BOLETÍN DE ALERTA

Boletín Nro.: 2015-15
Fecha de publicación: 01/12/2015
Tema: Campaña de distribución de Cryptowall en el país

Descripción:

Recientemente se ha observado un enorme aumento de casos de ransomware en el país, distribuido a través de correos electrónicos. Se ha identificado una campaña de distribución del ransomware CryptoWall, muy específica, que está afectando mayormente a nuestro país.

¿Qué es el Ransomware?
Ransomware es un tipo de software malicioso (malware) que infecta un dispositivo y restringe el acceso al mismo, en la mayoría de los casos, encriptando documentos personales hasta que la víctima pague un "rescate" exigido por el malware para desencriptarlos.

¿Cómo se transmite?
Si bien, el Ransomware se puede transmitir de diversas formas, hemos observado una campaña de distribución específica a través de correo electrónico.
Los correos electrónicos tienen como asunto una fecha y una hora, por ejemplo: "**12/1/2015 6:16:21 AM**". Los remitentes por lo general son desconocidos.
Los correos electrónicos contienen un archivo adjunto comprimido .zip, con diferentes nombres, por ejemplo: info.zip, img.zip, love.zip, etc. Estos archivos adjuntos contienen un archivo javascript que al ser abiertos se ejecutan de forma automática y descargan, ejecutan e instalan el ransomware Cryptowall.
Una vez que se abrió el archivo adjunto, la máquina queda infectada por CryptoWall y los archivos que se encuentran en dicha máquina quedan automáticamente encriptados.
Se ha observado que esta campaña de correo está siendo enviada a ciudadanos paraguayos de diversas industrias: gobierno, educativo, empresas de tecnología, PYMES, etc. Cuando una persona queda infectada por CryptoWall, es frecuente que las personas de la libreta de direcciones almacenadas en la máquina, reciban también correos electrónicos maliciosos, agrandándose así el círculo de personas afectadas.

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

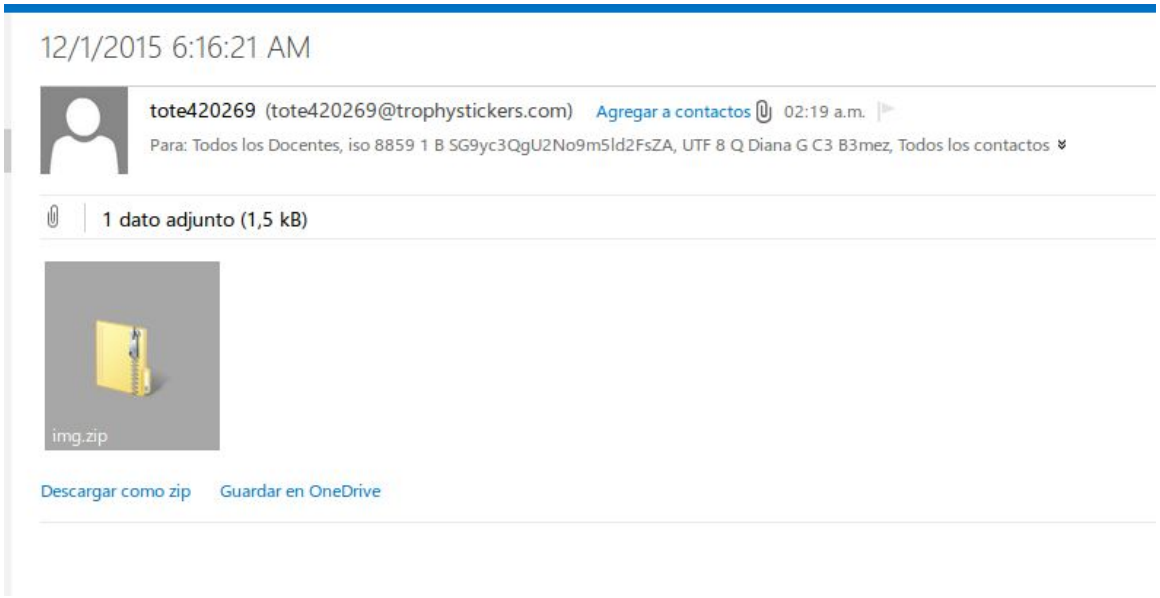

Figura 1: Correo de distribución del downloader de CryptoWall

¿Cómo funciona CryptoWall?

Al quedar infectado por Cryptowall, inmediatamente aparece una alerta en pantalla (ver Figura 2), alertando que los todos sus archivos se han cifrado y mostrando en pantalla las instrucciones para pagar el rescate y recuperar los archivos (ver Figura 3).

Para proceder al pago, se indican unas URLs en pantalla, con instrucciones específicas para la víctima infectada. El rescate exigido empieza en US$ 500 y va aumentando hasta llegar a US$ 1000 dólares; se exige en la moneda virtual Bitcoin (ver Figura 4).

Para aumentar la presión a la víctima, el ransomware establece un tiempo límite en el que esperan recibir el pago, antes de aumentar el pago exigido.

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

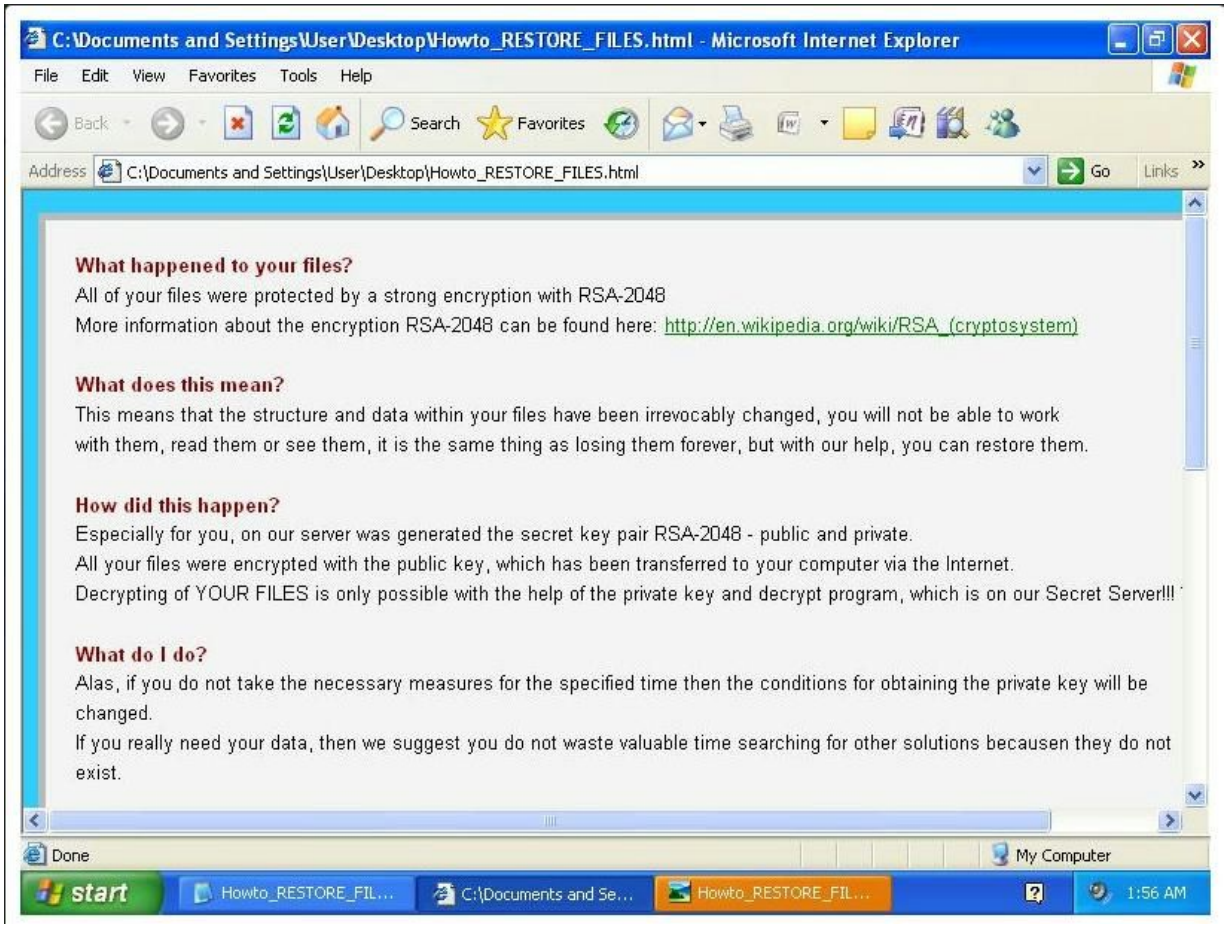

Figura 2: Mensaje de alerta por CryptoWall

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

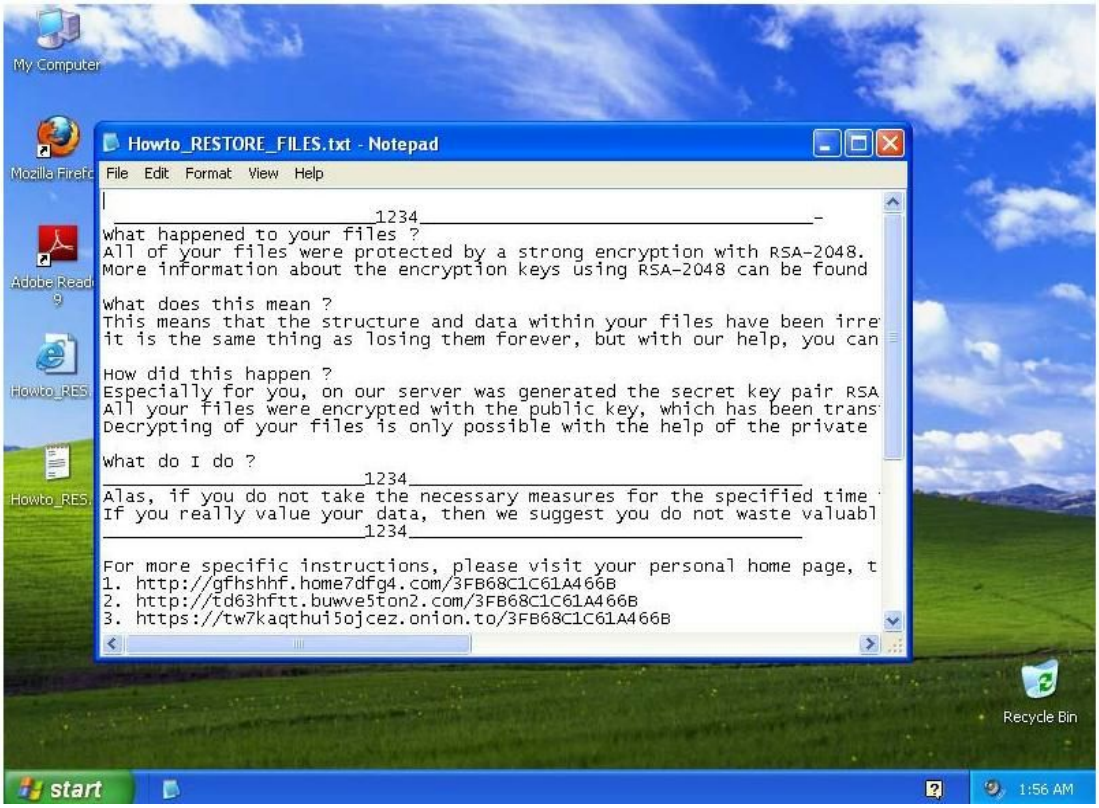

Figura 3: Instrucciones proporcionadas por CryptoWall

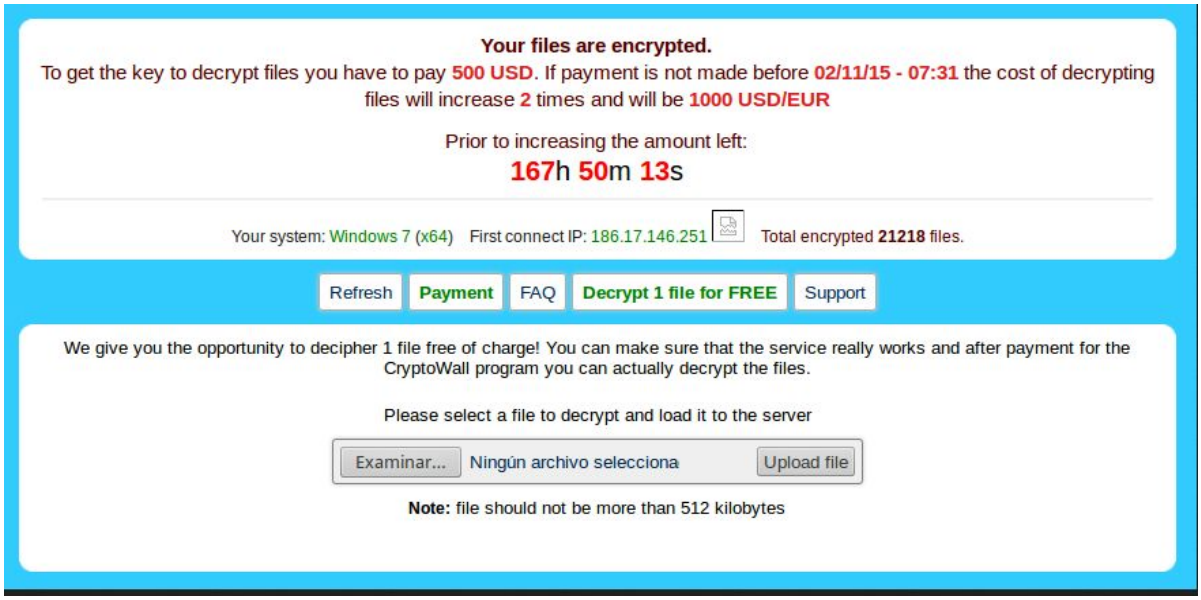

Figura 4: Instrucciones específicas para el pago

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

¿Qué sistemas operativos afecta?
CryptoWall afecta a equipos que cuentan con sistema operativo Windows.

Impacto:
El ransomware CryptoWall encripta los archivos usando estándares de encriptación robusta (RSA-2048), la cual no es reversible, por lo tanto lleva a una pérdida de los archivos.
Esto genera enormes daños, entre ellos:

- 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.

Mitigación y Prevención:
Debido a que CryptoWall utiliza mecanismos de encriptación no reversibles, hasta el momento no existen mecanismos para desencriptar los archivos sin la clave que está en poder de los atacantes.
Por lo general, las herramientas que se ofrecen en Internet para desencriptar archivos encriptados por ransomware (específicamente para CryptoWall) son en su mayoría software malicioso, por lo que al tratar de desencriptar los archivos, se corre un alto riesgo de quedar infectado con más malware.

Es por esto que las acciones preventivas son fundamentales:

- No abrir nunca 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.
- Evitar abrir los archivos adjuntos sospechosos. Incluso los archivos aparentemente inofensivos, como los documentos de Microsoft Word o Excel, pueden contener un virus, por lo que es mejor ser precavido.
- No ingresar a enlaces dudosos que le son enviados a través de correo electrónico, servicios de mensajería, redes sociales, etc.
- 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.

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

- 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 acceder nunca a ningún pago u acción exigida por el atacante.

En caso de recibir un correo electrónico con las características mencionadas en este boletín, recomendamos no abrirlo y dar aviso a un responsable de su organización.
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/
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

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