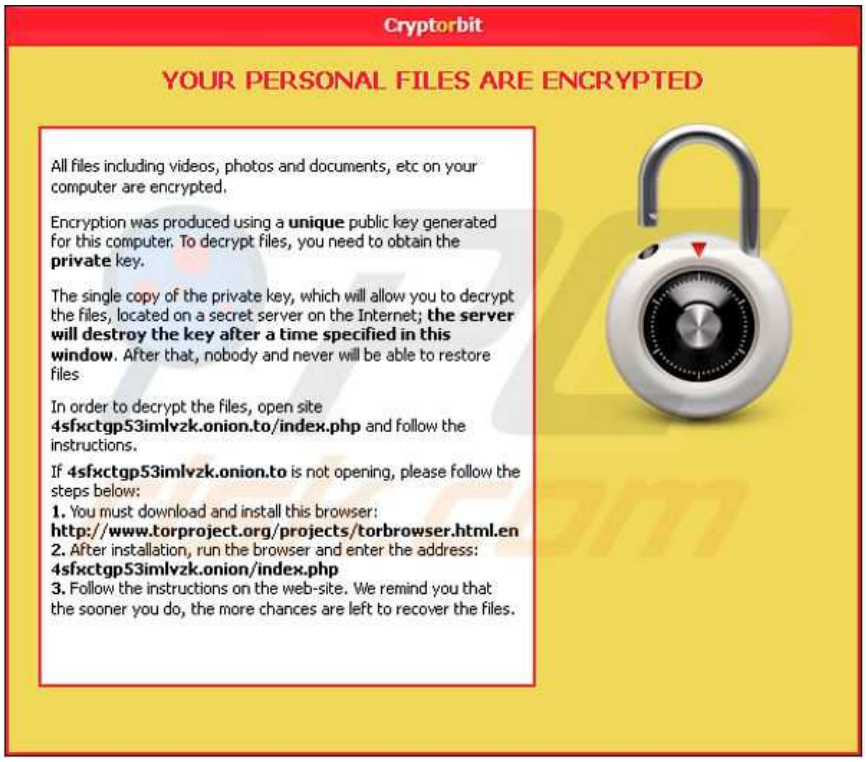
MOSTRADOR Web
Diseño de Sitios Web – Cómputo y Sistemas.

INSTRUCCIONES PARA ELIMINAR CRYPTORBIT
"¡SUS ARCHIVOS PERSONALES HAN SIDO ENCRIPTADOS!"

Virus Cryptorbit
Conocido también como: **Cryptorbit ransomware**
Tipo: **Ransomware**
Nivel de peligrosidad: **Extremo**
Propagación: **Alto**

Cryptorbit es un virus tipo ransomware (bloqueador de sistemas) que se infiltra en el PC del usuario a través de mensajes infectados de correo electrónico y redes P2P. Tras entrar en el sistema con éxito, este programa malicioso encripta los archivos almacenados en el PC (*.doc, *.docx, *.xls, *.ppt, *.psd, *.pdf, *.eps, *.ai, *.cdr, *.jpg, etc.) y exige el pago de un rescate de 0,5 BTC (Bitcoins) para desencriptar los archivos. En la fecha de publicación del artículo, 0,5 BTC equivalía a 400$ USD aprox. Este virus bloqueador de sistemas es idéntico a su variante anterior denominada Cryptolocker. Los usuarios deben ser conscientes de que, aunque no es complicado eliminar la infección, la desencriptación de los archivos afectados por este programa malicioso no es posible si no se abona la suma del rescate. En la fecha de nuestro análisis, no se encontraron herramientas o soluciones capaces de desencriptar los archivos encriptados por Cryptorbit.

Inmediatamente después de infectar el sistema operativo, este virus se comunica con su servidor de mando y control y genera una clave pública que se usa para desencriptar los datos. Tras completar la encriptación de los archivos encontrados, Cryptorbit mostrará un mensaje (véase captura de pantalla abajo) con información para recuperar los archivos. Tenga en cuenta que la clave privada que puede usarse para desencriptar los archivos se encuentra en los servidores de mando y control, gestionados por los ciberdelincuentes. La solución ideal en este caso sería eliminar el virus del sistema y restaurar los archivos afectados de una copia de seguridad.



Las infecciones con bloqueadores de sistema como Cryptorbit deberían motivarnos lo suficiente como para crear siempre copias de seguridad de todos los archivos guardados en el equipo. Tenga en cuenta que el hecho de pagar la suma del rescate equivale a enviar un pago (su dinero) a ciberdelincuentes; estaría apoyando el modelo de negocio fraudulento y además no tiene garantías de que los archivos se desencriptarán en algún momento. Para evitar que nuestros sistemas se infecten con un virus ransomware, debemos tener especial cuidado a la hora de abrir mensajes de email. Los ciberdelincuentes usan varios títulos atrayentes para engañar a los usuarios y que así abran los adjuntos infectados, por ejemplo "Mensaje de voz de desconocido", "Importante - formulario adjunto", "Justificante de nómina", "Nuevo acuerdo de contrato", etc. Según investigaciones recientes, los ciberdelincuentes también utilizan redes P2P para engañar a usuarios y que así se descarguen Cryptorbit.

Mensaje mostrado por el virus ransomware Cryptorbit:

Cryptorbit

SUS ARCHIVOS PERSONALES HAN SIDO ENCRIPTADOS

Se encriptarán todos los archivos, incluyendo vídeos, fotos y documentos, etc. de su sistema. La encriptación se ha producido usando una clave pública generada para este PC. Para desencriptar los archivos, necesita conseguir la clave privada. La única copia de la clave privada, que le permitirá desencriptar los archivos, se ubica en un servidor secreto en internet; el servidor destruirá la clave en el plazo de tiempo especificado en esta ventana. Después, nadie podrá recuperar los archivos jamás. Para desencriptar los archivos, abra el sitio 4sfxctgp53imlvzk.onion.to/index.php y siga los pasos a continuación: 1. Debe descargar e instalar este navegador: torproject.org/projects/torbrowser.html.en 2. Después de instalarlo, abra el navegador e introduzca esta dirección: 4sfxctgp53imlvzk.onion/index.php 3. Siga las instrucciones del sitio web. Le recordamos que cuanto antes pague, más posibilidades tiene de recuperar los archivos.

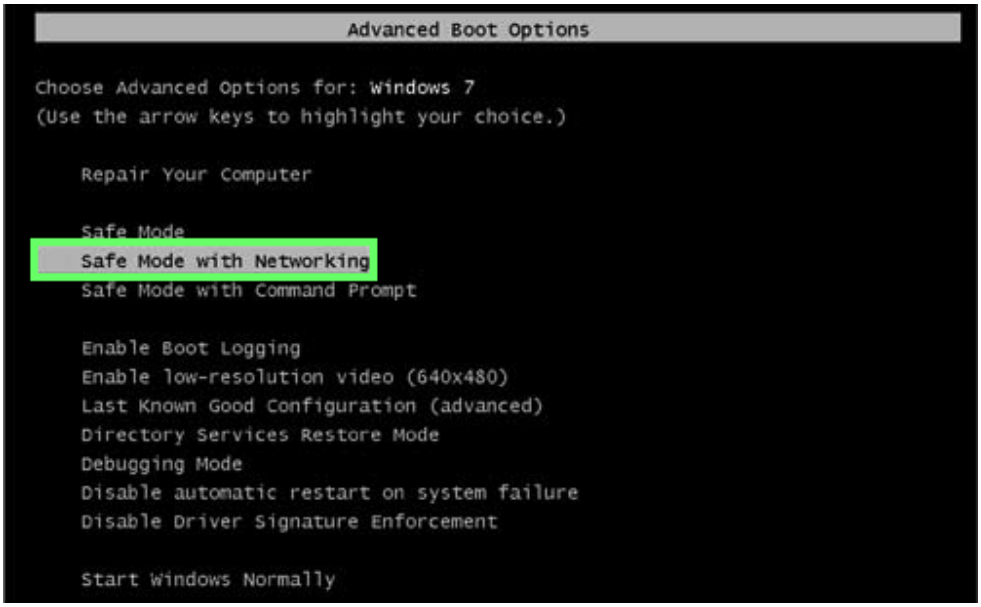
Captura de pantalla de "Cryptorbit Decryptor":

Tenga en cuenta que en la fecha de publicación del artículo todavía no había ninguna herramienta conocida que pudiera desencriptar los archivos encriptados por Cryptorbit. Actualizaremos el artículo en cuanto haya más información sobre la desencriptación de los archivos infectados.

Eliminar el virus Cryptorbit:

Paso 1

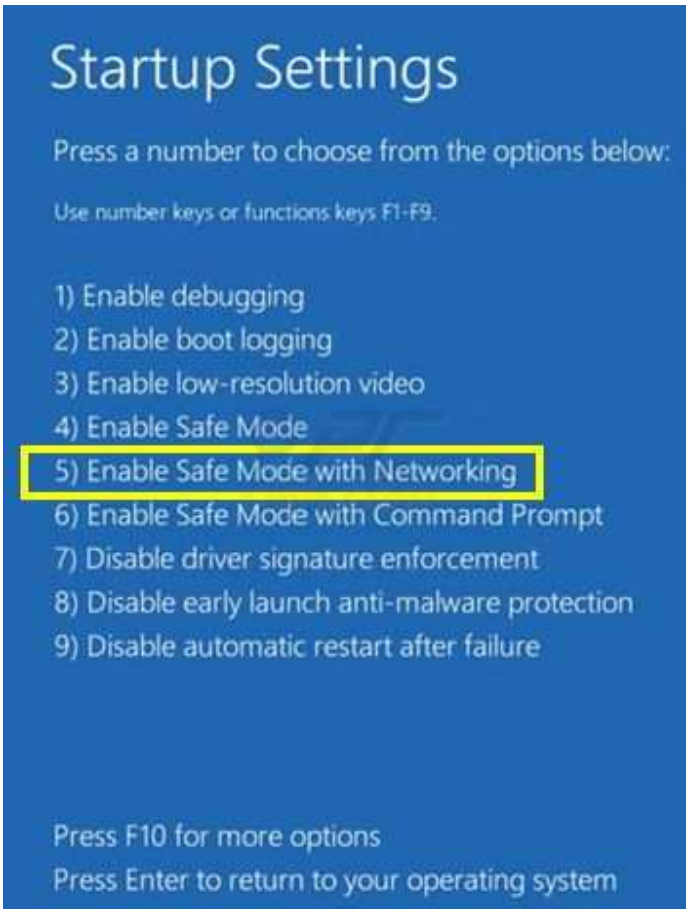
Usuarios de Windows XP y Windows 7: Durante el proceso de arranque de su ordenador, pulse la tecla F8 en su teclado varias veces hasta que aparezca el menú de Opciones avanzadas de Windows, luego seleccione Modo seguro con funciones de red de la lista y pulse ENTER.



Este vídeo muestra cómo iniciar Windows 7 en "Modo seguro con funciones de red":

https://www.youtube.com/watch?feature=player_embedded&v=kynlaYPDbeI

Usuarios de Windows 8: Diríjase a la pantalla de inicio de Windows 8, escriba Avanzado, en los resultados de búsqueda, seleccione Configuración. Haga clic en las opciones de inicio avanzadas; tras abrir la ventana de "Configuración general del PC", seleccione "Arranque avanzado". Haga clic en el botón de "Reiniciar ahora". Su PC se reiniciará ahora con el "Menú de opciones de arranque avanzadas". Haga clic en el botón de "Solucionar", luego haga clic en el botón de "Opciones avanzadas". En la pantalla de opciones avanzadas, haga clic en "Configuración de arranque". Haga clic en el botón "Reiniciar". Su PC se reiniciará con la pantalla de Configuración de arranque. Pulse "5" para arrancar en Modo seguro con símbolo de sistema.



Este vídeo muestra cómo iniciar Windows 8 en "Modo seguro con funciones de red":

https://www.youtube.com/watch?feature=player_embedded&v=CaCalUhx6ok

Paso 2

Inicie sesión con la cuenta que está infectada con el virus Cryptorbit. Abra su navegador web y descargue un programa legítimo anti-spyware. Actualice el software antiespía e inicie un análisis de sistema completo. Elimine todas las entradas que detecte.

DESCARGAR PROGRAMA DE DESINFECCION DE CRYPTORBIT.

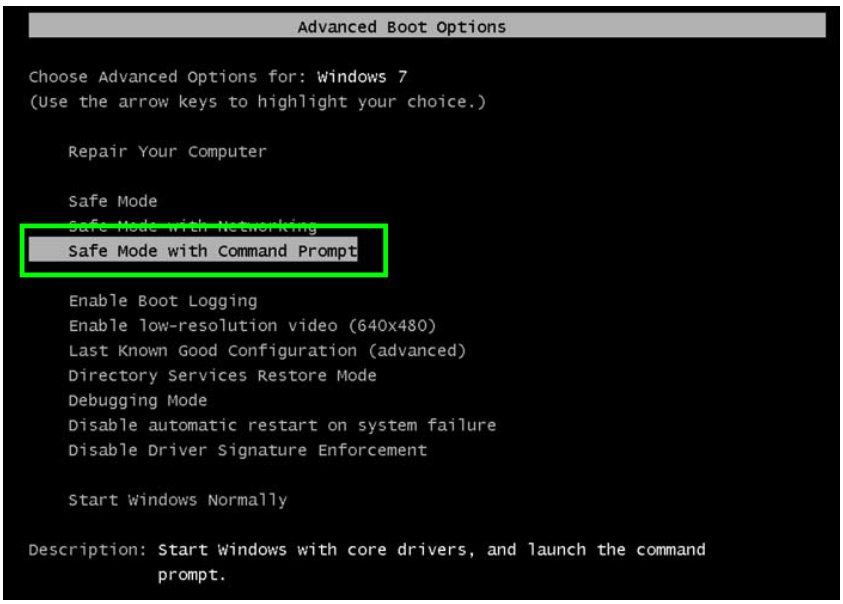
http://www.pcrisk.es/files/sh-remover.exe

Si no puede arrancar su equipo en modo seguro con funciones de red, pruebe con una restauración del sistema.

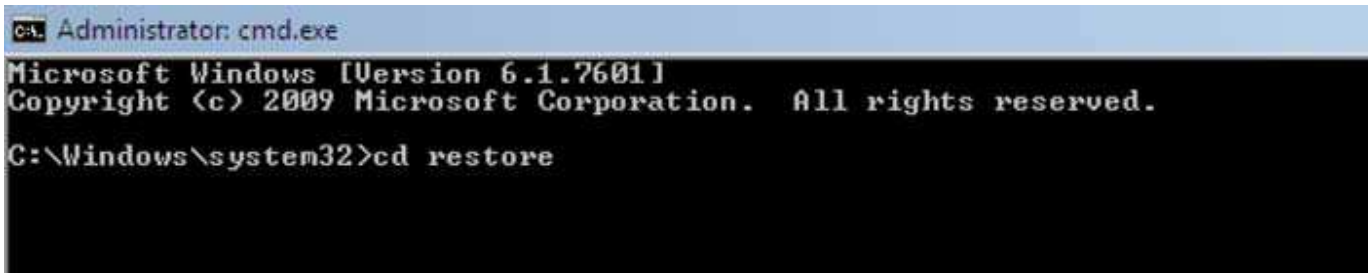
Este vídeo muestra cómo eliminar el virus ransomware usando "Modo seguro con funciones de red" y "Restaurar sistema":

https://www.youtube.com/watch?feature=player_embedded&v=xip4xl4uorQ

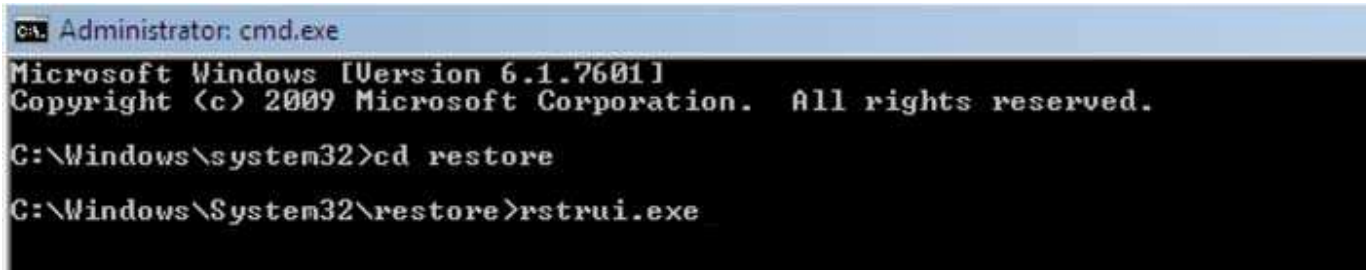
1. Inicie su sistema en modo seguro con símbolo de sistema - Durante el proceso de arranque de su ordenador, pulse la tecla F8 en su teclado varias veces hasta que aparezca el menú de Opciones avanzadas de Windows, luego seleccione Modo seguro con funciones de red de la lista y pulse ENTER..



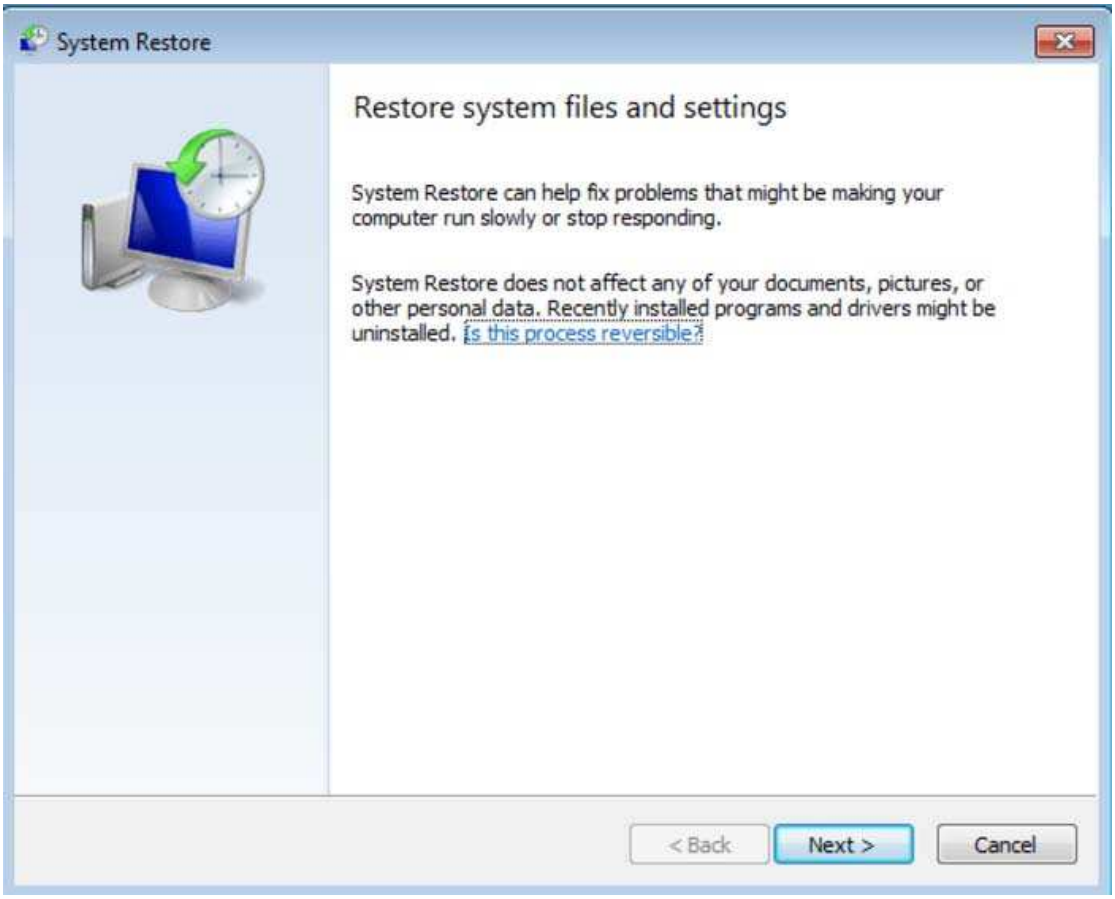
2. Cuando el símbolo del sistema se cargue, introduzca la siguiente línea: **cd restore** y pulse ENTER.



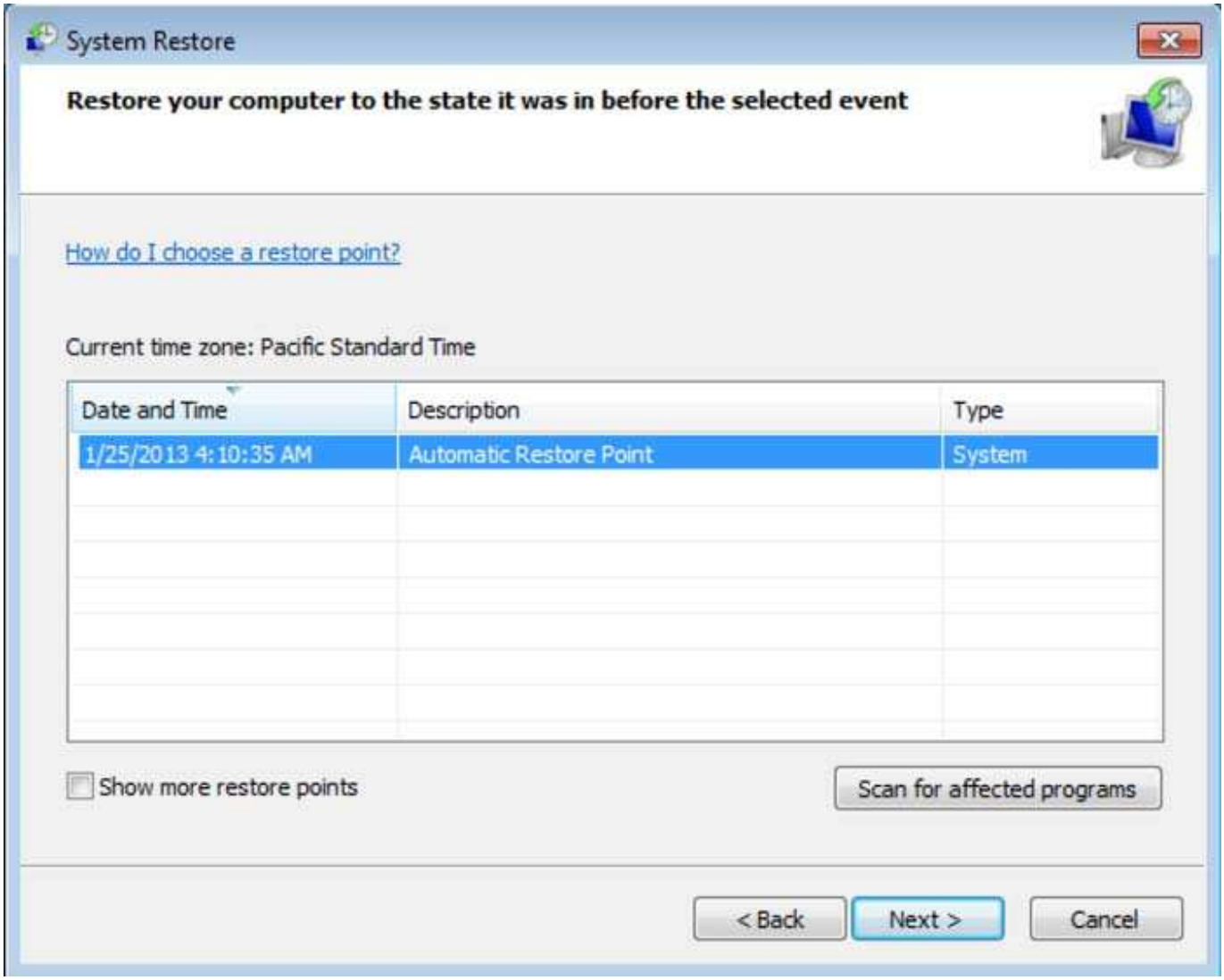
3. Luego teclee esta línea: **rstrui.exe** y pulse ENTER.



4. en la ventana abierta, haga clic en "Siguiente".



5. Seleccione uno de los puntos de restauración disponibles y haga clic en "Siguiente" (se restaurará el sistema de su equipo en una fecha anterior, antes de que el ransomware se colara en su PC).

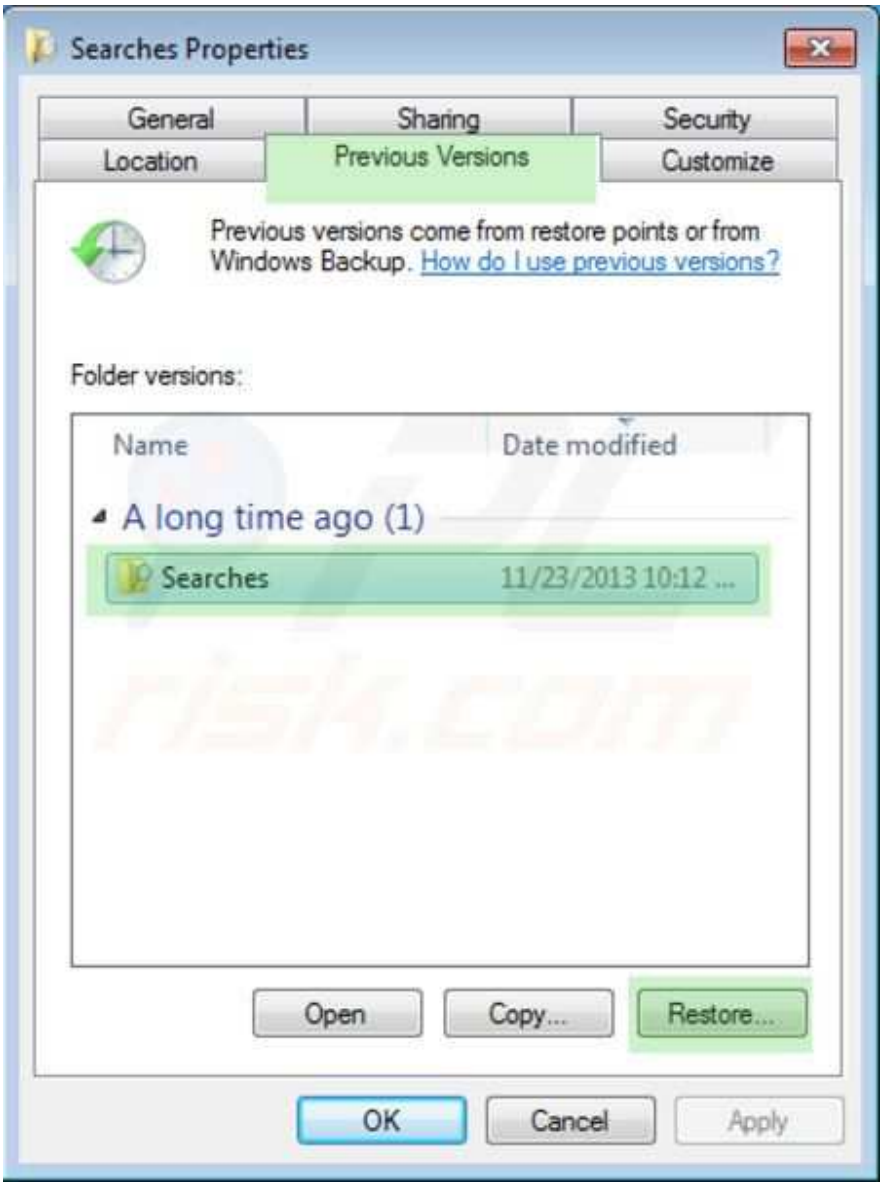


6. En la ventana abierta, haga clic en "Sí".

7. Después de restaurar su sistema a un punto anterior, descargue y analice su PC con un software antiespía recomendado para eliminar los remanentes del virus Cryptorbit.

Para restaurar individualmente cada archivo encriptado por este virus, los usuarios pueden probar con la función versiones anteriores de archivo. Este método es únicamente eficaz si la función de Restaurar sistema estaba activa en el sistema operativo infectado.

Para restaurar un archivo, haga clic con el botón derecho del ratón sobre el archivo, seleccione Propiedades y haga clic en la pestaña Versiones anteriores. Si el archivo en cuestión tiene su punto de restauración creado, selecciónelo y haga clic en el botón "Restaurar".



Si no puede iniciar su sistema en modo seguro con funciones de red (o con símbolo de sistema), debería iniciar su ordenador usando un disco de rescate. Algunos tipos de ransomware deshabilitan el modo seguro, por lo que la desinfección es más compleja. Para este paso, necesitará acceder a otro ordenador.

Otras herramientas conocidas para eliminar el virus Cryptorbit:

- iS3 STOPzilla
- Malwarebytes Anti-Malware

FUENTE ORIGINAL PCRISK.