



## Guía de seguridad

**Guía Nro.:** 2016-01

**Fecha de publicación:** 15/02/2016

**Tema:** Instructivo para la descricción 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:**



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.

Tesla viewer 0.0.2

File: E:\td\sample-decryption.docx.vvv

Browse...

Tesla identifier: 00000000

PublicKeyBC: 04C6E56362A19B733C5AFA974A2C0F1D610F73C67CCD7B380DCAE333763E41748057CEB8  
47C14AABF4EAB7EA9E0733FFD24ED84351E1DC9763C3EF41397138522B hex dec

SharedSecret1\*  
PrivateKeyBC: C62EEDFDC0BC3CA5F7CE1460A26F9EC2D7339155A93E1CF8F507FC367F41373CB9462954  
4105A138E3175BC382F1D1AC64A811677FAD86B19A98564B8C393AF8 hex dec

PublicKeyFile: 046A8A99442A67F52C4CBF03F61FF580E07E6EF3ABF90BF188EAC740C6338BA4C4C2B9A3A  
1F09D608BDEC36D8050AED19C388510DA9D97912F6149978AEF0ECB49 hex dec

SharedSecret2\*  
PrivateKeyFile: 314745B1349858B2489FF0A04386DF74AC9F3AC521BD05814516E9EF57A72C9C8C9802511  
1AD0FE01C414B0F6D024215F4F371783C26697401DC6BBBC8EA6EF8 hex dec

IV: 27510ABF318D69261778972B987DF69F

Original size: 98289

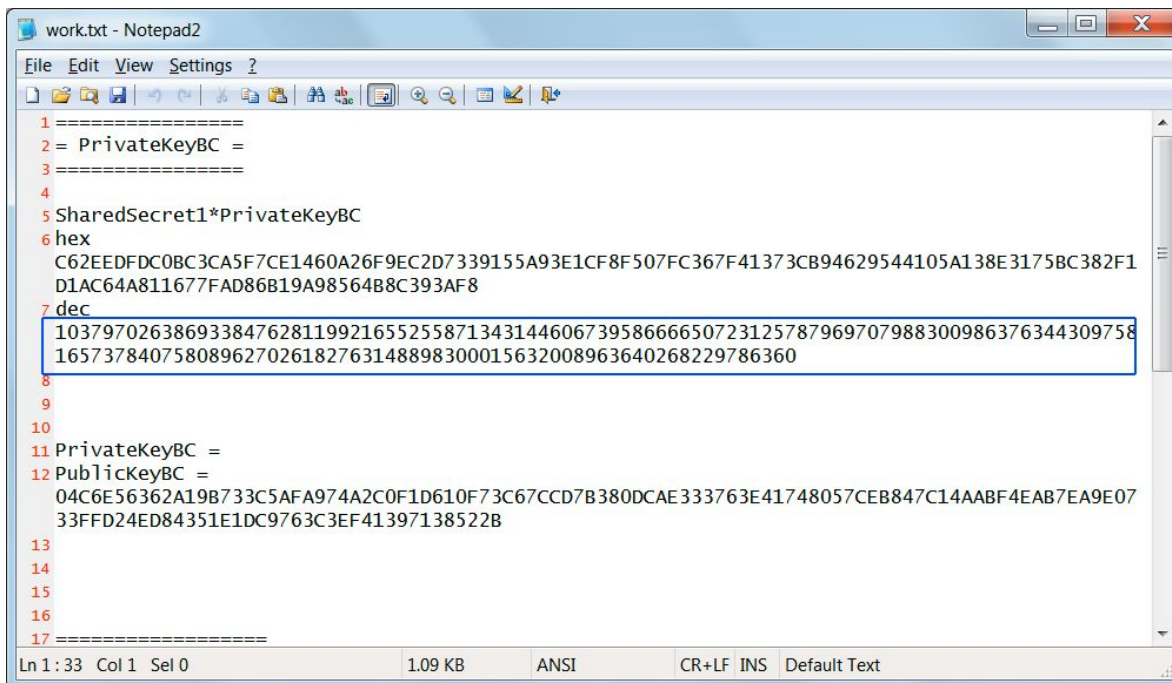
Create work.txt Close

### PASO 4:

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

#### 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/>



```
1 =====
2 = PrivateKeyBC =
3 =====
4
5 SharedSecret1*PrivateKeyBC
6 hex
7 C62EEDFDC0BC3CA5F7CE1460A26F9EC2D7339155A93E1CF8F507FC367F41373CB94629544105A138E3175BC382F1
8 D1AC64A811677FAD86B19A98564B8C393AF8
9 dec
10 10379702638693384762811992165525587134314460673958666650723125787969707988300986376344309758
11 165737840758089627026182763148898300015632008963640268229786360
12
13 PrivateKeyBC =
14 PublicKeyBC =
15 04C6E56362A19B733C5AFA974A2C0F1D610F73C67CCD7B380DCAE333763E41748057CEB847C14AABF4EAB7EA9E07
16 33FFD24ED84351E1DC9763C3EF41397138522B
17 =====
Ln 1: 33 Col 1 Sel 0 1.09 KB ANSI CR+LF INS Default Text
```

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 el 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.



The screenshot shows a web browser window with the URL <http://www.factordb.com>. The page has a navigation bar with links: Search, Sequences, Report results, Factor tables, Status, Downloads, and Login. A search bar contains the number 1037970263869338476281199216552558713431446067395866665072312578796970798830098637, followed by a 'Factorize!' button and a help icon. Below the search bar, a 'Result:' section displays a table with columns 'status', 'digits', and 'number'. The status is 'FF', digits are '155', and the number is a large integer with a blue highlight on the first part. Below the number, there is a 'More information' link and an 'ECM' link. At the bottom, a footer indicates 'factordb.com - 44 queries to generate this page (0.24 seconds) (limits) (Imprint)'.

status	digits	number
FF	155	1037970263...60<155> = 2^3 · 3 · 5 · 7 · 29 · 283 · 5441 · 23827 · 694407479587225887111618306307<30> · 65908736209941917092087881680509<32> · 26392081893794160933561951385008001<35> · 9614840347780751770439646130515390398878117<43>

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.



The screenshot shows a web browser window with the URL <http://www.factordb.com>. The page has a navigation bar with links: Search, Sequences, Report results, Factor tables, Status, Downloads, and Login. A search bar contains the number 1037970263869338476281199216552558713431446067395866665072312578796970798830098637, followed by a 'Factorize!' button. Below the search bar, the 'Result:' section shows the status 'CF' and the number '1037970263...60<155>' which is equal to the product of prime factors:  $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 29 \cdot 283 \cdot 5441 \cdot 23827 \cdot 1161376680...71<140>$ . There are links for 'status', 'digits', and 'number'. Below the result, there are sections for 'More information', 'ECM', and 'Report factors'. At the bottom, there is a 'Format' dropdown menu set to 'Auto detect (slow)' and a 'Report' button. The footer of the page indicates 'factordb.com - 24 queries to generate this page (0.25 seconds)' and provides links for 'limits' and 'Imprint'.

#### PASO 7:

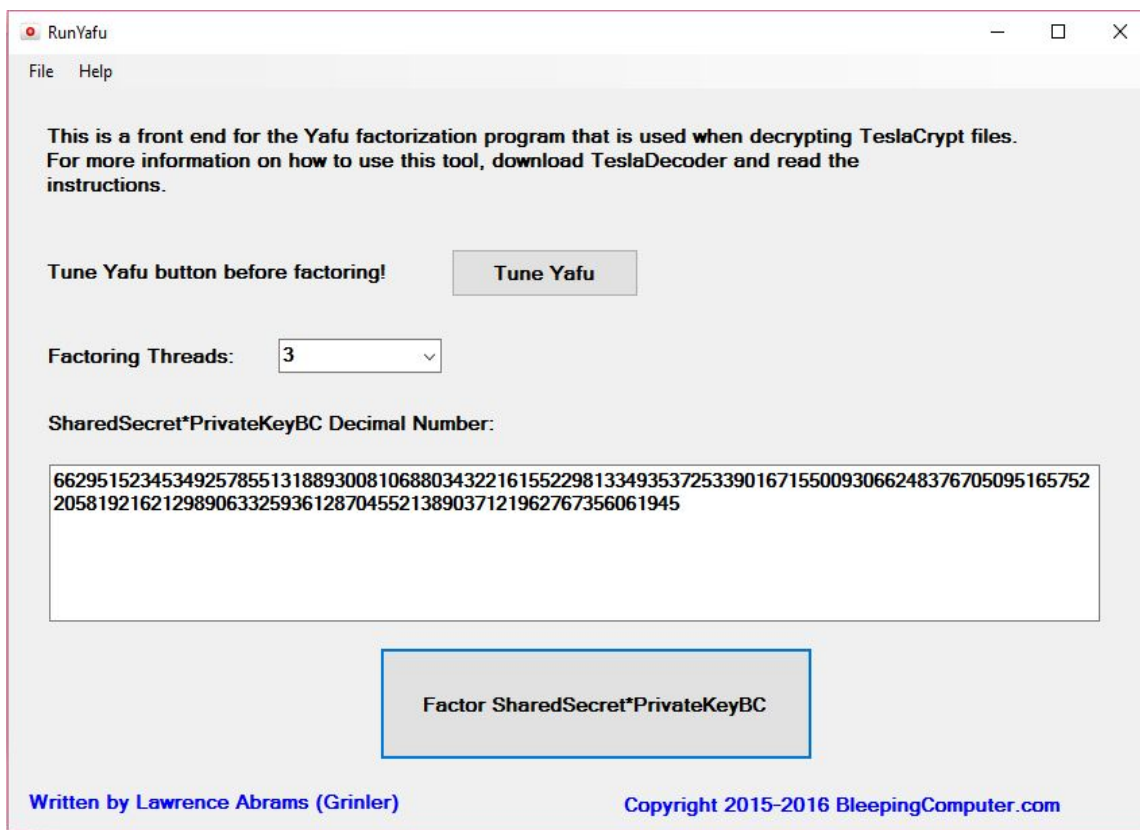
Ingresa a TD/Yafu y ejecute "RunYafu.exe". Haga click en "Tune Yafu" para optimizar Yafu con respecto a las características de su computadora. Este proceso puede tomar varios minutos, no cierra la ventana antes de que termine. Al finalizar, la ventana se cerrará sola y podrá pasar al paso 8.



#### 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"



#### 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.

```
C:\Windows\system32\cmd.exe

Enter the decimal number for SharedSecret1*PrivateKeyBC that you retrieved from
TeslaView:

Enter DEC SharedSecret1*PrivateKeyBC:1037970263869338476281199216552558713431446
06739586666507231257879697079883009863763443097581657378407580896270261827631488
98300015632008963640268229786360

Enter the amount of threads you wish to use to crack the key.
You can determine the amount of threads by opening Task Manager and clicking on
the Performance tab.
In that tab will be the amount of CPUs available. I suggest you enter NumCPUs-1
as your thread amount.
Amount of Threads:7

fac: factoring 10379702638693384762811992165525587134314460673958666650723125787
96970798830098637634430975816573784075808962702618276314889830001563200896364026
8229786360
fac: using pretesting plan: normal
fac: no tune info: using qs/gnfs crossover of 95 digits
div: primes less than 10000
fmt: 1000000 iterations
rho: x^2 + 3, starting 1000 iterations on C144
rho: x^2 + 2, starting 1000 iterations on C144
rho: x^2 + 2, starting 1000 iterations on C140
```

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.

```
C:\Windows\system32\cmd.exe

pm1: starting B1 = 15M, B2 = gmp-ecm default on C110
ecm: 343/616 curves on C110, B1=1M, B2=gmp-ecm default, ETA: 3.5 min
Total factoring time = 386.2482 seconds

***factors found***

P1 = 2
P1 = 2
P1 = 2
P1 = 3
P1 = 5
P1 = 7
P2 = 29
P3 = 283
P4 = 5441
P5 = 23827
P30 = 694407479587225887111618306307
P35 = 26392081893794160933561951385008001
P32 = 65908736209941917092087881680509
P43 = 9614840347780751770439646130515390398878117

ans = 1
Press any key to continue . . .
```

Pegue los factores restantes

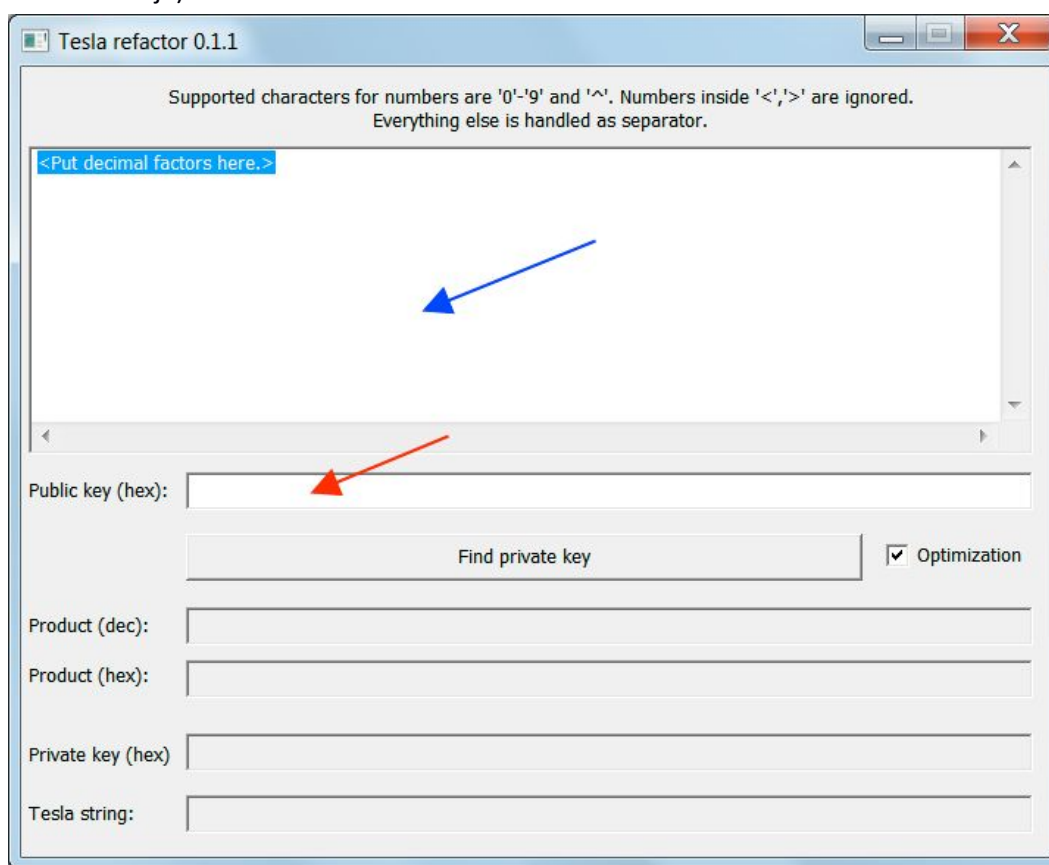


En caso de haber interrumpido el proceso antes de obtener los factores, deberá eliminar todos los archivos temporales generados por el programa. Para mayor simplicidad, elimine el directorio TD\Yafu y todo su contenido, y descárguelo y/o extraígallo nuevamente, antes de iniciar otro proceso de factorización.

#### PASO 10:

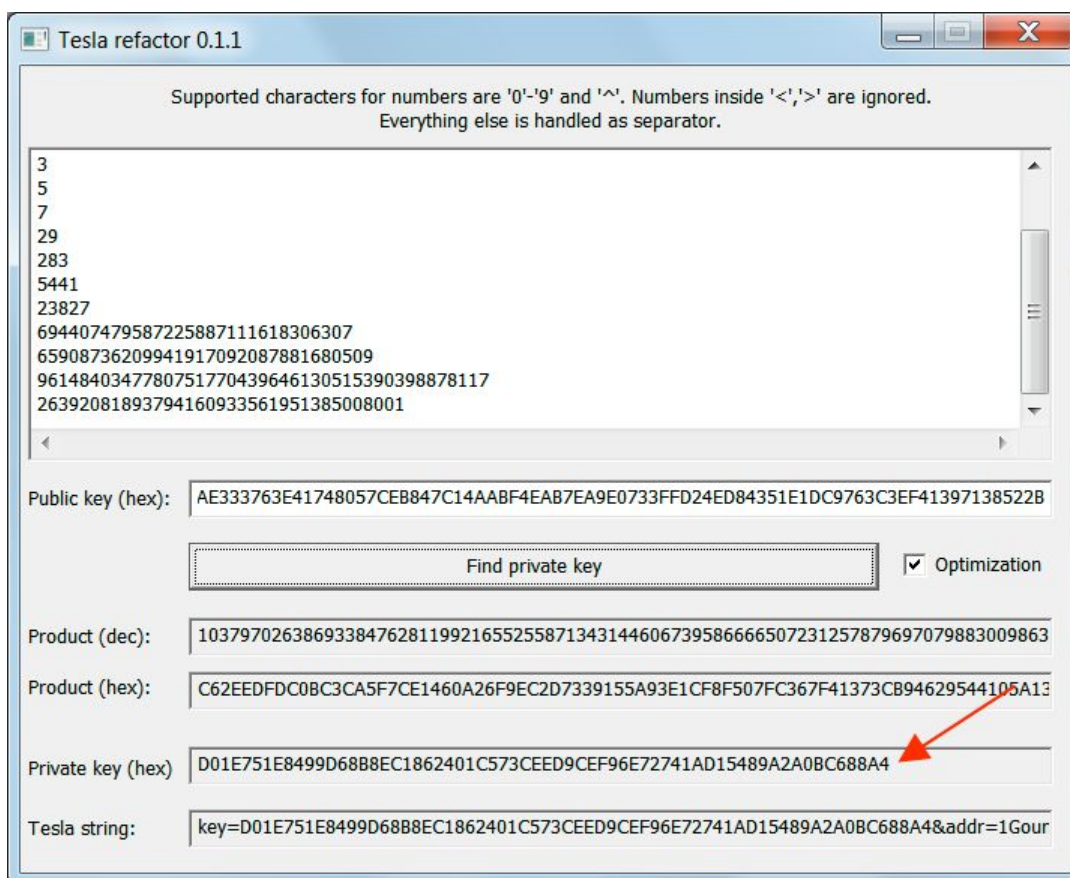
Ingresa a TD\TeslaDecoder y ejecute "TeslaRefactor.exe". Copie la lista de los factores que ha anotado en el archivo work.txt y péguelos en el recuadro de texto grande (ver flecha azul).

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).

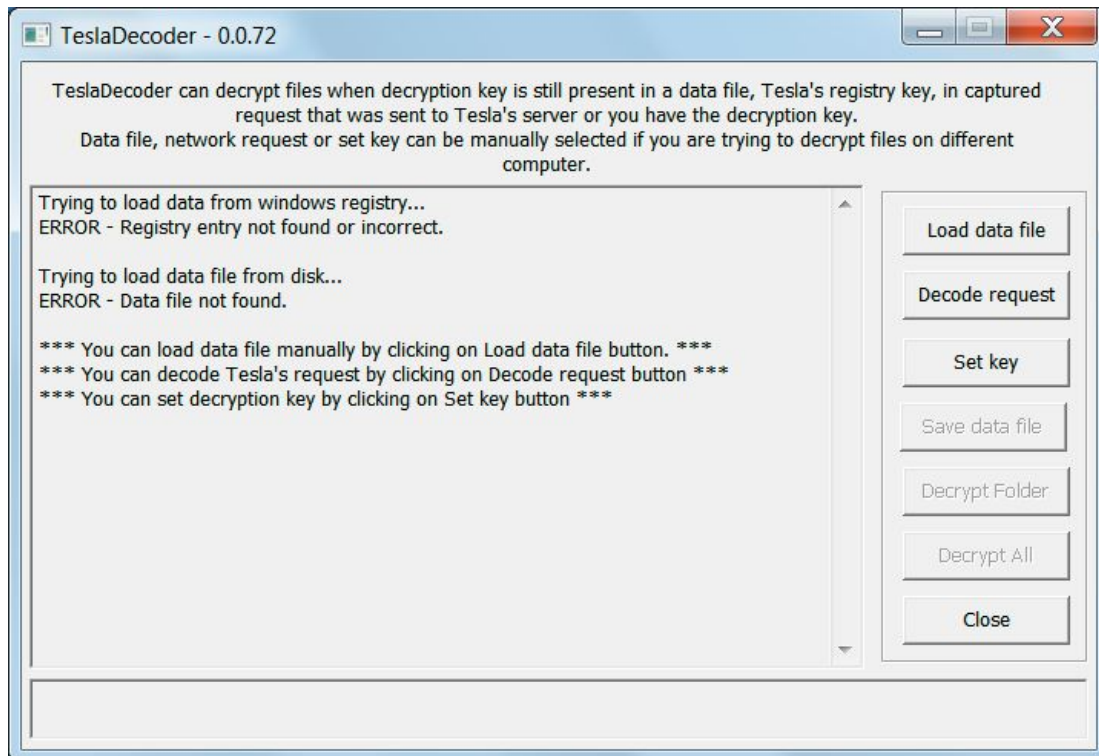


Para verificar el valor de esta clave, chequee si el valor de Product (dec) es igual al valor decimal de SharedSecret1\*PrivateKeyBC que se encuentra en el archivo work.txt.

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

#### PASO 12:

Ingresa 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").



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.





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 descriptados, 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 descriptado y copiarlo en la carpeta TD y repetir todo el proceso, desde el paso 3 hasta el final.

#### **Nota:**

El proceso de descriptación 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 descriptados en 10 minutos en el mejor de los casos, o varios días. Algunas víctimas han reportado que no han logrado descriptar 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/tesldecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/>

#### **Información adicional:**

<http://www.bleepingcomputer.com/news/security/teslacrypt-decrypt-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/tesldecoder-released-to-decrypt-exx-ezz-ecc-files-encrypted-by-teslacrypt/>