Subdirección de Seguridad0 0.la Información - UNAM-CERT -- DGTIC-UNAM

Nota de Seguridad0UNAM-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

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 seguridad0ESET, México es el país de Latinoam g.4 a cde Lins.