BOLETÍN DE ALERTA

Boletín Nro.: 2017-06
Fecha de publicación: 22/05/2017
Tema: Herramienta para desencriptar archivos encriptados por CrySIS/Dharma/Wallet

Descripción:

Hace unos días se han publicado las claves maestras de descifrado de Dharma, un ransomware relacionado a la familia Crysis/Dharma/Wallet, la cual ha permitido recuperar archivos encriptados por este ransomware. Un usuario anónimo compartió un enlace a una publicación en Pastebin en la que se podía observar la cabecera escrita en C conteniendo 198 claves maestras de descifrado.
No es la primera vez que la banda cibercriminal detrás de esta familia de ransomwares publican las claves maestras: en noviembre del año pasado habían publicado las claves de CrySIS, en marzo publicaron las de una versión de Dharma, y días atrás publicaron las de otra variante. Al igual que ha ocurrido en otras ocasiones, aquellas amenazas que ya no ofrecen ningún tipo de ganancias a los ciberdelincuentes son descatalogadas, y éstos toman la decisión de hacer públicas todas las claves de cifrado que se han empleado, para enfocarse a la distribución de nuevas versiones del ransomware. Sin embargo, cabe resaltar que no es frecuente ni está garantizado que una banda cibercriminal publique de forma voluntaria las claves maestras.
La familia de ransomware CrySIS/Dharma/Wallet es una familia de ransomware que apareció a mediados del año pasado y que ha afectado a numerosos ciudadanos y empresas en nuestro país, en los últimos meses. Se han observado diferentes vectores de infección, siendo el más común los 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.

¿Cómo funciona Dharma/Wallet/Crysis?
Al igual que la mayoría de las familias de ransomware, al quedar infectado, el ransomware se ejecuta e inmediatamente cifra la gran mayoría de los archivos y le añade una extensión característica. Las extensiones añadidas dependen de la variante del ransomware, pudiendo ser .dharma, .wallet, .crysis, tienen un formato similar a <filename>.id-<NUMBER>.<email@domain.com>.<extension>.

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 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

El ransomware encripta archivos con una gran cantidad de extensiones: desde las más comunes (.doc, .docx, .xlsx, .pdf, .png, .zip, etc.) hasta las más específicas, ya sea correspondientes a archivos de correo, de bases de datos, de código, máquinas virtuales, de diseño, etc. Algo muy común en muchas de estas variantes es que además encriptan los directorios compartidos en red a los que el equipo tiene acceso, afectando así a un amplio número de usuarios. Por lo general, el ransomware borra todas las instantáneas de recuperación (*Shadow Volume Copies*), de manera que no se pueden utilizar para restaurar los archivos de la víctima.

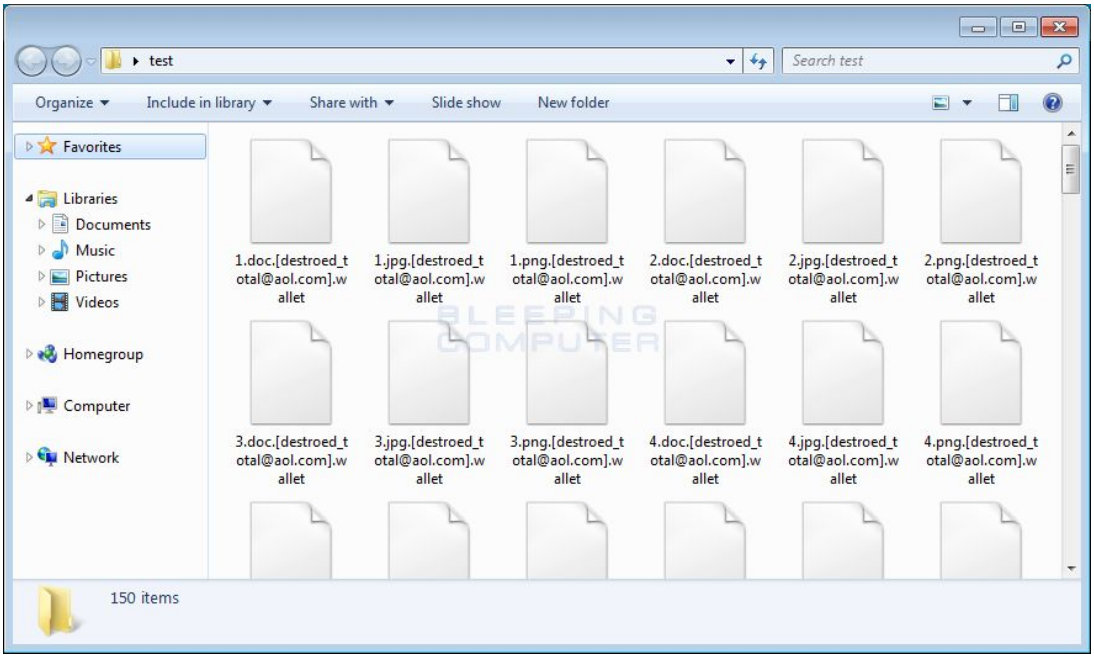

Figura 1: Archivos cifrados por una de las versiones de Dharma

Luego, el ransomware despliega un mensaje en pantalla y/o como fondo de pantalla, como una "nota de rescate" en la que proporcionan las instrucciones para el pago del rescate y la recuperación de los archivos. El pago exigido es en bitcoins, y los montos pueden variar entre 500 a 1500 USD.

Solución:

Luego de la publicación de las claves maestras y luego de que las mismas hayan sido analizadas y se haya confirmado su autenticidad, varias empresas de seguridad han desarrollado herramientas que incluyen estas claves para descifrar los archivos:

- Avast CrySIS Decryptor: http://files.avast.com/files/decryptor/avast_decryptor_crysis.exe

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 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

- Kaspersky Rakhni Decryptor: http://media.kaspersky.com/utilities/VirusUtilities/EN/RakhniDecryptor.zip
    - Guías de uso: https://support.kaspersky.com/viruses/disinfection/10556?cid=noransom
- ESET CrySIS Decryptor: https://download.eset.com/com/eset/tools/decryptors/crysis/latest/esetcrysisdecryptor.exe
    - Guías de uso: http://soporte.eset-la.com/kb6274/?viewlocale=es_ES

Antes de utilizar las herramientas para descifrar los archivos, es importante asegurarse que en su equipo no se encuentra latente ningún proceso del ransomware. La gran mayoría de los antivirus/antimalware detectan y eliminan los rastros del ransomware, por lo que es fundamental escanear su máquina previo a intentar el proceso de descifrado.

Debe tenerse en cuenta que, aunque ocasionalmente se da a conocer una manera de descifrar los archivos, esto normalmente suele coincidir con el inicio de la distribución de otras familias de ransomware, por lo que es fundamental reforzar las medidas preventivas.

Mitigación y Prevención:

- Verificar los accesos de RDP (Escritorio remoto) expuestos a Internet y asegurar que las contraseñas de todos los usuarios sean robustas (10 a 12 caracteres como mínimo, evitar palabras comunes, combinar minúsculas, mayúsculas, números, símbolos, etc.). Verificar además otros mecanismos de acceso remoto, tales como SSH, TeamViewer y otros. En caso de tener habilitado RDP u otros mecanismos de acceso remoto, deshabilitarlo en caso de que no sea estrictamente necesario.
- 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, estas copias deben hacerse de forma regular y deben mantenerse en un dispositivo independiente (disco duro externo, o servicios en la nube como OneDrive, Dropbox, etc.)
- Contar con soluciones de antivirus/firewall y mantenerlo actualizado, de modo a prevenir la infección.

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 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

- 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. Además de no existir ninguna garantía por parte de los cibercriminales, en muchas ocasiones, víctimas que han pagado el rescate no han podido recuperar sus archivos.

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).

Información adicional:

https://www.bleepingcomputer.com/news/security/wallet-ransomware-master-keys-released-on-bleepingcomputer-avast-releases-free-decryptor/

https://www.bleepingcomputer.com/news/security/alleged-master-keys-for-the-dharma-ransomware-released-on-bleepingcomputer-com/

http://blog.segu-info.com.ar/2017/05/claves-de-descifrado-de-wallet.html

https://www.cert.gov.py/application/files/2714/7930/0272/Boletin_20161116_CrySIS.pdf

https://www.cert.gov.py/application/files/3714/9546/9011/Boletin_20170517_Ransomware_Dharma.pdf

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 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py