





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:









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.

File: E:\td\samp	le-decryption.docx.vvv	
Tesla identifier:	0000000	•
PublicKeyBC:	04C6E56362A19B733C5AFA974A2C0F1D610F73C67CCD7B380DCAE333763E41748057CEB8 47C14AABF4EAB7EA9E0733FFD24ED84351E1DC9763C3EF41397138522B	hex dec
SharedSecret1* PrivateKeyBC:	C62EEDFDC0BC3CA5F7CE1460A26F9EC2D7339155A93E1CF8F507FC367F41373CB9462954 4105A138E3175BC382F1D1AC64A811677FAD86B19A98564B8C393AF8	hex dec
PublicKeyFile:	046A8A99442A67F52C4CBF03F61FF580E07E6EF3ABF90BF188EAC740C6338BA4C4C2B9A3A 1F09D608BDEC36D8050AED19C388510DA9D97912F6149978AEF0ECB49	hex dec
SharedSecret2* PrivateKeyFile:	314745B134985BB2489FF0A04386DF74AC9F3AC521BD05B14516E9EF57A72C9C8C9B02511 1AD0FE01C414B0F6D024215F4F371783C26697401DC6BBBC8EA6EF8	hex dec
IV:	27510ABF318D69261778972B987DF69F	
Original size:	98289	

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 <u>http://www.factordb.com/</u>

🔋 work.txt - Notepad2						۲.
<u>File Edit View Settings ?</u>						
🗋 😂 🛱 🛃 🥑 🗠 🐰 🖬 🏙 🛤 🍇 🗔	🥹 🤤 🖂	1				
1						
2 = PrivateKeyBC =						
3 ================						
4 chanadCacnat1*DrivataKavDC						
s Shareusecreti*PrivatekeyBC						
C62EEDEDC0BC3CA5E7CE1460A26E9E	C2D7339155	A93E1CE8E507	C 367F	413	73CB94629544105A138F3175BC382F1	Ξ
D1AC64A811677FAD86B19A98564B8C	393AF8		COUL	123		
7 dec						
103797026386933847628119921655	2558713431	446067395866	565072	312	5787969707988300986376344309758	
165737840758089627026182763148	8983000156	320089636402	582297	863	60	
8						
9						
11 PrivateKeyPC -						
12 PublicKeyBC =						
04C6E56362A19B733C5AFA974A2C0F	1D610F73C6	7CCD7B380DCA	33376	3E4	1748057CEB847C14AABF4EAB7EA9E07	6
33FFD24ED84351E1DC9763C3EF4139	7138522B					
13						
14						
15						
16						_
	1.00 //0	ANICI	CD	TALC	D. C. H.T. J	-
LN 1:33 COLT SELU	1.09 KB	AIN2I	CK+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 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.









e	ج (ح	http://www.factord 🎗 🗸 🖒 🎯 factordb.com 🛛 🗙	- □ ×	
<u>File</u>	dit <u>V</u> iew	v F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		
	Search	Sequences Report results Factor tables Status Downloads Status	Login	
	1	037970263869338476281199216552558713431446067395866665072312578796970798830098637 Factorize!	<u>?)</u>	
		Result:		
status (?)	digits	number		
FF	155 <u>(show)</u>	$\frac{103797026360_{<155>} = \underline{2^{A_3}} \cdot \underline{3} \cdot \underline{5} \cdot \underline{7} \cdot \underline{29} \cdot \underline{283} \cdot \underline{5441} \cdot \underline{23827} \cdot \underline{694407479587225887111618306307_{<30>} \cdot \underline{65908736209941917092087881680509_{<32>} \cdot \underline{26392081893794160933561951385008001_{<35>} \cdot \underline{9614840347780751770439646130515390398878117_{<43>}}$		
	More information 🥓			
		ECM 🄗		
	factordb.com - 44 queries to generate this page (0.24 seconds) (<u>limits</u>) (<u>Imprint</u>)			
5				

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.









C → Mttp://www.factord ♀ - ♥ @ factordb.com
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp
Search Sequences Report results Factor tables Status Downloads Login
1037970263869338476281199216552558713431446067395866665072312578796970798830098637 Factorize! (?)
Result:
status (?) digits number
CF 155 (show) $103797026360_{<155>} = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 29 \cdot 283 \cdot 5441 \cdot 23827 \cdot 116137668071_{<140>}$
More information 🔗
ECM 🊧
Report factors
Format: Auto detect (slow)
Report
Report
Report factordb.com - 24 queries to generate this page (0.25 seconds) (limits) (Imprint)

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.











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"









RunYafu	<u></u>		Х
File Help			
This is a front end for the Yafu factorization program that is used when decrypting TeslaCu For more information on how to use this tool, download TeslaDecoder and read the instructions.	ypt files.		
Tune Yafu button before factoring! Tune Yafu			
Factoring Threads: 3			
SharedSecret*PrivateKeyBC Decimal Number:			
6629515234534925785513188930081068803432216155229813349353725339016715500930662483 2058192162129890633259361287045521389037121962767356061945	376705095	165752	
Factor SharedSecret*PrivateKeyBC			
Written by Lawrence Abrams (Grinler) Copyright 2015-2016 BleepingC	computer.c	com	

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 <u>*</u> TeslaUiew:
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 9229786360
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 - Z P1 = 3	
P1 = 5	
P1 = 7	
P2 = 29	
P3 = 283	
P4 = 5441	
P5 = 23827	
P35 - 26332061633134160333361351363006001 P32 - 65908736209941917092087881680509	
P32 = 9614846347786751776439646136515396398878117	
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 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).

Tesla refactor 0.1.1	
Supported characters for numbers are '0'-'9' and '^'. Numbers inside '<','>' are Everything else is handled as separator.	ignored.
<put decimal="" factors="" here.=""></put>	*
4	<u></u>
Public key (hex):	
Find private key	Optimization
Product (dec):	
Product (hex):	
Private key (hex)	
Tesla string:	

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).









c	unported characters for numbers are '0'-'0' and '0'. Numbers inside '<' \5' are ignored	
3	Everything else is handled as separator.	
3 5 7 29 283 5441 23827 69440747958722 65908736209941	25887111618306307 .917092087881680509	•
96148403477807 26392081893794	751770439646130515390398878117 H60933561951385008001	_
4	F	×
Public key (hex):	AE333763E41748057CEB847C14AABF4EAB7EA9E0733FFD24ED84351E1DC9763C3EF41397138522	2B
	Find private key 🗸 🗸 Optimizatio	on
Product (dec):	1037970263869338476281199216552558713431446067395866665072312578796970798830098	63
Product (hex):	C62EEDFDC0BC3CA5F7CE1460A26F9EC2D7339155A93E1CF8F507FC367F41373CB94629544105A	13
Private key (hey)	D01E751E8499D68B8EC1862401C573CEED9CEF96E72741AD15489A2A0BC688A4	
i indie key (iiek)		

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").









Data file, network request or set key can be manually selected if you are the computer.	ying to decrypt fil	es on different
rying to load data from windows registry SROR - Registry entry not found or incorrect.	^	Load data filo
rving to load data file from disk		
ROR - Data file not found.		Decode reques
** You can load data file manually by clicking on Load data file button. *** ** You can decode Tesla's request by clicking on Decode request button *** ** You can set decryption key by clicking on Set key button ***		Set key
		Save data file
		Decrypt Folder
		Decrypt All
		Close

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.

Set cust	om key for decryption
You can s	et custom key for the decryption here. The key must be in hexadecimal format and bigger than 0.
The key ca - Tesla's p - PrivateKe - PrivateKe - PrivateKe TeslaDeco	n be one of the following keys used by TeslaCrypt: rivate key (Experimental) yBC (Private key used for calculation of ransom bitcoin address) ySHA256BC (SHA256 of the key above - the criminals send this key after payment) yFile (This key is directly used for AES encryption/decryption) der will automatically check the key and compute related keys if necessary.
Key (hex):	D01E751E8499D68B8EC1862401C573CEED9CEF96E72741AD15489A2A0BC688A4
Extension:	.xyz, .zzz, .aaa, .abc, .ccc, .wv
	Set key Cancel









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-f iles-encrypted-by-teslacrypt/

Información adicional:

http://www.bleepingcomputer.com/news/security/teslacrypt-decrypted-flaw-in-teslacrypt-allows-vict ims-to-recover-their-files/ https://github.com/Googulator/TeslaCrack http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information#ra nsom 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-f iles-encrypted-by-teslacrypt/

