ransomware-cifra-videojuegos
https://www.us-cert.gov/ncas/alerts/TA14-295A
http://www.fbi.gov/news/stories/2015/january/ransomware-on-the-rise/ransomware-on-the-rise
http://www.welivesecurity.com/la-es/2015/01/20/ctb-locker-ransomware-ataca-nuevo
http://digital-forensics.sans.org/blog/2014/09/09/torrentlocker-unlocked

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py