25 años
NextVision
IT + SEGURIDAD

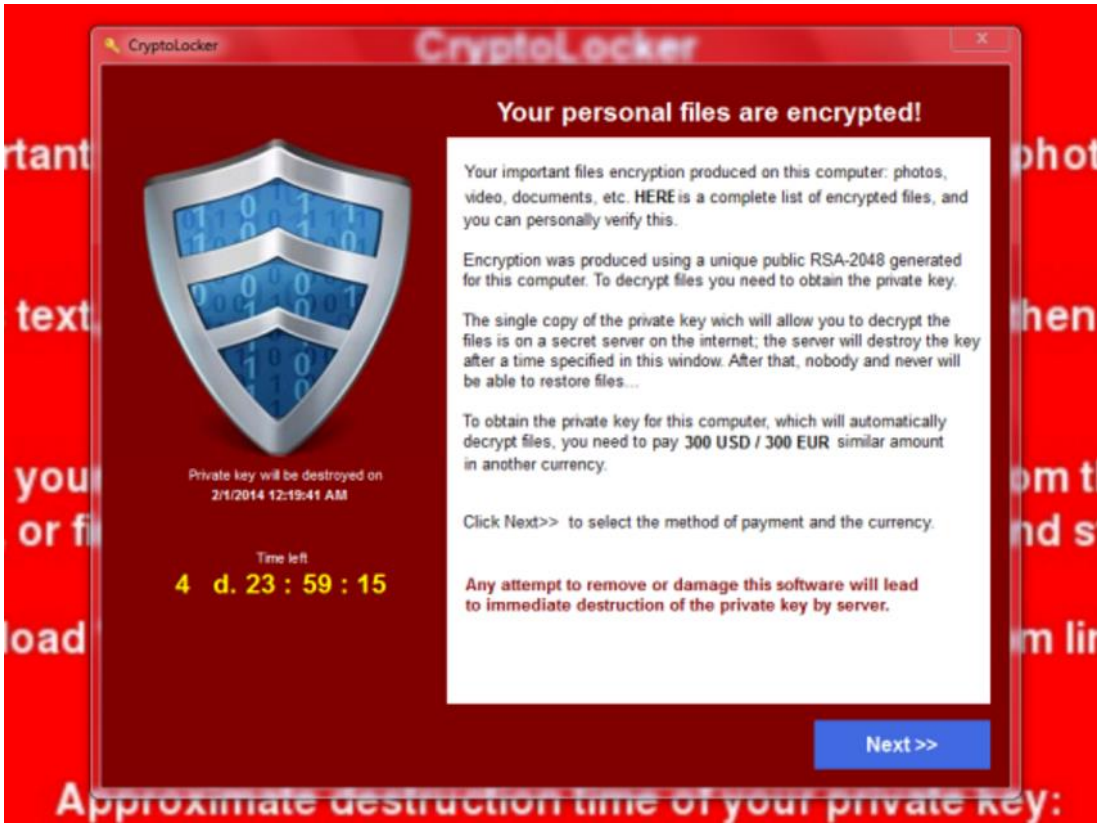
Cryptolocker

Qué es y cómo protegerse de esta amenaza.

nextvision.com

Cryptolocker, qué es?

- ✓ Cryptolocker es uno de los malware más peligrosos que se hayan conocido en los últimos años.
- ✓ Mediante un engaño al usuario final, logra que se ejecute el archivo adjunto que llega a través de un correo electrónico.
- ✓ Encripta (secuestra) documentos y pide dinero a cambio.
- ✓ **Una vez activado**: si el propietario no paga una suma de dinero en el plazo de tres o cuatro días a los creadores del malware, la clave con la que se bloquearon los archivos será borrada para siempre y por lo tanto la información será definitivamente inaccesible.


CryptoLocker
CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, video, documents, etc. HERE is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key wich will allow you to decrypt the files is on a secret server on the internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR similar amount in another currency.
Click Next>> to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to immediate destruction of the private key by server.
Next >>
Private key will be destroyed on
2/1/2014 12:19:41 AM
Time left
4 d. 23 : 59 : 15

¿Cómo prevenir la infección o defenderse?

- ✓ Mantener Actualizados
  - * El sistema antivirus
  - * Los parches de seguridad de sistemas operativos
  - * La herramienta AntiSpam

- ✓ Realizar campañas de concientización
- ✓ Prevenir la ejecución de archivos por políticas
- ✓ Mantener un cronograma de backup periódico
- ✓ Contar con soporte **profesional** del proveedor de seguridad

AntiVirus actualizado

Si bien no todas las **variantes del Cryptolocker** son detectadas por los antivirus, mantener el antivirus actualizado se considera una buena práctica ya que se van incorporado la mayoría de las variantes conocidas dentro de la categoría del Cryptolocker.

Parches de seguridad de sistemas operativos actualizados

Mantener los sistemas operativos con los últimos parches de seguridad actualizados permite minimizar los riesgos de ataques sobre vulnerabilidades detectadas.

De acuerdo a lo expresado por Microsoft, están trabajando periódicamente en actualizaciones que minimizan los riesgos relacionados con este tipo de malware.

Herramienta de AntiSpam actualizada

Sistema de AntiSpam:

- ✓ La primer barrera de defensa es el sistema de AntiSpam
- ✓ Cuentan con herramientas que analizan la “Reputación de URL”, mediante el análisis del contenido de los sitios web de destino, detectando el origen de la amenaza para bloquear software malicioso.

Campaña de concientización

Puntos a tener en cuenta:

- ✓ Cryptolocker ataca en base a dos puntos fundamentales:
  1. La mayor parte de los usuarios abren los archivos adjuntos que llegan a su cuenta de mail.
  2. Muy pocos usuarios guardan copias de seguridad recientes de sus documentos.
- ✓ "Tip" fundamental para evitar ser infectado: la **concientización**, que el usuario esté al tanto de cómo funciona y actúa esta amenaza (y muchas otras similares).
- ✓ Leer atentamente los mensajes antes de dar OK, aquí es donde validamos la instalación del malware.
- ✓ No acceder a sitios o páginas de internet a través de URLs que se encuentren contenidas en correos electrónicos.
- ✓ Desconfiar de correos sospechosos. Si no son mails que esperamos, no abrir los archivos adjuntos por ninguna razón.

Prevenir la ejecución de archivos por políticas (GPO)

- ✓ Una de las mejores practicas recomendadas, no solo para evitar los cryptolockers, sino así también para evitar la infección de otros malwares o virus; es la creación de políticas para bloqueo y ejecución de archivos en carpetas de sistemas.

- ✓ Microsoft permite de manera centralizada verificar la ejecución y aplicación de las políticas definidas en cada uno de los recursos. Reporte conocido como “Resultant Set of Policy”.

Mantener un Backup periódico

- ✓ Mantener un esquema de backup periódico nos garantiza poder recuperar la información a un punto en el tiempo anterior a la infección.

- ✓ Teniendo en cuenta que el sistema de encripción utilizado por este malware es de 1024 bits, técnicamente es imposible recuperar los archivos encriptados a su estado original en un tiempo razonable si no hay backup.

Brochure (PDF)
Descargar aquí

En este documento, conocé más sobre nuestras soluciones y servicios que ayudarán a tu empresa en la protección de la información.

Novedades
Suscribite aquí

Para recibir información actualizada sobre estos temas, envianos un mail indicando Nombre ,Apellido y Empresa.

MUCHAS GRACIAS!

info@nextvision.com

@nextvision_com

www.nextvision.com