Fuente:
ITConnect

El Laboratorio de Investigación de ESET Latinoamérica detectó una nueva variante de malware que cifra archivos y pide un rescate en bitcoins para recuperarlos.

El Laboratorio de Investigación de ESET Latinoamérica recibió múltiples reportes de una campaña de propagación de códigos maliciosos cuyo objetivo es cifrar los archivos de sus víctimas y pedir un rescate en **bitcoins** para recuperar la información. Se trata de **CTB-Locker**, un *ransomware* que se propaga a través de un falso correo electrónico que dice contener un fax y que está generado un gran impacto en Latinoamérica.

La campaña de propagación de este ataque comienza con un falso correo electrónico que llega a la bandeja de entrada de los usuarios. El asunto del correo simula ser un fax enviado al usuario con un adjunto, el mismo es detectado por las soluciones de ESET como *Win32/TrojanDownloader.Elenoocka.A*. Los usuarios que ejecuten esta amenaza tendrán todos sus archivos cifrados ya que este malware descarga un ransomware conocido como *Win32/FileCoder.DA*, y se les exigirá pagar un rescate en bitcoins para recuperar su información. Un ataque similar al que reportamos anteriormente con CryptoLocker.

El resultado es similar a **CrytoLocker** o **TorrentLocker**, los archivos con extensiones como mp4, .pem, .jpg, .doc, .cer, .db entre otros son cifrados por una clave. Una vez que el malware terminó de cifrar la información del usuario mostrará por pantalla un cartel de alerta y además cambiará el fondo del escritorio con un mensaje similar al que ven en la siguiente imagen:

Si bien el mensaje que ve la víctima afectada por este malware cuenta con traducción al alemán, holandés e italiano y no al español, el Laboratorio ha recibido un gran número de reportes de estas campañas de propagación en Latinoamérica. Según los sistemas de Alerta Temprana de ESET el ranking de los países más afectados en nuestra región es:

Frente a esta amenaza existen ciertas medidas de seguridad que se recomiendan para usuarios y empresas:
• Habilitar las funcionalidades de filtrado de extensiones posiblemente maliciosas en las soluciones de seguridad para servidores de correos. Esto ayudará a bloquear archivos con extensiones .scr como el caso de *Win32/TrojanDownloader.Elenoocka.A*.

• Evitar abrir adjuntos de dudosa procedencia en correos que no se ha identificado el remitente

• Eliminar los correos o marcarlos como Spam para evitar que otros usuarios o empleados de la empresa se

vean afectados por estas amenazas

• Mantener actualizadas las soluciones de seguridad para detectar las últimas amenazas que se están propagando.

“El impacto que esto puede tener para una empresa o un usuario que no cuenta con una solución de backup, es capaz de convertirse en un verdadero problema”, comentó Pablo Ramos, especialista en seguridad de ESET Latinoamérica. “Contrarrestar este tipo de ataques puede no ser una tareas sencilla y es necesario tomar una postura proactiva, apoyar a la tecnología con educación y por sobre todo estar atentos a los correos que se reciben.”

Disponible en:

http://itclat.com/2015/01/23/ctb-locker-010101/ [1]

Links
[1] http://itclat.com/2015/01/23/ctb-locker-010101/