BOLETÍN DE ALERTA

Boletín Nro.: 2016-14
Fecha de publicación: 16/11/2016
Tema: Herramienta para desencriptar archivos encriptados por CrySIS

Descripción:

Hace unos días se han publicado las claves maestras de descifrado del ransomware CrySIS, la cual ha permitido recuperar archivos encriptados por este ransomware. Un usuario anónimo con el seudónimo crss7777 compartió un enlace a una publicación en Pastebin en la que se podía observar la cabecera escrita en C conteniendo las claves maestras de descifrado de Crysis, así como también información acerca de cómo utilizarla para descifrar los archivos cifrados por este ransomware.

El ransomware CrySIS es una familia de ransomware que apareció a medidados de este año y ha afectado a numerosos ciudadanos y empresas en nuestro país, en los últimos meses.

Se han observado diferentes vectores de infección, en los primeros meses las campañas de distribución se basaban en correos electrónicos con adjuntos maliciosos (archivos con doble extensión, documentos de Microsoft Word con macros maliciosas, archivos .zip con dropper JS, entre otros). Sin embargo, a finales de agosto se observaron los primeros casos en los que el ransomware infectó un equipo de forma directa, luego de un ataque de fuerza bruta a servicios RDP (Remote Desktop Protocol) expuestos a Internet con credenciales débiles. Luego de ingresar a un equipo a través de RDP, los atacantes obtienen acceso e infectan los dispositivos y recursos compartidos con el equipo inicial. De esta manera, lograron infectar una gran cantidad de servidores de archivos, afectando con un solo ataque a varias computadoras de una red.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 / +595 962 271 071
Asunción – Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

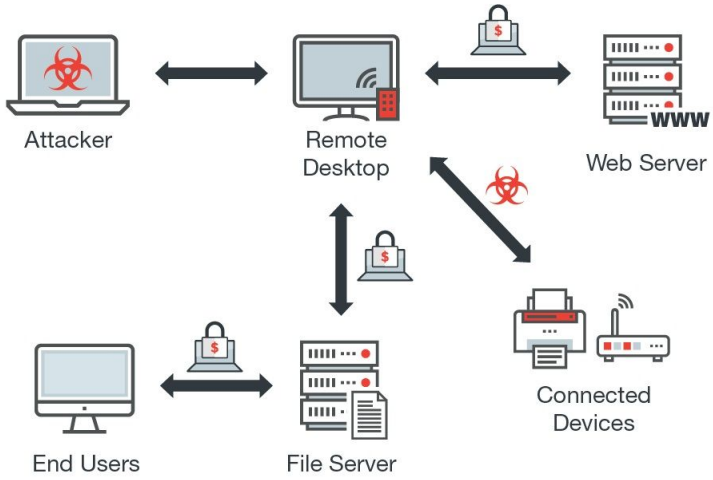


Figura 1: Infección de CrySIS mediante ataques de fuerza bruta RDP

Tras encriptar todos los archivos y cambiar las extensiones (.crysis, o .<extension>.<id-number>.<email>.xtbl), deja un archivo de texto llamado "How to decrypt your files.txt" en el Escritorio. En algunos casos, está acompañado de la imagen "DECRYPT.jpg", que muestra el mensaje de rescate como fondo de pantalla. La información provista inicialmente está limitada a dos direcciones de correo de contacto de los extorsionadores (generalmente, @india.com o @aol.com). Tras enviarles el e-mail, la víctima recibe más instrucciones. Entre otras cosas, incluye el precio de la herramienta de descifrado, que oscila entre 400 y 1500 euros. La víctima recibe la orden de comprar bitcoins y enviarlos a la billetera virtual de los operadores, especificada al final del mensaje.

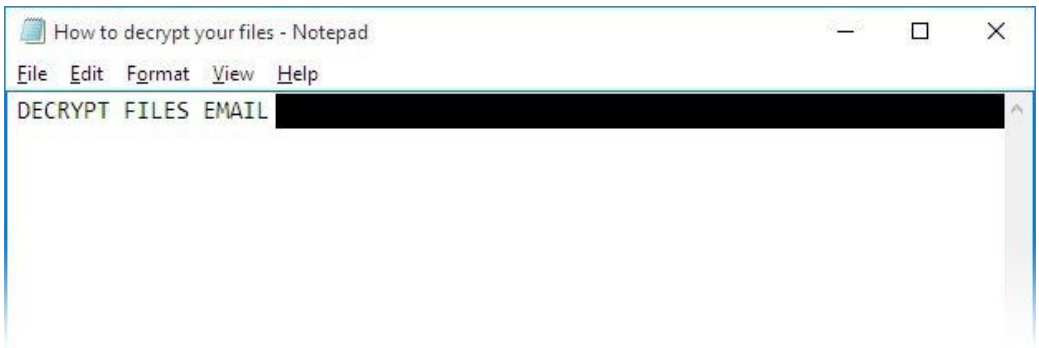


Figura 2: Ejemplo de nota dejada por CrySIS

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 / +595 962 271 071
Asunción – Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

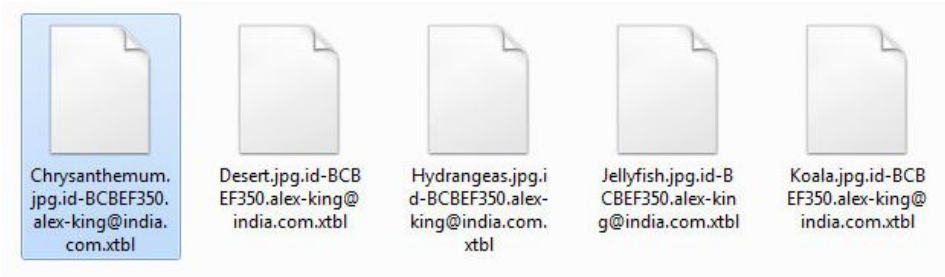


Figura 3: Archivos encriptados por CrySIS

Se desconoce la razón por la cual el usuario anónimo, quien probablemente tenga relación con la banda de cibercriminales detrás de CrySIS, publicó las claves. Este comportamiento, así como otras características de CrySIS, son similares a los observados con otra familia de ransomware, Teslacrypt, en la que la banda cibercriminal publicó las claves maestras de su última versión Teslacrypt 3.0, la cual hasta ese momento no tenía solución. Sin embargo, cabe resaltar que no es frecuente ni está garantizado que una banda cibercriminal publique de forma voluntaria las claves maestras.

Solución:

Luego de la publicación de las claves maestras y luego de que las mismas hayan sido analizadas y se haya confirmado su autenticidad, la empresa de seguridad Kaspersky actualizó su herramienta **RakhniDecryptor** para incluir estas claves. Gracias a esta herramienta, los usuarios afectados por cualquiera de las variantes de Crysis pueden recuperar sus archivos sin tener que pagar nada a cambio.
Es probable que próximamente se desarrollen otras herramientas similares, puesto que cualquier investigador puede revisar la cabecera y crear su propia versión para conseguir el descifrado de los archivos afectados.

A continuación, se detallan las instrucciones para desencriptar los archivos utilizando esta herramienta:

1. Descargar la herramienta RakhniDecryptor y extraer la aplicación en la máquina en la que se encuentran los archivos encriptados:
   http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip

2. Ejecutar la herramienta. Se verá la pantalla principal:

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 / +595 962 271 071
Asunción – Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

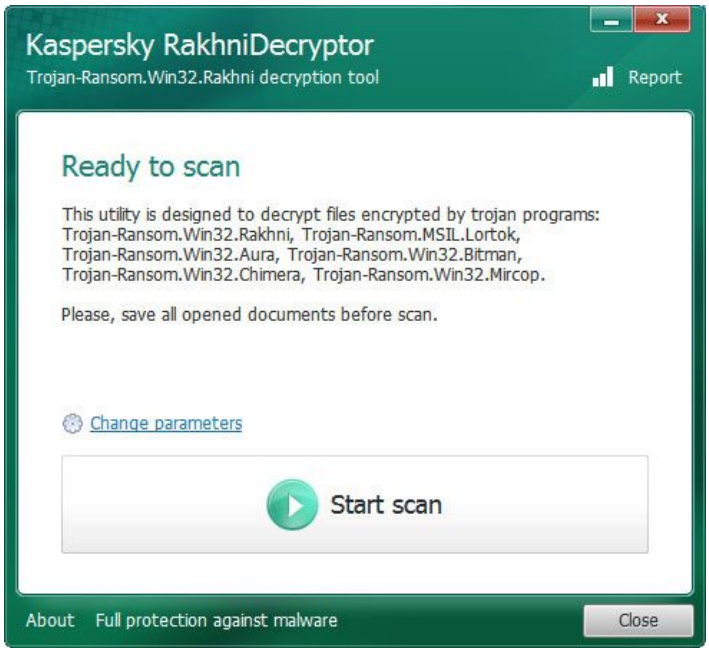


Figura 4: Pantalla principal de Kaspersky RakhniDecryptor

3. Antes de empezar, el usuario se tiene que asegurar que esté usando la versión 1.17.8.0 o superior, que es la que incluye el soporte descifrar el ransomware CrySis. Para comprobar eso, hacer click sobre el enlace *About* situado en la parte inferior izquierda en la pantalla principal. Esto mostrará una pequeña ventana que indicará la versión de RakhniDecryptor que se está utilizando.

4. En caso de confirmarse que la versión de RakhniDecryptor es la mencionada o superior, hacer click en ***Start scan.***

5. Aparecerá un diálogo en el cual tendrá que seleccionar un fichero. Navegar hasta las carpetas que contienen los ficheros cifrados por CrySis y seleccionar uno, pudiendo ser este de Word, Excel, PDF, música o una imagen (formato original del fichero). No se debe seleccionar ningún fichero de texto plano (.txt) debido a que éstos no pueden ser usados para descifrar el resto de ficheros.

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 / +595 962 271 071
Asunción – Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

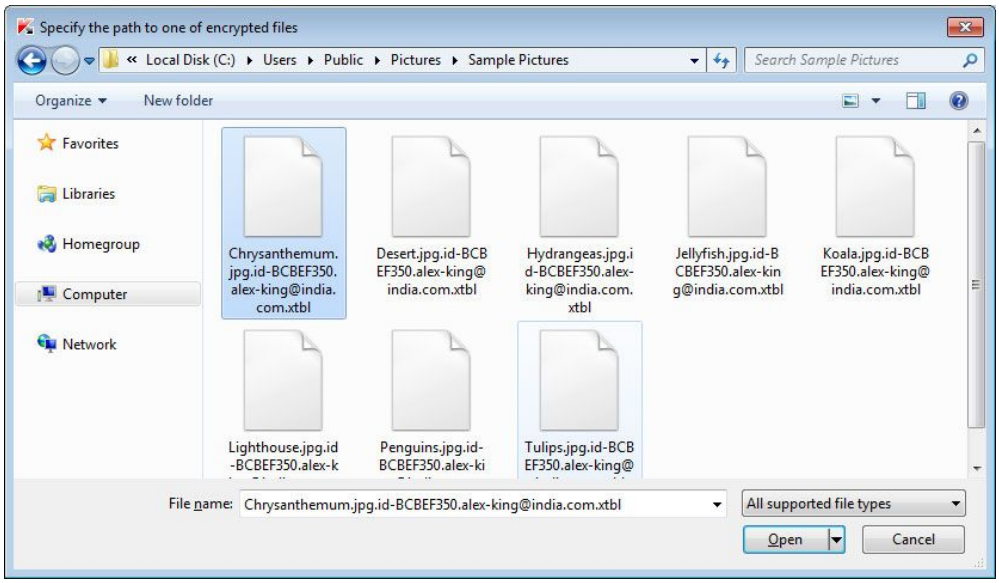
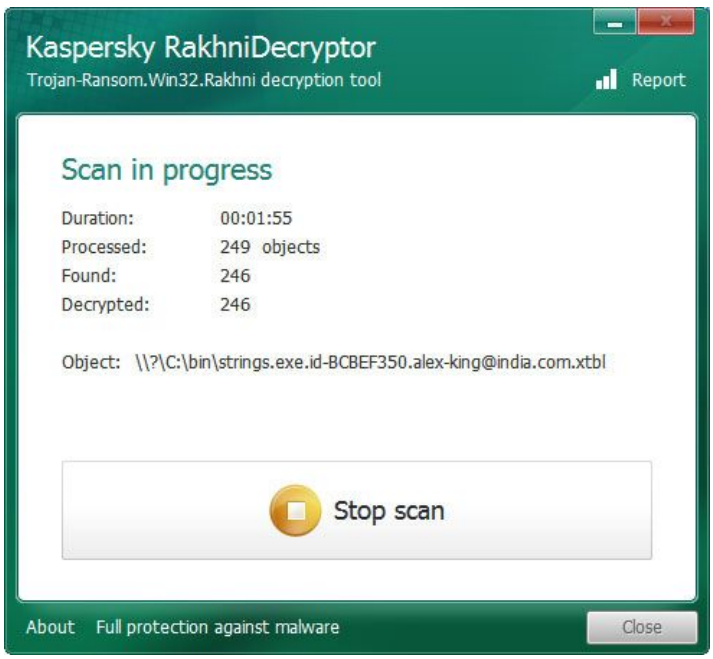


Figura 5: Selección de un archivo encriptado

6. Una vez seleccionado el fichero a descifrar, pulsar sobre el botón ***Open*** para que RakhniDecryptor inicie el proceso de descifrado de todos los ficheros afectados por CrySis en la computadora.

El proceso de descifrado puede demorar varias horas, no se debe interrumpir el proceso. Se recomienda asegurar que el equipo se encuentre conectado a la corriente eléctrica y con la batería cargada. Antes de iniciar el proceso, es recomendable realizar una copia de seguridad de los archivos encriptados, de modo a evitar la pérdida de los mismos en caso de que el proceso falle.



CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 / +595 962 271 071
Asunción – Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

Figura 6: Proceso de desencriptación de los archivos

Una vez terminado el proceso de descifrado, RakhniDecryptor mostrará la pantalla con la lista de todos los ficheros descifrados.

Mitigación y prevención:

Si bien, en esta ocasión, la banda cibercriminal o un allegado a ella publicó la clave maestra, esto no es frecuente ni existen garantías de que esto vaya a ocurrir con otras familias de ransomware. Por lo tanto, las medidas preventivas para evitar la pérdida de información son fundamentales.

- No abrir nunca correos sospechosos, tanto si vienen de usuarios conocidos como desconocidos. Asegurarse siempre de que la persona que le ha enviado el correo realmente le quería remitir ese adjunto.
- Evitar abrir los archivos adjuntos sospechosos. Incluso los archivos aparentemente inofensivos, como los documentos de Microsoft Word o Excel, pueden contener un virus, por lo que es mejor ser precavido.
- No ingresar a enlaces dudosos que le son enviados a través de correo electrónico, servicios de mensajería, redes sociales, etc.
- Realizar copias de seguridad (backup) de toda la información crítica para limitar el impacto de la pérdida de datos o del sistema y para facilitar el proceso de recuperación. Idealmente, estos datos se debe mantener en un dispositivo independiente, y las copias de seguridad se deben almacenar offline.
- Contar con soluciones de antivirus/firewall y mantenerlo actualizado, de modo a prevenir la infección.
- Mantener su sistema operativo y el software siempre actualizado, con los últimos parches.
- No acceder nunca a ningún pago u acción exigida por el atacante. No existe garantía de que se recupere los archivos, además se estará contribuyendo al financiamiento de otras actividades ilegales.
- De ser posible, evitar exponer servicios sensibles al exterior de su red (RDP, SSH, FTP, etc.) En caso de requerir estos servicios, utilizar contraseñas robustas y controles de acceso lo más restrictivos posible (restricciones por IP, VPN, límites de intentos fallidos, etc.)

Uno de los vectores de infección más frecuentes es la explotación de plugins vulnerables del navegador (Adobe Flash Player, Java, etc.) mediante drive-by-download. Algunas recomendaciones específicas para evitar esto, son:

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 / +595 962 271 071
Asunción – Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

- Evitar la ejecución automática de plugins como Adobe Flash Player, Java, etc. La mayoría de los navegadores modernos permiten configurarlo de modo a que se solicite permiso al usuario cada vez que un sitio web intente ejecutar un plugin.
- Contar con mecanismos de protección contra la publicidad invasiva, muy ligada al malvertising (anuncios maliciosos embebidos en la web). Existen complementos muy útiles como por ejemplo AdBlock Plus, disponible para varios sistemas operativos y navegadores.
- Evitar la ejecución automática de Javascript. Existen complementos como No-Script y ScriptSafe que deshabilitan por defecto la ejecución de Javascript, permitiendo al usuario habilitarlo sólo en las páginas en las que confía.

Para más información sobre la técnica de drive-by-download, lea nuestro boletín:
http://www.cert.gov.py/application/files/4714/4587/6816/Boletin_20151026_Drive_by_Download.pdf

Cuando un equipo fue infectado por un ransomware, es importante no modificarlo: no se debe eliminar archivos ni reinstalar el sistema operativo, hasta tanto se haya realizado un análisis detallado de la infección, que debe ser llevado a cabo por expertos en la materia. En caso de víctima de ransomware se recomienda realizar la denuncia a los organismos correspondientes; puede reportarlo al Centro de respuestas ante Incidentes Cibernéticos (CERT-PY).
Aún no habiendo una solución en el momento de la infección, es importante guardar los archivos encriptados importantes ya que es posible que en un futuro sea desarrollada una solución.

Información adicional:
http://muyseguridad.net/2016/11/15/descifrar-crysis-ransomware/
http://www.welivesecurity.com/la-es/2016/06/07/ransomware-crysis-teslacrypt/
http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/

CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 217 9000 / +595 962 271 071
Asunción – Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py