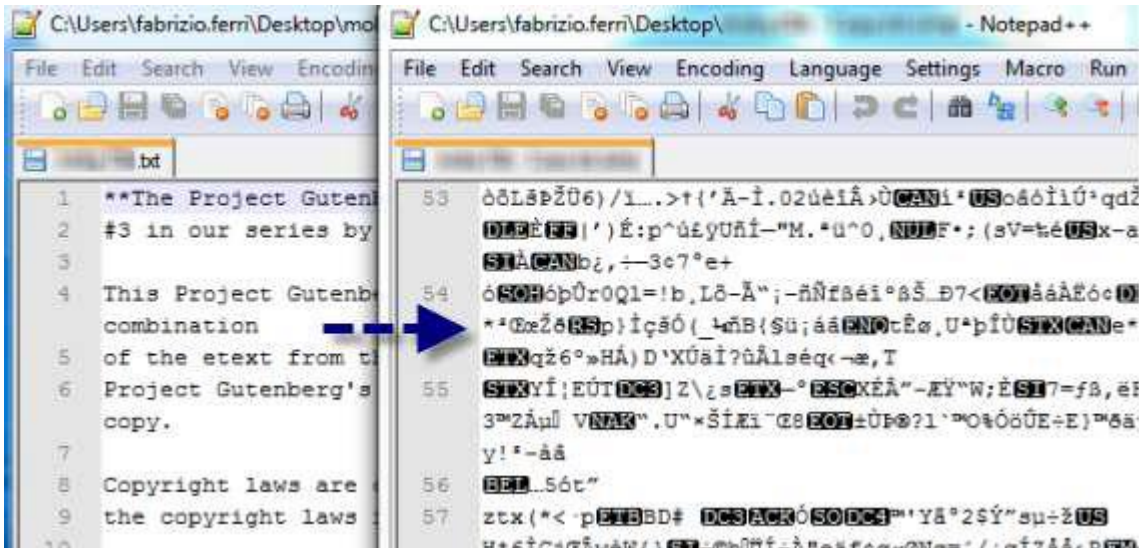
VIRUS CRYPTOLOCKER

DEFINICIÓN: Es un virus calificado como software malicioso del tipo llamado ramsomware (software malicioso que al infectar nuestro equipo lo bloquea y nos pide un rescate para recuperar el control), afecta al sistema operativo Windows, el más extendido en el mundo, aunque hay alguna versión también para Android, este virus es calificado como peligroso ya que ha afectado a millones de computadores a nivel mundial.

FUNCIONALIDAD: Puede llegar al ordenador/móvil de varias formas: al entrar en una página web que llama a descargar un archivo o al abrir archivos de correos enviados por empresas fantasma que llaman la atención del usuario de alguna forma, cuando el software malicioso se pone a trabajar en el ordenador, se conecta a los servidores de los ciberdelincuentes para generar un par de claves de encriptado RSA de 2048 bits. Envía la clave pública a la máquina infectada y comienza a cifrar documentos.

Estos archivos se vuelven inaccesibles. Los archivos se cifran con una clave que solo poseen los autores de CRYPTOLOCKER, lo que imposibilita la recuperación. Al mismo tiempo, este virus lanza su terrible amenaza: si el propietario no paga una suma de dinero en el plazo de tres o cuatro días, la clave con la que se bloquearon los archivos será borrada para siempre, y los archivos ya no se podrán rescatar. Esto es como encerrar a alguien en una celda indestructible y tirar la llave.



Los archivos infectados por Cryptolocker se vuelven ilegibles debido al cifrado El pago que solicitan es a través de MoneyPak, Ukash y Bitcoin, una moneda virtual cuyas transacciones se efectúan sin controles.

Las formas de pago que acepta el virus Cryptolocker dificultan la identificación de los autores

ARCHIVOS Y EXTENSIONES QUE ATACA EL VIRUS: Extensión de Microsoft Office, OpenDocument (LibreOffice, PDF), fotografías, imágenes y otros.

odt, .ods, .odp, .odm, .odc, .odb, .doc, .docx, .docm, .wps, .xls, .xlsx, .xlsm, .xlsb, .xlk, .ppt, .pptx,.pptm, .mdb, .accdb, .pst, .dwg, .dxf, .dxg, .wpd, .rtf, .wb2, .mdf, .dbf, .psd, .pdd, .pdf, .eps, .ai, .indd, .cdr, .jpg, .jpe, .jpg, .dng, .3fr, .arw, .srf, .sr2, .bay, .crw, .cr2, .dcr, .kdc, .erf, .mef, .mrw, .nef, .nrw, .orf,.raf, .raw, .rwl, .rw2, .r3d, .ptx, .pef, .srw, .x3f, .der, .cer, .crt, .pem, .pfx, .p12, .p7b, .p7c.

CÓMO PREVENIR INFECCIONES POR CRYPTOLOCKER

Los autores de CRYPTOLOCKER diseñaron su virus con dos prejuicios en mente: que todos abrimos los archivos adjuntos y que nadie guarda copias de seguridad recientes de sus documentos.

1. Para empezar, desconfíe de los correos sospechosos. Si no son correos que espera o sea conocidos, no debes abrir los archivos adjuntos por ninguna razón. Lo mismo aplica si estás usando correo web: si no has solicitado nada, no hagas clic. Esta regla evitará la mayoría de infecciones oportunistas, el medio principal de propagación del virus.

2. Para evitar que el virus se propague en sus equipos debemos instalar la herramienta CryptoPrevent la cual deshabilitará el tipo de permisos que el virus aprovecha para instalarse. La herramienta modifica las políticas de seguridad de Windows para evitar que un programa pueda ejecutarse desde la carpeta de Datos de programa

(AppData). Ésta herramienta se puede bajar en la siguiente dirección web: http://www.foolishit.com/vb6-projects/cryptoprevent/

3. Si no lo ha hecho, es conveniente que cree su propio plan de copias de seguridad de sus equipos, es decir activar las copias de seguridad desde el menú de Propiedades de Sistema, al que puedes acceder con un clic derecho sobre el icono de Mi Pc, o también desde el Panel de control, dentro de la sección Sistema.

4. Sacar respaldos de sus archivos (Trabajos, informes, proyectos, etc.), al menos cada quince días a un dispositivo externo (Disco duro externo, CD, DVD) y mantener a buen recaudo la información, para restaurar en caso de necesitarlo.

QUÉ HACER EN CASO DE INFECCIÓN DE CRYPTOLOCKER

- Si observa la pantalla de CRYPTOLOCKER, desconecta el equipo de la red para que el virus no pueda cifrar más archivos ni tampoco comunicarse con los criminales.

- Desconectar la conexión a Internet también evita que tus archivos en Dropbox o Google Drive se sobrescriban con las copias infectadas.

Una forma rápida de desactivar la conexión es ir al panel de Red y desactivar los dispositivos.

Acto seguido, ha de preguntarte qué quiere hacer, si pagar la suma del rescate o eliminar el virus e intentar recuperar los archivos. **SE RECOMIENDA NO PAGAR**.

CÓMO ELIMINAR EL VIRUS CRYPTOLOCKER DEL PC

Usar la herramienta **NORTON POWER ERASER,** la cual es un potente anti-troyanos de Symantec,sedebebajardelasiguientedirecciónweb:

https://support.norton.com/sp/en/us/home/current/solutions/kb20100824120155EN_EndUserProfile_en_us

Una vez que le ejecuten esta herramienta, el equipo se reinicia y todo rastro de CRYPTOLOCKER habrá desaparecido.

CÓMO RECUPERAR LOS ARCHIVOS INFECTADOS POR CRYPTOLOCKER

CRYPTOLOCKER solo ataca documentos que se encuentran en el PC y en las unidades de red. No ataca archivos que se encuentran en unidades desconectadas o en servidores que están en Internet. Para recuperar los archivos podrá hacerlo a través de los respaldos que usted como usuario haya tenido en otros medios tecnológicos y en últimos de los casos se tendrá que llevar a un servicio técnico, los Centros de Cómputo de las Unidades Policiales o Coordinaciones de Comunicaciones para su análisis y resolución.

Fuente : Boletín 01 Seguridad 2015 – DNC/DNCE