Boletin de Seguridad UNAM-CERT-2014-014 Crypto Ransomware

Ransomware es un tipo de software malicioso que infecta una computadora y restringe el acceso a la misma hasta que se paga un rescate para desbloquearla. El crypto ransomware además de bloquear cifra archivos.

- **Fecha de Liberación:** 22-Oct-2014
- **Ultima Revisión:** 23-Oct-2014
- **Fuente:** https://www.us-cert.gov/ncas/alerts/TA14-295A

1. Descripción

Ransomware es un tipo de software malicioso que infecta una computadora y restringe el acceso a la misma hasta que se paga un rescate para desbloquearla. Ésta alerta es el resultado del análisis del Centro Canadiense de Respuesta a Incidentes Cibernéticos (CCIRC, por sus siglas en inglés) en coordinación con el Departamento de Seguridad Nacional de los Estados Unidos (DHS, por sus siglas en inglés) para proveer información adicional sobre crypto ransomware, una variante que cifra la información de los usuarios afectados, específicamente para:

- Presentar sus principales características, explicar la prevalencia del ransomware y la proliferación de variantes que hacen uso de sistemas criptográficos (crypto ransomware).
- Ofrecer información sobre prevención y mitigación.

2. ¿Qué es el ransomware?

Ransomware es un tipo de software malicioso que infecta una computadora y restringe el acceso a la misma. Éste tipo de malware, que ha sido observado por varios años, intenta extorsionar a las víctimas y hacerlas pagar al desplegar una alerta en pantalla. Estas alertas usualmente aseguran que la computadora ha sido bloqueada, o que todos los archivos han sido cifrados, y exigen que se pague un rescate para reestablecer el acceso. El rescate usualmente oscila entre los $100 y $300 dólares, y algunas veces se exige el pago a través de una moneda virtual, como Bitcoin.

El ransomware es típicamente distribuido a través de correos phishing que contienen adjuntos maliciosos y mediante instalación por descarga. La instalación por descarga ocurre cuando un usuario vista un sitio infectado y el malware es descargado e instalado de manera automática, sin conocimiento del usuario. El crypto ransomware, una variante que cifra los archivos, es distribuido a través de métodos similares y ha sido distribuido mediante aplicaciones web de mensajería instantánea.

3. ¿Por qué es tan efectivo?

Los autores del ransomware inducen miedo y pánico a sus víctimas, haciendo que sigan un enlace o paguen un rescate, ocasionando que se infecten como más malware. Algunos de los mensajes usados por los atacantes son:

- Su computadora ha sido infectada con un virus. Haga clic aquí para remover la infección.
- Su computadora fue usada para visitar sitios web con contenido ilegal. Para desbloquear su equipo debe pagar una multa de $100USD.
- Todos los archivos en tu computadora han sido cifrados. Debes de pagar el rescate en menos de 72hrs para tener acceso a tus datos.

4. Proliferación de variantes

En 2012, Symantec, usando datos de un servidor *Command and Control* (C&C) de 5,700 computadoras infectadas en un mismo día, estimó que aproximadamente el 2.9% de los usuarios infectados pagó el rescate. Con un rescate promedio de $200 USD, los atacantes consiguieron ganancias por $33,600 USD al día, o $394,400 USD al mes con un solo servidor C&C.

El éxito financiero de este ataque ha impulsado la proliferación de variantes. En 2013 surgieron variantes más destructivas y lucrativas como *Xorist*, *CryptorBit* y *CryptoLocker*. Algunas variantes no solo cifran los archivos del sistema afectado, sino que también afectan archivos compartidos o discos en red. Éstas variantes son consideradas destructivas porque cifran los archivos del usuario y la organización, volviéndolos inservibles hasta que los criminales reciben el rescate.

Entre las variantes observadas en 2013 se encuentra *CryptoDefense* y *Cryptowall*, las cuales también son consideradas como destructivas. Informes indican que *CryptoDefense* y *Cryptowall* comparten el mismo código y solo difieren en el nombre. Al igual que *CryptoLocker*, estas variantes cifran los archivos en el equipo local, así como los archivos compartidos por red y dispositivos removibles.

5. Ligas a otro tipo de malware

Frecuentemente, los sistemas infectados por ransomware también son infectados por otro tipo de malware. En el caso de *CryptoLocker*, un usuario se infecta al abrir un adjunto malicioso en un correo electrónico. Éste adjunto malicioso contiene Upatre, malware que descarga una variante de *GameOver Zeus*. *GameOver Zeus* es una variante del troyano *Zeus*, el cual roba información sobre banca electrónica y es usado para robar otro tipo de datos. Un vez que el sistemas es infectado con *GameOver Zeus*, Upatre descarga *CryptoLocker*. Finalmente, *CryptoLocker* cifra los archivos en el sistema infectado y solicita el pago del rescate.

La estrecha relación entre el ransomware y otro tipo de malware quedó demostrada tras la reciente operación en contra de la botnet usada por *GameOver Zeus*, que también tuvo efecto contra *CryptoLocker*. En junio de 2014, una operación internacional logró exitosamente debilitar la infraestructura usada por *GameOver Zeus* y *CryptoLocker*.

6. Impacto

El ransomware no solo tiene como objetivo usuarios caseros, los equipos usados en la industria también pueden ser infectados, lo que podría generar consecuencias negativas como:

- Pérdida temporal o permanente de información sensible o propietaria

- Interrupción de operaciones
- Pérdidas financieras causadas al restaurar sistemas y archivos
- Daño potencial a la reputación de la organización

Pagar un rescate no garantiza que los archivos serán descifrados, solo garantiza que los atacantes recibirán el dinero de la víctima y posiblemente su información bancaria. Además, descifrar los archivos no significa que la infección sea removida.

7. Solución

Éstas infecciones pueden ser devastadoras para un usuario o una organización, la recuperación puede ser un proceso difícil que tal vez requiera los servicios de un especialista en recuperación de datos.

Para proteger redes de computadoras de una infección por ransomware US-CERT y CCIRC recomiendan a usuarios y administradores las siguientes medidas preventivas:

- Realizar respaldos regulares de toda la información crítica para limitar el impacto causado por la pérdida de datos o sistemas y ayudar en el proceso de recuperación. Idealmente, estos datos deben ser almacenados en un dispositivo diferente y los respaldos no deben estar conectados a la red.
- Tener un antivirus actualizado.
- Actualizar el sistema operativo y otro software con los parches más recientes.
- No seguir enlaces en correos no solicitados.
- Tener precaución al abrir archivos adjuntos en correos electrónicos,
- Seguir prácticas seguras al navegar en Internet.

Se recomienda a usuarios y organizaciones no pagar rescate, ya que pagar no garantiza recuperar los archivos afectados. Adicionalmente se recomienda reportar estos casos de ransomware a las autoridades locales, por ejemplo, en México puede reportar a malware@cns.gob.mx para dar seguimiento legal. Para reportar un sitio que distribuye malware o correos con archivos adjuntos maliciosos puede escribir a malware@seguridad.unam.mx.

8. Referencias

http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-detects-mobile-Trojan-Svpeng-Financial-m
http://www.cod.edu/about/information_technology/security/pdf/ransomware20131031_cryptolocker.pdf
http://nakedsecurity.sophos.com/2014/06/18/whats-next-for-ransomware-cryptowall-picks-up-where-cryptoloc
http://www.symantec.com/connect/blogs/cryptodefense-cryptolocker-imitator-makes-over-34000-one-month
http://www.symantec.com/connect/blogs/cryptolocker-thriving-menace
http://www.symantec.com/connect/blogs/cryptolocker-qa-menace-year
http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Demian Roberto Garcia Velazquez (dgarcia at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez at seguridad dot unam dot mx)

UNAM-CERT
Equipo de Respuesta a Incidentes UNAM
Subdirección de Seguridad de la Información

incidentes at seguridad.unam.mx
phishing at seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 47