Guía de seguridad

Guía Nro.: 2016-01
Fecha de publicación: 15/02/2016
Tema: Instructivo para la desencripción de archivos con TeslaDecoder

Introducción:

La herramienta TeslaDecoder permite recuperar los archivos encriptados por Teslacrypt, desde la versión 0.3.4a a la 2.2.0, distribuida a fines de noviembre de 2015. Las extensiones de los archivos cifrados compatibles son: .ecc (0.3.4a+), .ezz, .exx, .xyz, .zzz, .aaa, .abc, .ccc, .vvv
TeslaCrypt 3.0.0, que añade extensiones .xxx, .ttt y .micro, y posteriores no se puede descifrar por este método.
TeslaDecoder es una herramienta que funciona sobre sistema operativo Windows. Se recomienda ejecutarla como Administrador.
Cabe señalar que el tiempo para la determinación de la clave de descifrado para un archivo cifrado podría ser muy corto (menos de 5 minutos) o muy largo (un par de días), dependiendo de la dificultad de factorización de la clave de determinado archivo, así como de la potencia de procesamiento de la computadora en la cual se ejecutará el proceso. La potencia de procesamiento de factorización es enormemente mayor en computadoras que cuentan tarjeta de vídeo que incorporan tecnología GPU. No hay manera de determinar lo rápido que será recuperar la clave de descifrado.

Instrucciones:

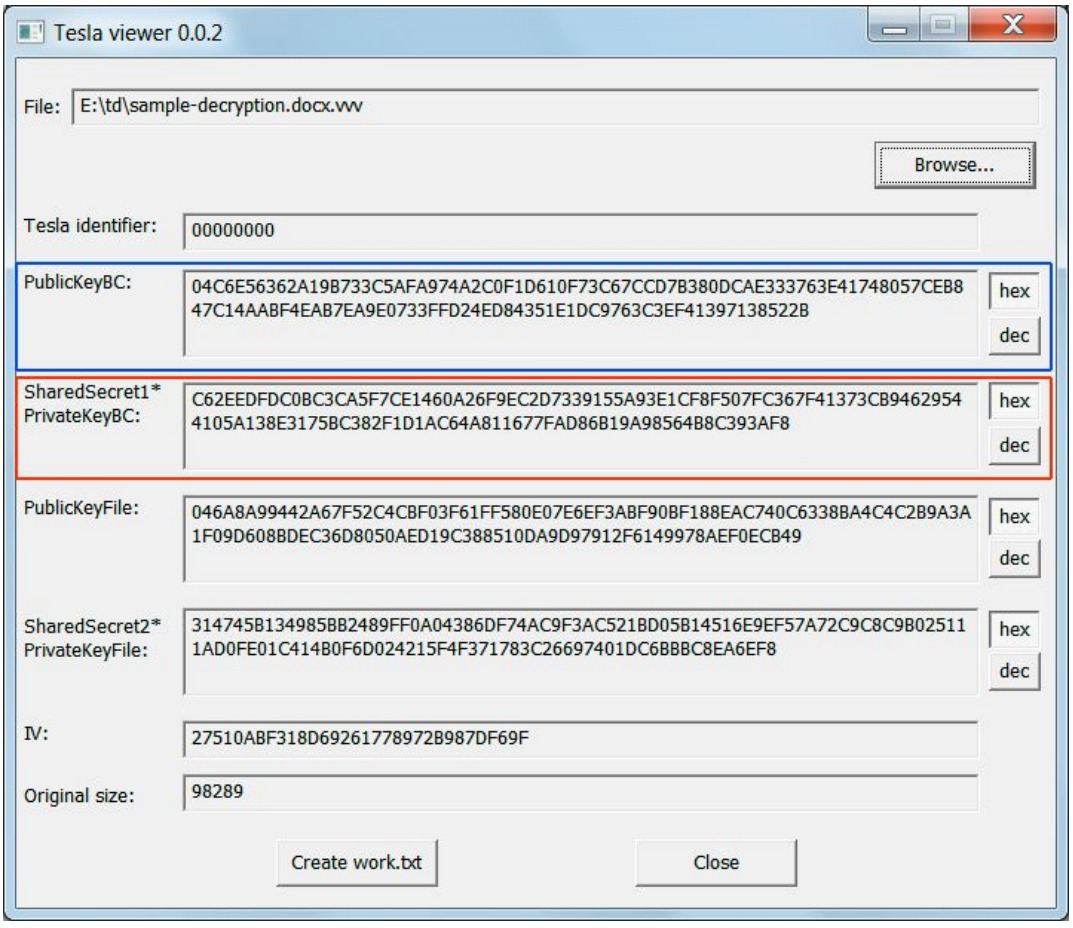
PASO 1:
Cree una carpeta, la cual será utilizada como carpeta de trabajo. Se puede elegir cualquier nombre, sin embargo, para esta guía será nombrada TD. Copie un archivo encriptado en la carpeta TD. Inicialmente copie solo UN archivo de muestra, independientemente de que posea más archivos encriptados.
En caso de tratarse de archivos .ecc o .ezz debe copiar, además, el archivo key.dat que se encuentra en la carpeta % appdata% o el archivo RECOVERY_KEY.TXT ó RECOVERY_FILE.TXT que se encuentra en la carpeta Mis documentos.

PASO 2:

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

Descargue TeslaDecoder del siguiente enlace, y extráigalo en el directorio TD:
http://download.bleepingcomputer.com/BloodDolly/TeslaDecoder.zip
Descargue Yafu del siguiente enlace, y extráigalo en el directorio TD:
http://download.bleepingcomputer.com/td/yafu.zip

PASO 3:
Ingrese al directorio TD\TeslaDecoder, ejecute "TeslaViewer.exe" y haga click en "Browse". Seleccione el archivo encriptado que ha copiado en el directorio TD. Para variantes .ecc o .ezz encryption seleccione el archivo key.dat en vez del archivo encriptado.
Visualizará información acerca de las claves de encriptación que serán necesarias.

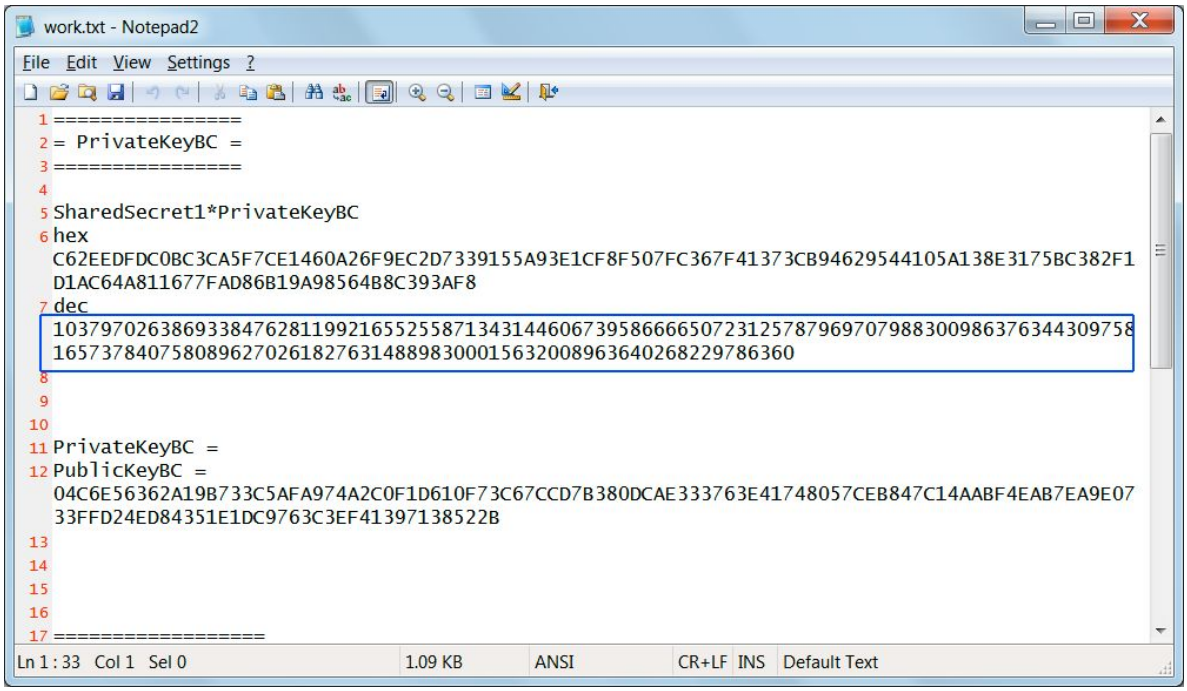


PASO 4:
Haga click en "Create work.txt". Se generará un archivo work.txt que se almacenará en TD\TeslaDecoder, donde estará esta información.

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

PASO 5:

Será necesario realizar la descomposición en factores primos del número decimal SharedSecret1 * PrivateKeyBC. Es posible que este número ya se haya factorizado previamente, para lo cual podemos chequear el sitio http://www.factordb.com/

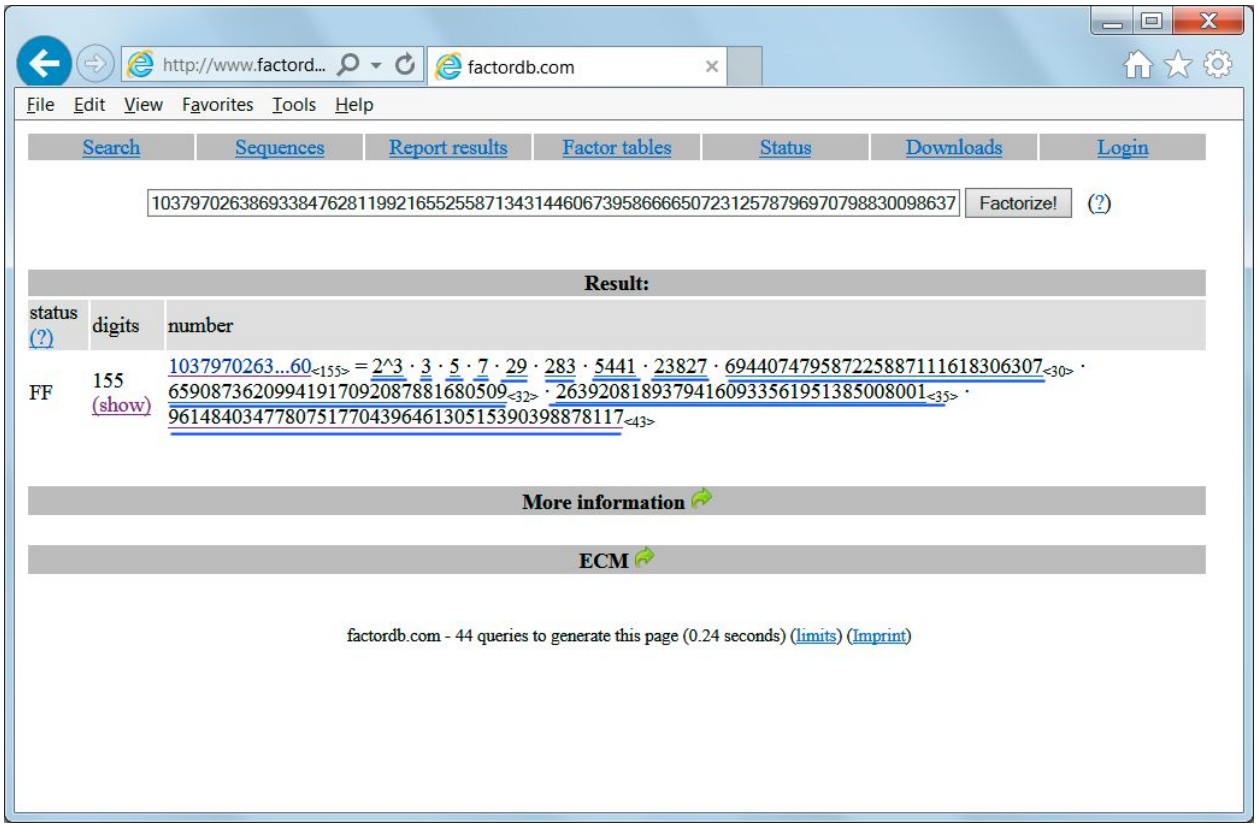


Abra este sitio en el navegador e introduzca el valor decimal de SharedSecret1 * PrivateKeyBC (ver recuadro azul de la imagen anterior) en el buscador de FactorDB y haga click en "Factorize!"..

Cuando aparezcan los resultados, observe la columna "Status". Si es estado es FF como se muestra a continuación, significa que el número se encuentra completamente factorizado. Copie los factores en work.txt, cada uno en líneas separadas y vaya al paso 10.

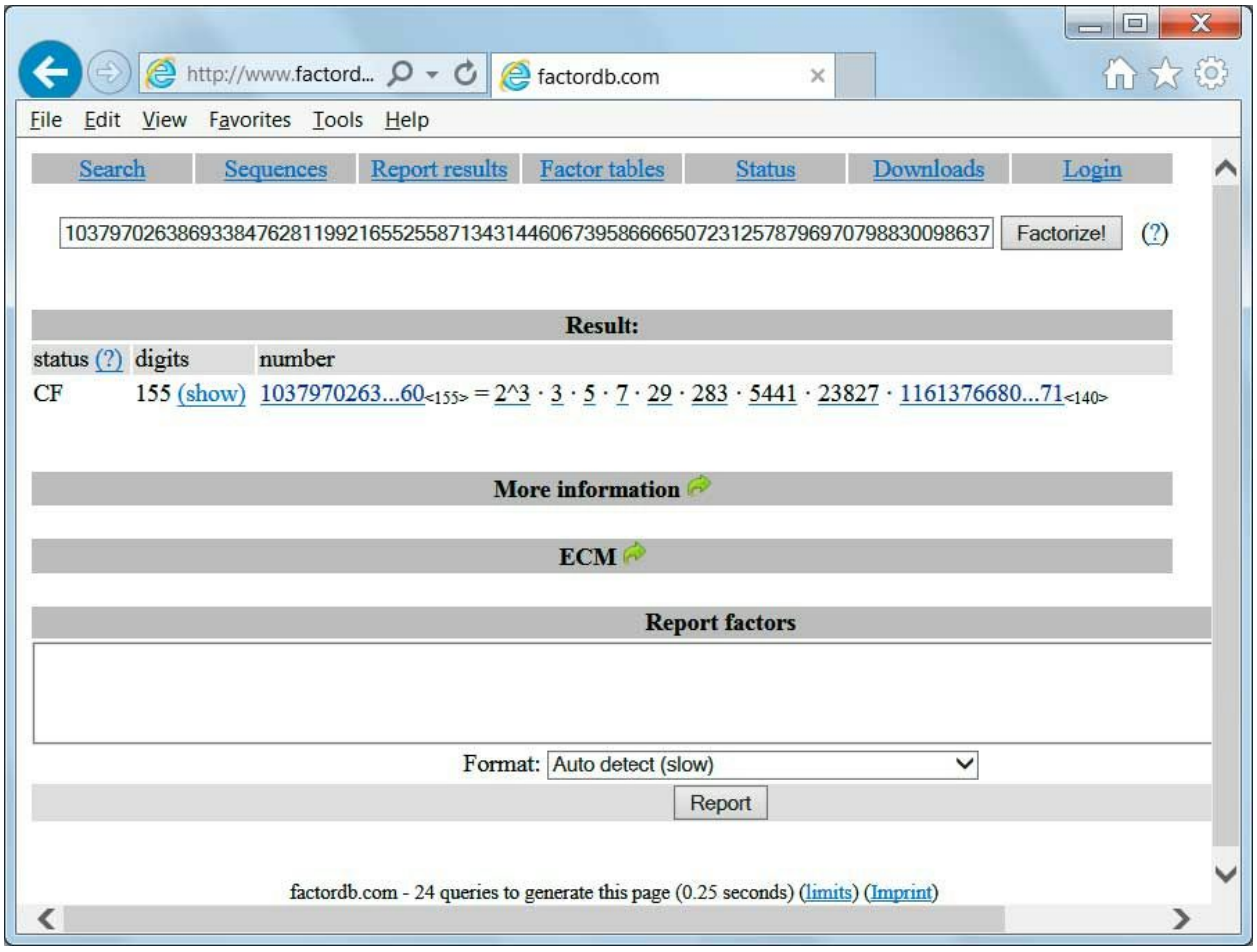
En el caso de factores largos, para ver el número completo, debe hacer click sobre el mismo.

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



Si el estado es CF, sólo algunos de los factores son conocidos y se necesita realizar la factorización del paso 7. Para visualizar completamente el número que no pudo ser factorizado, haga click sobre el número resaltado en azul. Por lo general será el número de mayor longitud (la longitud se encuentra indicada entre paréntesis en la esquina inferior izquierda del número). Copie los factores conocidos en work.txt, en líneas separadas. Copie el número no factorizado en algún documento temporal antes de pasar al paso 7.

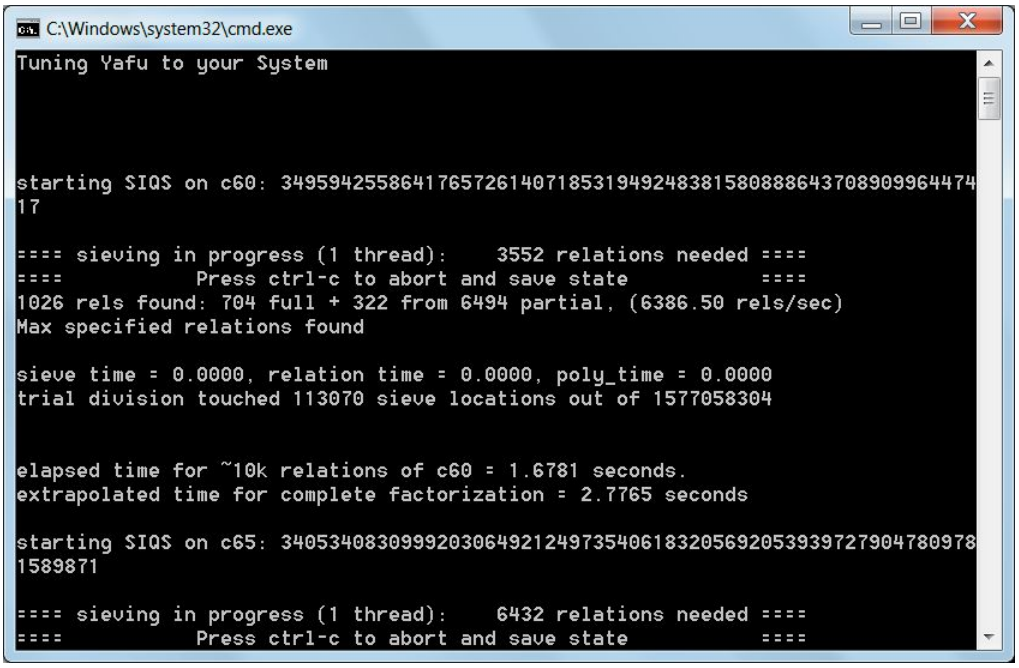
CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py



PASO 7:

Ingrese a TD/Yafu y ejecute "RunYafu.exe". Haga click en "Tune Yafu" para optimizar Yafu con respecto a las características de su computadora. Este proceso puede tomar varios minutos, no cierra la ventana antes de que termine. Al finalizar, la ventana se cerrará sola y podrá pasar al paso 8.

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

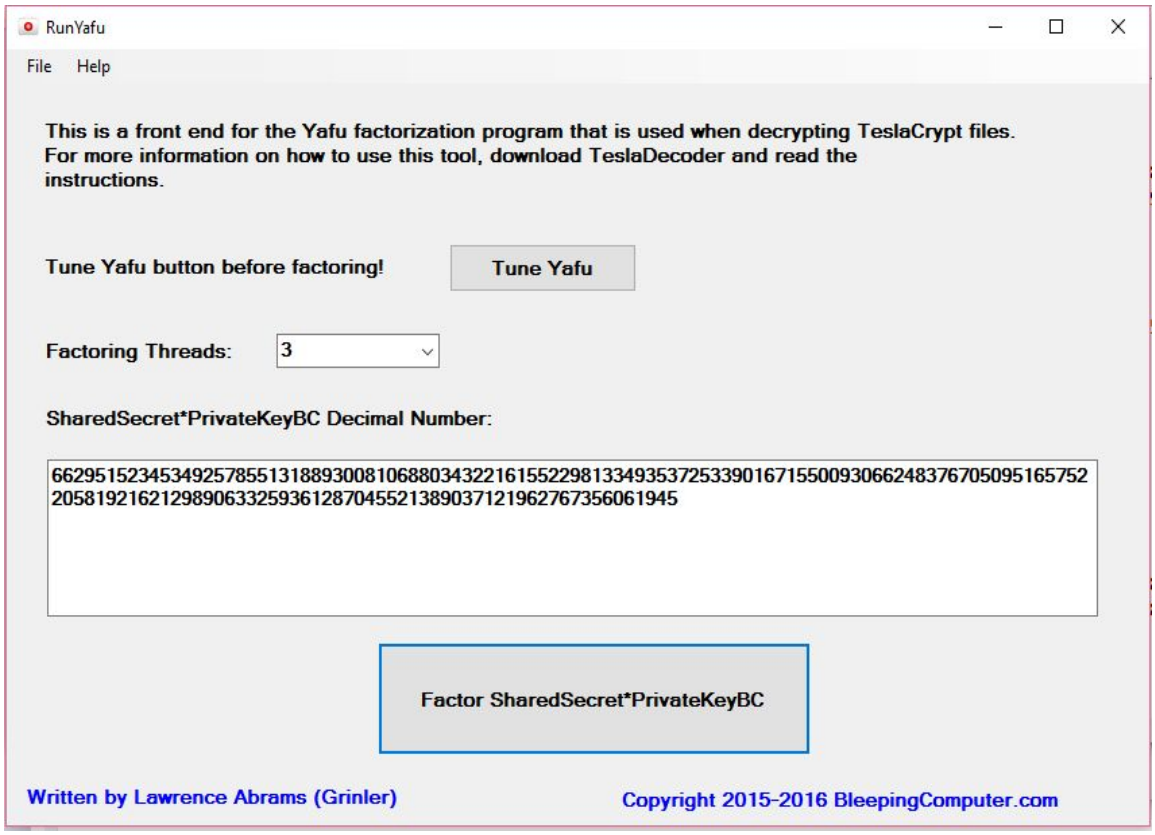


PASO 8:

Pegue el número no factorizado que obtuvo de FactorDB.com en el paso 6 en el recuadro "SharedSecret1 * PrivateKeyBC". En "Factoring Threads" puede elegir la cantidad de núcleos de procesador que dedicará al proceso, de acuerdo a los disponibles. Cuanto mayor cantidad de núcleos elija, más rápido será el proceso. Sin embargo, en caso de que desee trabajar en paralelo en otras tareas, debe elegir un número menor de núcleos. Por ejemplo: Si entre las opciones observa de 1 a 4, elija 3 si quiere poder trabajar en otras tareas en paralelo.

Haga click en "Factor SharedSecret1*PrivateKeyBC"

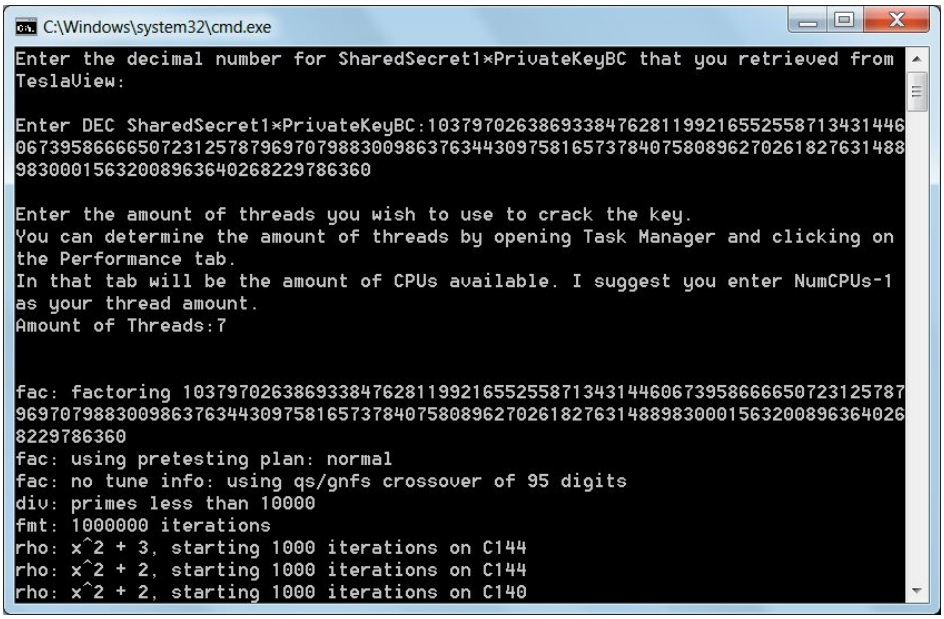
CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py



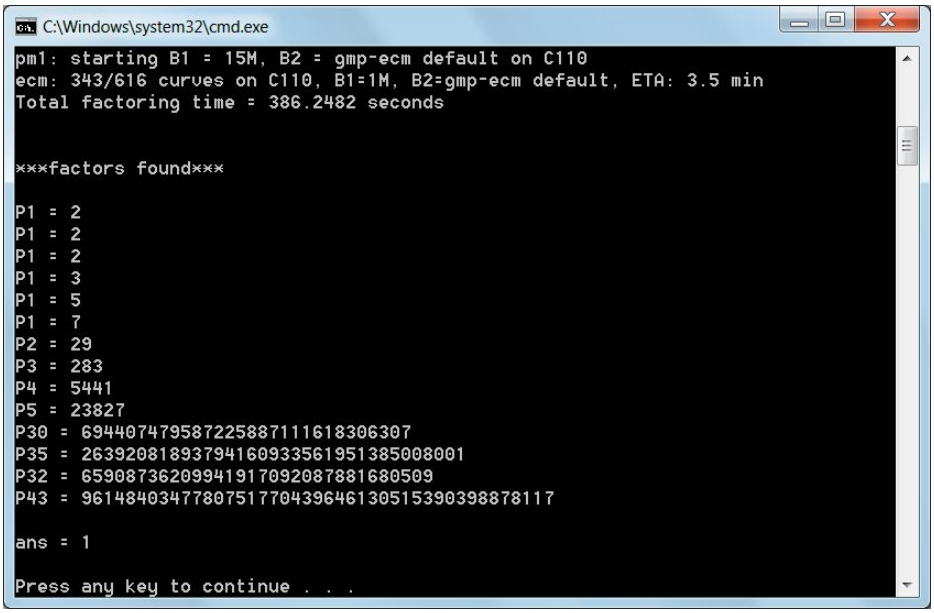
PASO 9:

Iniciará el proceso de factorización, el cual puede demorar desde unos pocos minutos hasta días. No debe cerrar la ventana hasta que el proceso haya terminado.

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



Al finalizar el proceso, se listarán los factores del número. Deberá copiar dichos factores en el archivo work.txt, debajo de los factores que obtuvo en el paso 6, en líneas separadas, y presionar cualquier tecla para cerrar la ventana.



Pegue los factores restantes

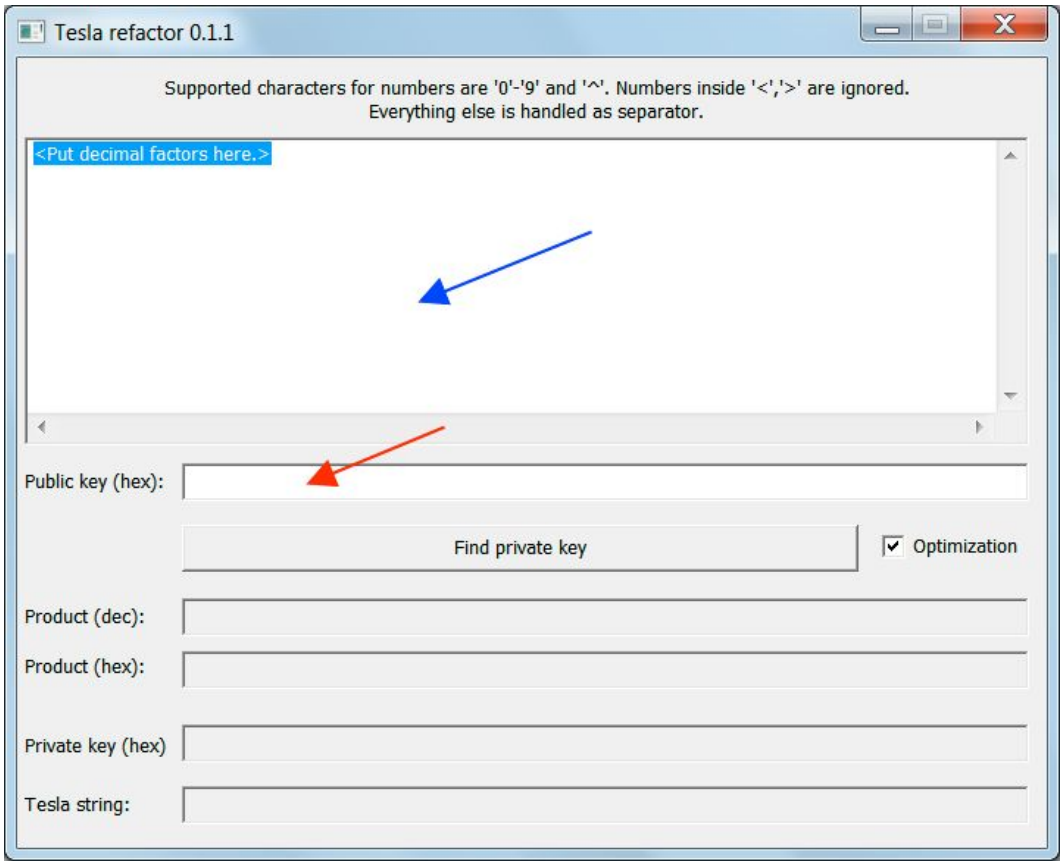
CERT-PY Equipo de Respuestas ante Emergencias Cibernéticas
Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs)
Gral. Santos y Concordia – Complejo Santos – Ofic. E14
cert@cert.gov.py | +595 21 201014 | +595 21 3276902
Asunción - Paraguay | www.cert.gov.py
@CERTpy
/CERT-Py

En caso de haber interrumpido el proceso antes de obtener los factores, deberá eliminar todos los archivos temporales generados por el programa. Para mayor simplicidad, elimine el directorio TD\Yafu y todo su contenido, y descárguelo y/o extráigalo nuevamente, antes de iniciar otro proceso de factorización.

PASO 10:

Ingrese a TD\TeslaDecoder y ejecute "TeslaRefactor.exe". Copie la lista de los factores que ha anotado en el archivo work.txt y péguelos en el recuadro de texto grande (ver flecha azul).

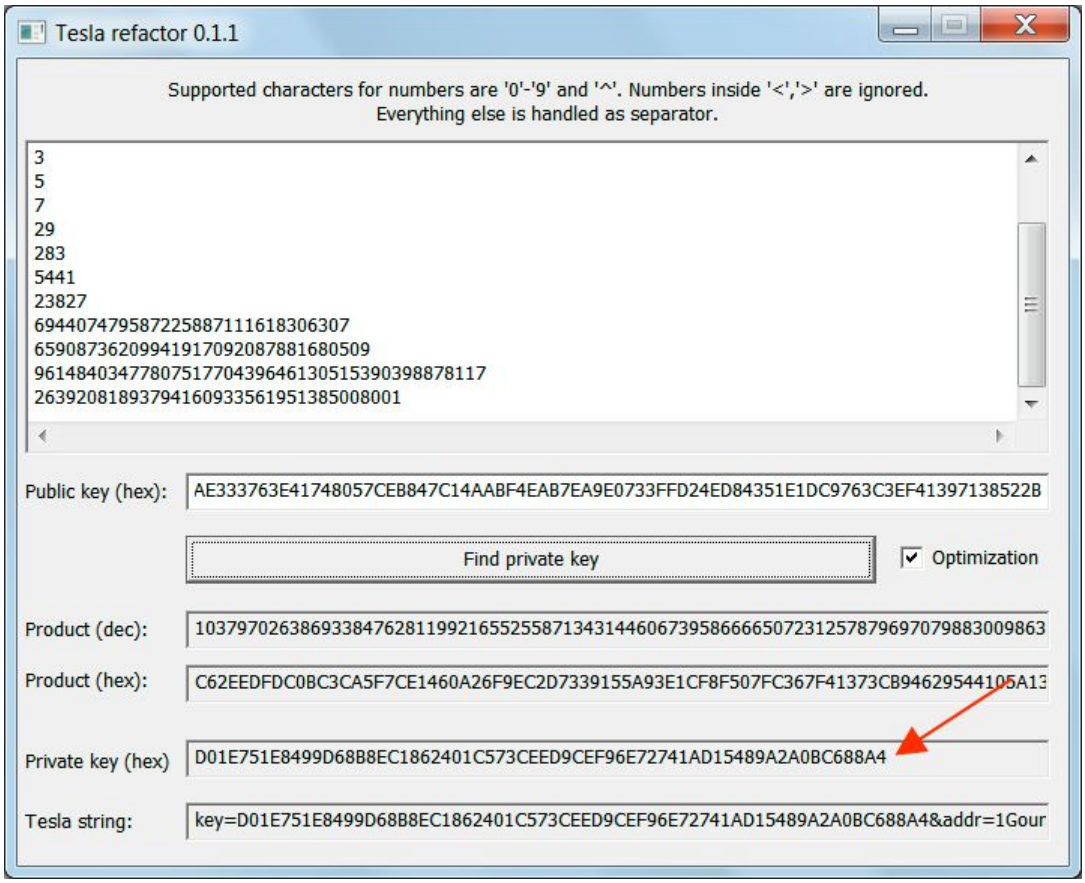
Copie el valor PublicKeyBC que se encuentra en el archivo work.txt y péguelo en el campo "Public key (hex)" (ver flecha roja).



PASO 11:

Una vez completados los campos, haga click en "Find Private Key". TeslaRefactor reconstruirá el valor de la clave, la cual aparecerá en el campo "Private key (hex)" (ver flecha roja).

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



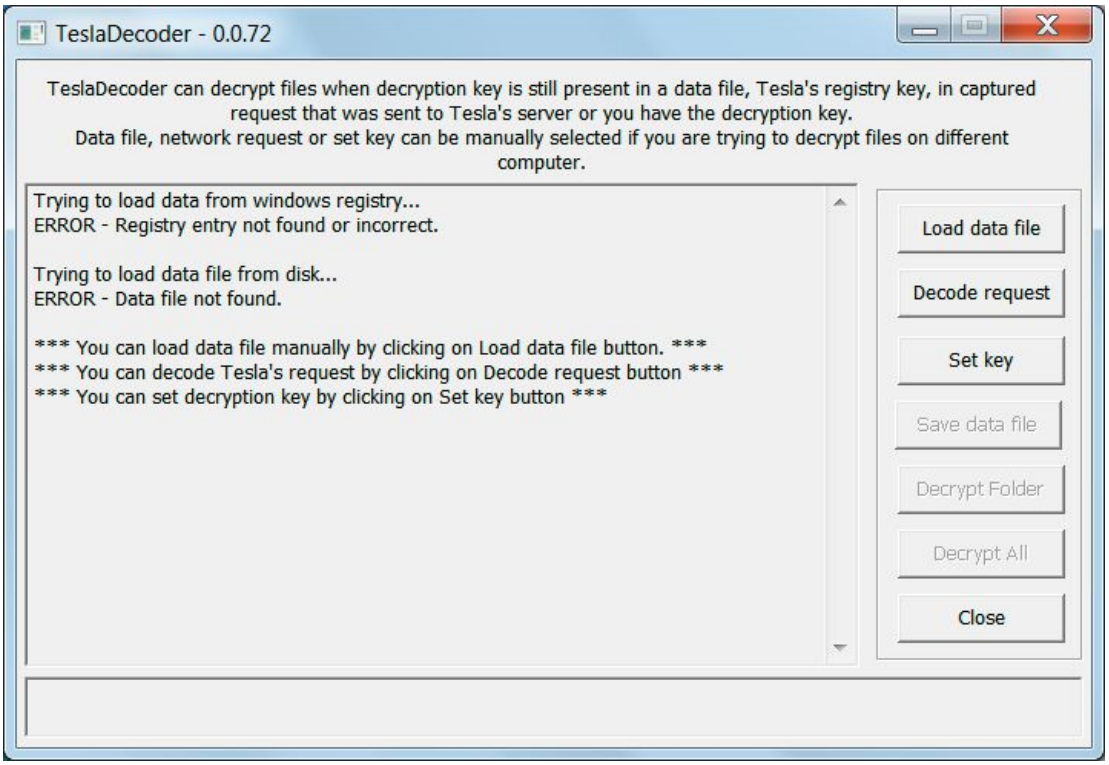
Para verificar el valor de esta clave, chequee si el valor de Product (dec) es igual al valor decimal de SharedSecret1*PrivateKeyBC que se encuentra en el archivo work.txt.

Copie el valor de "Private key (hex)" en work.txt antes de continuar al siguiente paso.

PASO 12:

Ingrese a TD\TeslaDecoder y ejecute "TeslaDecoder.exe" como administrador. Para ello debe hacer click derecho sobre el programa y seleccionar "Run as Administrator" (o "Ejecutar como Administrador").

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



Haga click en "Set key" y ingrese el valor de "Private key (hex)" que obtuvo en el paso anterior. Seleccione la extensión de sus archivos.

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

Haga click en "Set key". Ahora puede realizar una prueba de descifrado en el archivo de muestra que ha copiado previamente en la carpeta TD. Para ello, haga click en "Decrypt Folder" y seleccione el directorio TD. Si el archivo se descifra con éxito, a continuación, haga click en "Decrypt All" para descifrar todos los archivos en su disco duro.

En caso de que no todos los archivos fueran desencriptados, es posible que el conjunto de archivos en los que falló el proceso posean otra clave. Para esto, debe tomar como muestra un archivo no desencriptado y copiarlo en la carpeta TD y repetir todo el proceso, desde el paso 3 hasta el final.

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.

En caso de dudas o problemas, puede contactar al CERT-PY, a través de la información de contacto que se encuentra en el pie de página, o consultar en los foros especializados, los cuales cuentan con un soporte activo de la comunidad y del autor de la herramienta, BloodDolly:
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/

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
http://www.bleepingcomputer.com/forums/t/576600/tesladecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-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