Subdirección de Seguridad de la Información - UNAM-CERT -- DGTIC-UNAM

Nota de Seguridad UNAM-CERT-2015-001 Uso masivo del Ransomware CTB-Locker para pedir rescate por información

Ransomware es un tipo de software malicioso secuestrador de información, sesión o navegador del usuario. Los mantiene bloqueados o cifrados hasta que la víctima paga para recuperar la información y/o el control del sistema [1].

- **Fecha de Liberación:** 10-Feb-2015
- **Ultima Revisión:** 10-Feb-2015
- **Fuente:**
- **Riesgo** Importante
- **Problema de Vulnerabilidad** Local

1. Descripción

El software malicioso CTB-Locker cifra los archivos de la víctima para pedir un rescate por ellos. Recientemente, UNAM-CERT ha observado que los ataques inician con correos electrónicos phishing que contienen un archivo ZIP malicioso adjunto, que a su vez contiene otro archivo comprimido con el mismo nombre y éste último aloja un binario con extensión SCR que es el downloader. Una vez que se ejecuta, abre un documento en Microsoft Word (incluido en el software malicioso) y se descarga el ransomware identificado como *"CTB-Locker"*, *"FileCoder"* o *"Critroni"*, que cifra archivos en el equipo comprometido y solicita el pago del rescate en bitcoins.

De acuerdo la firma de seguridad ESET, México es el país de Latinoamérica más afectado por este tipo de amenaza [2]. A continuación se muestran algunos indicadores encontrados en la campaña observada por UNAM-CERT [3]:

Características del correo electrónico Phishing:

- Asunto: Fax2mail
- Adjunto: nonchalantly.zip | attornment.zip

Características a nivel de sistema:

- El ejecutable SCR descarga el archivo: pack.tar.gz
- El ransomware se copia a sí mismo en la ruta: C:\Users\[NombreDeUsuario] \AppData\Local\Temp\sgxxnjk.exe [4]
- En la carpeta "Documentos" crea dos archivos: "Decrypt All Files [TerminaciónAleatoria].txt" y "Decrypt All Files [TerminaciónAleatoria].bmp"

2. Impacto

Un sistema infectado con alguna variante del software malicioso CTB-Locker puede generar consecuencias negativas como:

- Pérdida temporal o permanente de información
- Interrupción en la continuidad del negocio

- Pérdidas financieras por la restauración de sistemas y archivos
- Afectar la reputación de la organización

3. Solución

Una vez que CTB-Locker infecta el equipo, inicia el cifrado de archivos y aparece un mensaje solicitando el rescate, por lo que en un sistema infectado se pueden tomar las siguientes medidas:

- Apagar el equipo inmediatamente para evitar que CTB-Locker continúe cifrando archivos.
- Recuperar los archivos que no hayan sido cifrados, desde un sistema limpio.

El cifrado de archivos por este tipo de amenazas hace prácticamente imposible recuperarlos, por lo que se recomienda a los usuarios y organizaciones tener en cuenta las siguientes medidas preventivas de seguridad:

- Generar respaldos de su información periódicamente [5].
- Si la organización cuenta con una solución de seguridad para servidores de correo, habilitar la funcionalidad de filtrado por extensiones para alertar o bloquear archivos ".scr" y ".exe".
- Evitar abrir archivos adjuntos sospechosos en los correos electrónicos [6].
- Actualizar las soluciones antivirus, las aplicaciones instaladas en el equipo y el sistema operativo con los últimos parches de seguridad [7].

Es importante tomar en cuenta que el pago del rescate no garantiza recuperar los archivos.

4. Reportar incidentes

UNAM-CERT gestiona reportes de phishing y sitios web que alojan páginas falsas o software malicioso para buscar evitar que más usuarios se conviertan en víctimas.

- Reportar correos de phishing a phishing@seguridad.unam.mx.
- Para reportar un sitio que distribuye malware o correos con archivos adjuntos maliciosos puede escribir a malware@seguridad.unam.mx

5. Referencias

[1] Crypto Ransomware
[2] CTB-Locker en Latinoamérica: ¿cuál es el país más afectado?
[3] Ransomware CTB-Locker, propagación masiva
[4] Reporte del análisis en VirusTotal. Recuperado el 9 de febrero de 2015
[5] Copias de seguridad y recuperación personal
[6] Qué hacer y qué no hacer con el correo electrónico
[7] Siete pasos para tener una computadora segura

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

- Jonathan Banfi Vázquez (jbanfi 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