BOLETÍN DE ALERTA

Boletín Nro.: 2016-05
Fecha de publicación: 15/02/2016
Tema: Herramienta para desencriptar archivos encriptados por Teslacrypt

Descripción:

Recientemente se ha encontrado una vulnerabilidad en el ransomware Teslacrypt, la cual ha permitido recuperar archivos encriptados por este ransomware.
A fines de noviembre del año pasado se observó un aumento importante de campañas de distribución de una nueva versión de Teslacrypt, a través de correos electrónicos con adjuntos .zip. Teslacrypt es un ransomware, un tipo de software malicioso (malware) que encripta los archivos, exigiendo que la víctima pague un "rescate" de 500 ~ 1000 US$ para desencriptarlos.

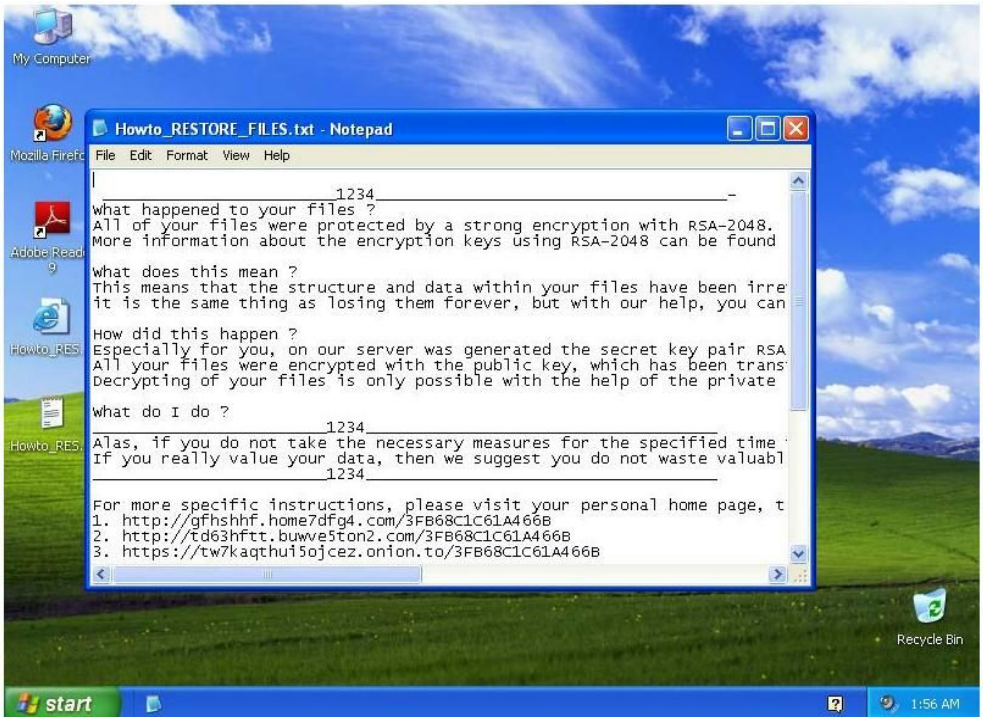

Figura 1: Mensaje de alerta de Teslacrypt

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

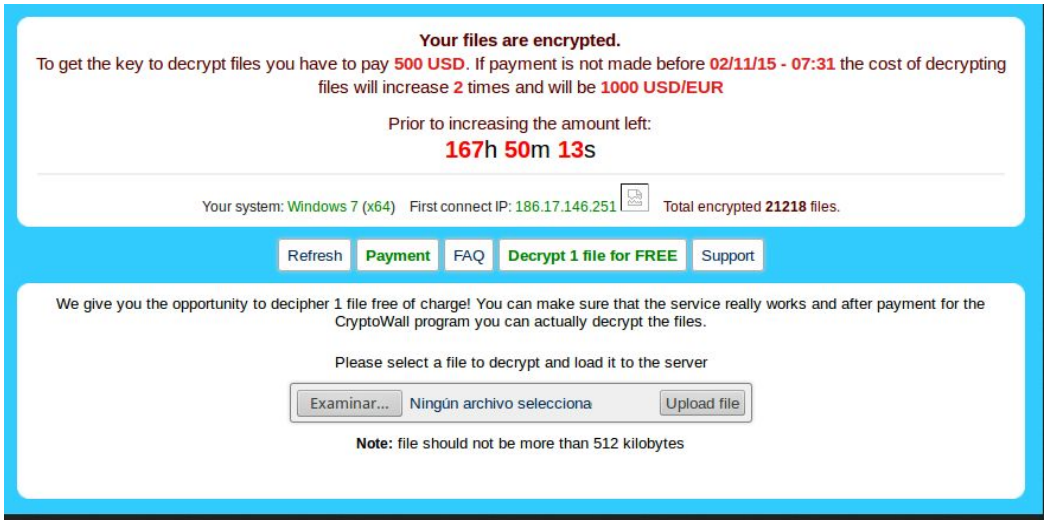

Figura 2: Instrucciones para el pago de Teslacrypt

Investigadores han descubierto una vulnerabilidad en el ransomware, que permite la desencripción de aquellos archivos encriptados por las versiones anteriores a Teslacrypt 3.0, la cual añade extensiones **.ECC**, **.EZZ**, **.EXX**, **.XYZ**, **.ZZZ**, **.AAA**, **.ABC**, **.CCC**, y **.VVV** a los archivos encriptados.

La vulnerabilidad se encuentra en la manera en que se almacenan las claves de cifrado en el ordenador de la víctima. Cuando TeslaCrypt encripta los archivos utiliza el algoritmo de cifrado AES, un algoritmo de cifrado simétrico, es decir, que utiliza la misma clave para cifrar y descifrar un archivo. Cada vez que se reinicia TeslaCrypt, se genera una nueva clave AES y se almacena en los archivos que fueron cifrados durante esta sesión. Esto significa que algunos archivos en la máquina de la víctima podría ser cifrados con una clave diferente a otros archivos. Dado que los desarrolladores de Teslacrypt querían almacenar estas claves en todos los archivos cifrados, necesitaban una manera de asegurar que la víctima no pudiera simplemente extraer su clave y descifrar sus archivos. Para proteger esta clave, los desarrolladores utilizaron otro algoritmo, ECDH, para cifrar esta clave y luego almacenar la información de esta clave cifrada en cada archivo cifrado. La robustez del algoritmo ECDH se basa, principalmente, en la longitud de los números primos elegidos como base.

```
struct file_data_struct
{
    int reserved;
    char master_btc_pub_oct[65];           //byte representation
    char master_ecdh_secret_mul_hex[130];  //string representation
    char session_pub_oct[65];              //byte representation
    char session_ecdh_secret_mul_hex[130]; //string representation
    char iv[16];                           //init-vector for AES-CBC
    int orig_file_size;                    //original file size
};
```

Figura 3: Cabecera de archivo encriptado por Teslacrypt

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

Sin embargo, la longitud de esta clave almacenada no es lo suficientemente larga para la potencia de procesamiento promedio disponible actualmente. Así fue posible utilizar programas especializados para factorizar estos grandes números con el fin de recuperar sus números primos. Una vez que se recuperaron los números primos, con la ayuda de una herramienta construida por un investigador, TeslaCrack, es posible reconstruir la clave de descifrado.
Como los números primos varían para cada víctima, a algunos, el proceso de recuperación de los archivos podría tomar tan poco como 5 minutos, mientras que a otros podría llevar días.

Solución:

La herramienta Teslacrack fue desarrollada por un investigador de alias Googulator, y se encuentra disponible en el siguiente enlace: https://github.com/Googulator/TeslaCrack.
Ha sido escrita en Python, y puede ser ejecutada en sistema operativo Unix o Windows. Sin embargo, la misma requiere un nivel de conocimiento técnico intermedio/avanzado.
Otro investigador de alias Bloodydolly ha incorporado parte de esta herramienta y sus conceptos en la antigua herramienta TeslaDecoder, la cual servía para versiones antiguas de Teslacrypt. Con esta actualización, TeslaDecoder permite también desencriptar los archivos encriptados por las versiones nuevas. Esta herramienta requiere un conocimiento técnico básico/intermedio y se encuentra disponible aquí:
http://download.bleepingcomputer.com/BloodDolly/TeslaDecoder.zip
La misma es más sencilla de usar, ya que no requiere estar familiarizado con el uso de la consola de línea de comandos de Windows ni con Python. La misma debe ser ejecutada en sistema operativo Windows.
Ambas herramientas permiten desencriptar archivos que han sido encriptados por aquellas versiones de Teslacrypt que añaden extensiones ECC, .EZZ, .EXX, .XYZ, .ZZZ, .AAA, .ABC, .CCC, o .VVV.

Recientemente los desarrolladores de Teslacrypt han corregido la vulnerabilidad y publicado una nueva versión, Teslacrypt v3.0 que añade una extensión '.xxx', '.micro' y '.ttt', las cuales hasta el momento no pueden ser desencriptadas.

El CERT-PY ha desarrollado una guía para la desencripción de los archivos utilizando la herramienta TeslaDecoder, la misma puede ser obtenida aquí:
Guia_TeslaDecoder.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

Nota:
El proceso de desencripción de los archivos depende principalmente de la longitud de los primos utilizados durante la encriptación de las claves AES, los cuales varían cada vez que Teslacrypt se ejecuta. Es por eso que el proceso puede variar en cada víctima, incluso entre los diversos archivos de una misma víctima, pudiendo ser desencriptados en 10 minutos en el mejor de los casos, o varios días. Algunas víctimas han reportado que no han logrado desencriptar sus archivos con ninguna de las dos herramientas.

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://www.bleepingcomputer.com/news/security/teslacrypt-decrypted-flaw-in-teslacrypt-allows-victims-to-recover-their-files/
https://github.com/Googulator/TeslaCrack
http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information#ransom
http://www.bleepingcomputer.com/news/security/new-telsacrypt-version-adds-the-vvv-extension-to-encrypted-files/
http://download.bleepingcomputer.com/BloodDolly/TeslaDecoder.zip

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