

SIN CLASIFICAR



Informe Código Dañino CCN-CERT ID-07/16

Ransom.TeslaCrypt

Mayo de 2016

SIN CLASIFICAR

**LIMITACIÓN DE RESPONSABILIDAD**

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. SOBRE CCN-CERT	5
2. RESUMEN EJECUTIVO	6
3. INFORMACIÓN DE VERSIONES DEL CÓDIGO DAÑINO	6
3.1 VERSIONES DEL CÓDIGO DAÑINO	6
3.1.1 PRIMERA VERSIÓN.....	6
3.1.2 SEGUNDA VERSIÓN	7
3.1.3 TERCERA VERSIÓN - ALPHACRYPT	7
3.1.4 CUARTA VERSIÓN.....	7
3.1.5 QUINTA VERSIÓN	8
3.1.6 SEXTA VERSIÓN	8
3.1.7 SÉPTIMA VERSIÓN.....	9
3.1.8 OCTAVA VERSIÓN	9
3.1.9 NOVENA VERSIÓN	9
3.1.10 DÉCIMA VERSIÓN.....	9
3.1.11 UNDÉCIMA VERSIÓN	10
3.1.12 DUODÉCIMA VERSIÓN	10
3.1.13 DECIMOTERCERA VERSIÓN	10
3.1.14 DECIMOCUARTA VERSIÓN	11
3.1.15 DECIMOQUINTA VERSIÓN – TESLACRYPT 4.0	11
3.2 EXTENSIONES CIFRADAS.....	11
3.3 EXTENSIÓN AÑADIDA A LOS ARCHIVOS CIFRADOS	12
3.4 DESCIFRADO	13
3.5 ARCHIVOS DE RESCATE	13
4. CARACTERÍSTICAS DEL CÓDIGO DAÑINO	15
5. DETALLES GENERALES	15
6. PROCEDIMIENTO DE INFECCIÓN.....	16
7. CARACTERÍSTICAS TÉCNICAS	16
8. CIFRADO Y OFUSCACION	22
9. PERSISTENCIA EN EL SISTEMA	23
10. CONEXIONES DE RED	24
10.1 USER-AGENT	25
11. ARCHIVOS RELACIONADOS	25

12.DETECCIÓN	26
12.1 UTILIDAD DEL SISTEMA	26
12.2 MANDIANT	27
13.DESINFECCIÓN.....	27
14.DESCIFRADO	28
14.1 TESLADECODER	28
14.2 ESET TESLACRYPT DECRYPTOR	29
15.INFORMACIÓN DEL ATACANTE	31
15.1 RESIDENCIALMONTEBELLO.COM	31
15.1.1 DIRECCIÓN IP	31
15.1.2 GEOLOCALIZACIÓN.....	32
15.2 SANTESERENITESUCCES.COM	33
15.2.1 DIRECCIÓN IP	33
15.2.2 GEOLOCALIZACIÓN.....	34
15.3 YALCINGULTEN.COM	34
15.3.1 DIRECCIÓN IP	34
15.3.2 GEOLOCALIZACIÓN.....	35
15.4 CALIFORNIADAR.ORG	36
15.4.1 DIRECCIÓN IP	36
15.4.2 GEOLOCALIZACIÓN.....	37
15.5 SHREEVISWAKARMAENGWORKS.COM.....	38
15.5.1 DIRECCIÓN IP	38
15.5.2 GEOLOCALIZACIÓN.....	38
16.REFERENCIAS	39
17.ANEXOS	40
ANEXO I: INDICADOR DE COMPROMISO – IOC	40
ANEXO II: YARA.....	41

1. SOBRE CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. RESUMEN EJECUTIVO

El presente documento recoge el análisis del código dañino "**Ransom.TeslaCrypt**", el cual ha sido diseñado para instalarse en el sistema, comunicarse con un dominio de Internet, cifrar ciertos archivos y extorsionar a la víctima mostrando una notificación sobre el procedimiento de pago para rescatar los archivos cifrados.

Existen 3 versiones distintas del código dañino. Entre dichas versiones de la familia se observan diferencias en los siguientes aspectos:

- Las extensiones a cifrar.
- La extensión añadida en los archivos cifrados.
- Si guarda la clave usada para cifrar en el sistema comprometido
- El algoritmo de cifrado utilizado para proteger la clave de cifrado.
- La forma de presentación del rescate de los archivos.

Los objetivos de este código dañino son todo tipo de usuarios y empresas en cualquier parte del mundo.

A mediados de mayo del 2016 los desarrolladores del código dañino hicieron pública la clave maestra usada para la generación de claves privadas de las últimas versiones de la familia Teslacrypt. Ésto permitió que la compañía de seguridad ESET publicara una herramienta que descifra los archivos secuestrados.

< > wbozgkln06x2vfrk.onion/

Project closed
master key for decrypt 440A241DD80FCC5664E861989DB716E08CE627D8D40C7EA360AE855C727A49EE
[BloodDolly Decryption software](#)
we are sorry!

Ilustración 1 Publicación de la clave maestra

3. INFORMACIÓN DE VERSIONES DEL CÓDIGO DAÑINO

El código dañino presenta diferencias entre sus versiones. En este apartado se muestran las diferencias y los cambios producidos entre ellas.

3.1 VERSIONES DEL CÓDIGO DAÑINO

Existen 15 versiones distintas del código dañino. En este apartado se indican los puntos que las distinguen entre sí. Se tiene que tener en cuenta que las versiones se han agrupadas en 3 versiones principales.

Las primeras 4 versiones engloban la primera versión principal; las versiones desde la 5 a la 8 engloban la segunda versión principal (2.x.x); y las versiones 9 a la 15 engloban la tercera versión principal (3.x.x).

3.1.1 PRIMERA VERSIÓN

- Cifra con la extensión .ecc
- Ubicación de la clave de cifrado "%AppData%\key.dat".

- No usa el registro para almacenar la clave.
- Se puede descifrar usando la herramienta TeslaDecoder.
- Se puede obtener la clave de cifrado si se captura el paquete que la envía al servidor C2.
- Si la clave de descifrado fue borrada parcialmente se puede descifrar igualmente con la herramienta TeslaDecoder. Si la clave fue borrada de forma completa no se puede descifrar.
- El código dañino se descubre a finales de febrero de 2015.

3.1.2 SEGUNDA VERSIÓN

- Cifra con la extensión .ecc
- Ubicación de la clave de cifrado "%AppData%\key.dat".
- No usa el registro para almacenar la clave.
- Se puede descifrar con la herramienta TeslaDecoder.
- Se puede obtener la clave de cifrado del paquete enviado con ella al servidor C2 en el caso de que dicho paquete pueda ser capturado.
- La diferencia con respecto a la primera versión es el tamaño del key.dat, en esta versión es de 656 bytes.

3.1.3 TERCERA VERSIÓN - ALPHACRYPT

- Su fecha de descubrimiento data de finales de abril de 2015.
- Cifra con la extensión .ezz
- Sólo admite pagos mediante BitCoins.
- Ubicación de la clave de cifrado "%AppData%\key.dat".
- Establece el fondo del escritorio con el archivo de rescate creado en el escritorio "%Desktop%\HELP_TO_SAVE_FILES.bmp".
- Se puede descifrar con la herramienta TeslaDecoder.
- Se mantiene una lista de los archivos cifrados en el sistema comprometido en el archivo "%AppData%\Log.html".

3.1.4 CUARTA VERSIÓN

- Cifra con las extensiones .ecc y .ezz
- Vuelve a usar el nombre TeslaCrypt.
- Se usa el registro para almacenar información: "HKCU\Software\Microsoft\Windows\CurrentVersion\SET".
- Ubicación de la clave de cifrado "%AppData%\key.dat".

- La información de la clave ocupa 752 bytes tanto en disco como en el registro.
- Se puede descifrar con la herramienta TeslaDecoder.
- Se puede obtener la clave de cifrado del paquete enviado con ella al servidor C2 en el caso de que dicho paquete pueda ser capturado.
- Si la información de la clave fue borrada no es posible recuperar la información con TeslaDecoder. En caso contrario, sí se puede.
- Su primera aparición data de mayo de 2015.

3.1.5 QUINTA VERSIÓN

- Cifra con las extensiones .exx y .ezz
- Se usa el registro para almacenar información: "HKCU\Software\Microsoft\Windows\CurrentVersion\Settings\storage".
- Ubicación de la clave de cifrado "%LocalAppData%\storage.bin".
- La información de la clave ocupa 752 bytes tanto en disco como en el registro.
- El archivo de la clave y la información de ella en el registro está cifrado con AES 256.
- Se puede descifrar con la herramienta TeslaDecoder.
- Se puede obtener la clave de cifrado del paquete enviado con ella al servidor C2 en el caso de que dicho paquete pueda ser capturado.
- Si la información de la clave fue borrada no es posible recuperar la información con TeslaDecoder. En caso contrario, si se puede.
- Los archivos cifrados con extensión .exx llevan incluida la información del archivo de la clave.
- Su primera aparición data de julio de 2015.

3.1.6 SEXTA VERSIÓN

- Cifra con las extensiones .xyz, .zzz, .aaa, .abc, .ccc
- Se usa el registro para almacenar información: "HKCU\Software\%random%".
- Se puede descifrar con la herramienta TeslaDecoder.
- Se puede obtener la clave de cifrado del paquete enviado con ella al servidor C2 en el caso de que dicho paquete pueda ser capturado.
- La única forma de descifrar los archivos es capturando la clave en el momento que se envía al servidor C2. A partir de la versión 2.1.0 del código dañino esto ya no es posible.
- Su primera aparición data de agosto de 2015.

3.1.7 SÉPTIMA VERSIÓN

- No altera el nombre del archivo.
- Se puede obtener la clave de cifrado del paquete enviado con ella al servidor C2 en el caso de que dicho paquete pueda ser capturado.
- La única forma de descifrar los archivos es capturando la clave en el momento que se envía al servidor C2.
- Excepto capturando la clave, tal y como es indicado en el punto anterior, no es posible descifrar los archivos cifrados por esta versión.
- Su primera aparición data de finales de agosto de 2015.

3.1.8 OCTAVA VERSIÓN

- Cifra con la extensión .ccc
- Se pueden descifrar los archivos si se captura la clave cuando se utiliza en el proceso de cifrado, y a su vez hibernando o suspendiendo el sistema comprometido.
- Excepto capturando la clave, tal y como es indicado en el punto anterior, no es posible descifrar los archivos cifrados por esta versión.
- Su primera aparición data de septiembre de 2015.

3.1.9 NOVENA VERSIÓN

- Cifra con la extensión .vvv
- Se pueden descifrar los archivos si se captura la clave cuando se utiliza en el proceso de cifrado, y a su vez hibernando o suspendiendo el sistema comprometido.
- Usa el cifrado RSA-4096.
- Excepto capturando la clave, tal y como es indicado en el punto anterior, no es posible descifrar los archivos cifrados por esta versión.
- Su primera aparición data de octubre de 2015.

3.1.10 DÉCIMA VERSIÓN

- Cifra con la extensión .vvv
- Se pueden descifrar los archivos si se captura la clave cuando se utiliza en el proceso de cifrado, y a su vez hibernando o suspendiendo el sistema comprometido.
- Excepto capturando la clave, tal y como es indicado en el punto anterior, no es posible descifrar los archivos cifrados por esta versión.
- Usa el cifrado RSA-4096

- Con dicha clave obtenida se puede descifrar con la herramienta "TeslaDecoder".
- Su primera aparición data de noviembre de 2015.

3.1.11 UNDÉCIMA VERSIÓN

- Cifra con la extensión .ttt
- Se pueden descifrar los archivos si se captura la clave cuando se utiliza en el proceso de cifrado, y a su vez hibernando o suspendiendo el sistema comprometido.
- Excepto capturando la clave, tal y como es indicado en el punto anterior, no es posible descifrar los archivos cifrados por esta versión.
- Su primera aparición data de diciembre de 2015.
- A mediados de mayo del 2016 los desarrolladores del código dañino hicieron pública la clave maestra usada para la generación de claves privadas, permitiendo la publicación de una herramienta que descifra los archivos secuestrados.

3.1.12 DUODÉCIMA VERSIÓN

- Cifra con la extensión .xxx
- Se pueden descifrar los archivos si se captura la clave cuando se utiliza en el proceso de cifrado, y a su vez hibernando o suspendiendo el sistema comprometido.
- Excepto capturando la clave, tal y como es indicado en el punto anterior, no es posible descifrar los archivos cifrados por esta versión.
- Su primera aparición data de enero de 2016.
- A mediados de mayo del 2016 los desarrolladores del código dañino hicieron pública la clave maestra usada para la generación de claves privadas, permitiendo la publicación de una herramienta que descifra los archivos secuestrados.

3.1.13 DECIMOTERCERA VERSIÓN

- Cifra con la extensión .micro
- Se pueden descifrar los archivos si se captura la clave cuando se utiliza en el proceso de cifrado, y a su vez hibernando o suspendiendo el sistema comprometido.
- Excepto capturando la clave, tal y como es indicado en el punto anterior, no es posible descifrar los archivos cifrados por esta versión.
- Su primera aparición data de enero de 2016.

- A mediados de mayo del 2016 los desarrolladores del código dañino hicieron pública la clave maestra usada para la generación de claves privadas, permitiendo la publicación de una herramienta que descifra los archivos secuestrados.

3.1.14 DECIMOCUARTA VERSIÓN

- Cifra con la extensión .MP3
- Se pueden descifrar los archivos si se captura la clave cuando se utiliza en el proceso de cifrado, y a su vez hibernando o suspendiendo el sistema comprometido.
- Excepto capturando la clave, tal y como es indicado en el punto anterior, no es posible descifrar los archivos cifrados por esta versión.
- Su primera aparición data de febrero de 2016.
- A mediados de mayo del 2016 los desarrolladores del código dañino hicieron pública la clave maestra usada para la generación de claves privadas, permitiendo la publicación de una herramienta que descifra los archivos secuestrados.

3.1.15 DECIMOQUINTA VERSIÓN – TESLACRYPT 4.0

- No cambia la extensión de los archivos cifrados.
- Su primera aparición data de mediados de marzo de 2016.
- No utiliza el comando "vssadmin" para eliminar los Shadow Volumes, en su lugar usa el comando "wmic".
- No envía las claves al servidor C2 de forma que puedan ser capturadas. En su lugar usa el algoritmo ECDH junto con AES para cifrar su propia clave de cifrado.
- A mediados de mayo del 2016 los desarrolladores del código dañino hicieron pública la clave maestra usada para la generación de claves privadas, permitiendo la publicación de una herramienta que descifra los archivos secuestrados.

3.2 EXTENSIONES CIFRADAS

El código dañino cifra todos los archivos con ciertas extensiones en su nombre. A continuación se muestran las extensiones que cifran las dos primeras versiones:

```
.7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .sc2save, .sie, .sum, .ibank, .t13, .t12, .qdf,
.gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvp1,
.hplg, .hkdb, .mdbbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mcgame,
.vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .001, .vtf, .dazip, .fpk, .mlx,
.kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2,
.mcmeta, .vfs0, .mpqge, .kdb, .db0, .DayZProfile, .rofl, .hkx, .bar, .upk, .das, .iwi,
```

.litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, .unity3d, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbfv, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt

A partir de AlphaCrypt, éstas son las extensiones de archivos que se cifran:

.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13, .t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs, .hvpl, .hplg, .hkdb, .mdbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip, .fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc, .lrf, .m2, .mcmeta, .vfs0, .mpqge, .kdb, .db0, .dba, .rofl, .hkx, .bar, .upk, .das, .iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big, .wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb, .odc, .odm, .odp, .ods, .odt

3.3 EXTENSIÓN AÑADIDA A LOS ARCHIVOS CIFRADOS

En las cuatro primeras versiones (versión 0.4.1 e inferiores) a los archivos cifrados se les cambia la extensión original por alguna de las siguientes:

.ecc, .ezz, .exx

Desde la quinta a la octava versión (versión 2.2.0 e inferiores) las extensiones por las que se cambian las originales son:

.xyz, .zzz, .aaa, .abc, .ccc, .vvv

Desde la novena hasta la decimocuarta versión (versión 3.0.0 y 3.0.0.x) el código dañino añade a la extensión original del archivo alguna de las siguientes:

.micro, .ttt, .xxx, .MP3

En la última versión (Teslacrypt 4.0 o versión 3.0.1 interna) no se cambia la extensión de los archivos cifrados.

3.4 DESCIFRADO

Los archivos cifrados por las cuatro primeras versiones del código dañino se pueden descifrar usando la herramienta “TeslaDecoder”¹. En el resto de versiones, salvo la última, se puede utilizar la misma herramienta, pero hace falta obtener la clave previamente.

Para la última versión, Teslacrypt 4.0 o 3.0.1 interna, no existe herramienta para descifrar los archivos.

3.5 ARCHIVOS DE RESCATE

El código dañado crea los siguientes archivos en todas las carpetas en las que haya podido cifrar algún archivo:

```
help_recover_instructions+<cadena_aleatoria_de_tres_carácteres>.txt
```

```
help recover instructions+<cadena aleatoria de los mismos tres caracteres>.html
```

Además, en el escritorio del sistema comprometido crea los mismos archivos citados anteriormente junto con otros dos más:

%DESKTOP%\help_recover_instructions.BMP

%DESKTOP%\help_recover_instructions.HTM

Todos los archivos llevan la misma información indicando los pasos a seguir para poder recuperar los archivos cifrados:

NOT YOUR LANGUAGE? USE <https://translate.google.com>

What happened to your files ?

All of your files were protected by a strong encryption with RSA-4096.

More information about the encryption keys using RSA-4096 can be found here:
[http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

How did this happen ?

!!! Specially for your PC was generated personal RSA-4096 KEY, both public and private.

!!! ALL YOUR FILES were encrypted with the public key, which has been transferred to your computer via the Internet.

Decrypting of your files is only possible with the help of the private key and decrypt program, which is on our secret server.

¹ <http://download.bleepingcomputer.com/BloodDolly/TeslaDecoder.zip>

What do I do ?

So, there are two ways you can choose: wait for a miracle and get your price doubled, or start obtaining BTC NOW, and restore your data easy way.

If You have really valuable data, you better not waste your time, because there is no other way to get your files, except make a payment.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. http://kjsdfuo9ndskj4.flueymari.com/<id_unico>
2. http://p5vnwj4nfszlk.chamablunk.com/<id_unico>
3. http://g4nsjn45nldflef.polypdicot.com/<id_unico>

If for some reasons the addresses are not available, follow these steps:

1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: wbozgkln06x2vfrk.onion/<id_unico>
4. Follow the instructions on the site.

!!! IMPORTANT INFORMATION:

!!! Your personal pages:

http://kjsdfuo9ndskj4.flueymari.com/<id_unico>

http://p5vnwj4nfszlk.chamablunk.com/<id_unico>

http://g4nsjn45nldflef.polypdicot.com/<id_unico>

!!! Your personal page in TOR Browser: [wbozgkln06x2vfrk.onion/ <id_unico>](http://wbozgkln06x2vfrk.onion/<id_unico>)

!!! Your personal identification ID: <id_unico>

El identificador único, <id_unico>, es el valor generado por el código dañino al comenzar su ejecución. Este identificador será utilizado para acceder a la web de descifrado indicada en el mensaje del secuestro y para que los autores del código dañino sepan a qué sistema corresponde la petición.

4. CARACTERÍSTICAS DEL CÓDIGO DAÑINO

El código dañino examinado posee las siguientes características:

- Conecta con un C2 preestablecido en su código.
- Si su infección viene por una descarga desde Internet, intenta evitar mensajes de alerta al usuario.
- El código dañino se encuentra empaquetado.
- Crea una entrada en el registro de Windows para asegurar su persistencia.
- Crea múltiples hilos para ralentizar el proceso de análisis.
- Elimina todas las imágenes de recuperación de "Shadow Volumes" del sistema.
- Cifra archivos en todas las unidades conectadas al equipo.
- Muestra información acerca del cifrado y como recuperar los archivos.
- Crea un hilo con el que finaliza determinadas aplicaciones en ejecución en el sistema comprometido.

5. DETALLES GENERALES

Las muestras analizadas se corresponden con las siguientes firmas MD5:

```
eb4c18d2df9bb127ae0f51b2f2136938
578b49c2a7e1540a318afd90e93f1007
8cb4f8d9b8a36a06036888c9c37968c0
```

Todos tienen formato PE (*Portable Executable*), es decir, son ejecutables para sistemas operativos Windows, concretamente para 32 bits, que van desde Windows XP hasta Windows 10. Aunque son binarios para plataforma de 32 bits, también funcionan en sistemas operativos de 64 bits.

En las muestras analizadas se puede observar que las fechas internas de creación son muy modernas como, en este caso, del 23 de enero del 2016.

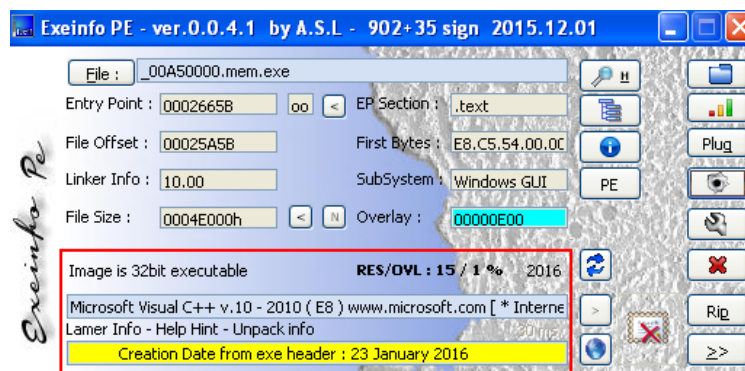


Ilustración 2 Detalles del binario Diferencias en el compilador y en la fecha

6. PROCEDIMIENTO DE INFECCIÓN

La infección en el equipo se produce al ejecutar el fichero que contiene el código dañino. Una vez ejecutado realiza las siguientes acciones en el equipo de la víctima:

- Se copia a sí mismo en el sistema.
- Elimina los puntos de restauración de los "Shadow Volumes" que puedan existir en el sistema comprometido.
- Modifica el registro de Windows para iniciarse de forma automática en el arranque del sistema.
- Enumera todos los archivos y carpetas del sistema en busca los que tengan algunas extensiones determinadas para cifrarlos.
- En la ejecución inicial, antes de finalizarse, procede a ejecutar un comando mediante el interprete de comandos del sistema para borrar al código dañino.
- En las versiones iniciales del código dañino almacena la clave de cifrado en un archivo en el disco duro del sistema comprometido.
- En las penúltimas versiones del código dañino, crea una conexión a un servidor remoto y envía información de la clave generada para cifrar los archivos en el sistema comprometido.
- En las últimas versiones del código dañino no envía ni recibe del C2 ninguna clave "crítica" para el proceso de generación de claves, ni de cifrado. Con "crítica" se entiende la posibilidad de poder capturar información que permitiera automatizar el descifrado de archivos sin necesidad de pagar el rescate de los archivos.

7. CARACTERÍSTICAS TÉCNICAS

El código dañino se encuentra empaquetado por algoritmos propios que incorpora diversas técnicas antidepuración para dificultar su análisis.

Cuando se inicia el código dañino se descifra en memoria y comienza su funcionalidad obteniendo las rutas del sistema comprometido al igual que las direcciones de memoria de las funciones "Wow64DisableWow64FsRedirection" y "Wow64RevertWow64FsRedirection".

Dichas funciones permiten deshabilitar y habilitar la redirección existente en plataformas de 64 bits para que las aplicaciones de 32 bits sean redirigidas al directorio nativo donde están sus librerías, "%WINDIR%\SysWOW64", y no al que intentan acceder de forma natural, "%WINDIR%\System32", que contiene las librerías de 64 bits². En plataformas de 32 bits estas funciones no existen.

² <https://msdn.microsoft.com/es-es/library/windows/desktop/aa365743>

Por defecto la redirección en el sistema de archivos está habilitada y el código dañino intentará deshabilitar dicha redirección para realizar una serie de operaciones, como se puede ver posteriormente en este mismo informe, para después volver a rehabilitarla.

Lo siguiente que realiza es borrar el ADS, *Alternate Data Stream*, del código dañino con el nombre `%s:Zone.Identifier`:

```

push    offset FileName ; Dst
call    _wcscpy_s
add     esp, 0Ch
push    offset aZone_identifie ; ":Zone.Identifier"
push    1000h           ; SizeInWords
push    offset FileName ; Dst
call    _wscat_s
add     esp, 0Ch
push    offset FileName ; lpFileName
call    ds:DeleteFileW

```

Ilustración 3. Detección del ADS "`%s:Zone.Identifier`" y su posterior eliminación

Cuando un binario es descargado de Internet con un navegador como Internet Explorer, éste añade ese ADS de forma automática a los ficheros con la zona desde la que fueron descargados para poder identificarlos y lanzar un aviso de seguridad previo a su ejecución. En el caso de que exista el ADS, el código dañino procederá a realizar el borrado de dicho ADS para evitar el aviso.

Posteriormente obtiene el "Token" del usuario activo y lo compara con valores preestablecidos para detectar si la cuenta de usuario activa es Administradora o incluso con permisos superiores. En el caso de que así sea, procederá a darse el permiso "SeDebugPrivilege". Dicho permiso permite realizar acciones de depuración como acceder a otros procesos que, de base, no se tendría permiso.

Tras esta acción, el código dañino se copia en la ruta `%APPDATA%` del sistema comprometido con un nombre formado por letras y números aleatorios junto con la cadena fija "he45.exe" aunque ésta depende de la muestra.

Tras realizar la copia comprobará si está en la ruta `%APPDATA%`, en el caso de que no sea así procederá a ejecutarse a sí mismo desde la ruta `%APPDATA%` y finalizar su ejecución borrándose mediante una llamada al interprete de comandos del sistema comprometido.

Posteriormente el código dañino intentará crear un *Mutex* con el nombre:

```
__sys_234238233295
```

Este nombre puede cambiar entre versiones del código dañino. En el caso de que el *Mutex* exista en el sistema el código dañino finaliza su ejecución.

En el caso de que el *Mutex* pueda ser creado con éxito, el código dañino procede a modificar entradas en el registro para asegurar su persistencia en el equipo comprometido.

Tras ello, el código dañino creará diversos hilos para realizar distintas tareas, como son, el cifrado de archivos, la eliminación de puntos de restauración de

"Shadow Volumes", la comunicación con su servidor C2 y la creación de un hilo para finalizar la ejecución de determinados programas activos en el sistema

El hilo anterior, que finaliza la ejecución de ciertos programas, se ejecuta con un intervalo de 200 milisegundos por interacción. Dicho hilo enumera todos los procesos del sistema buscando determinados patrones en el nombre de los procesos. En el caso de que se encuentre alguno de los patrones en sus nombres, dicho proceso es terminado automáticamente.

Las cadenas buscadas son:

- "askmg": Gestor de tareas, taskmgr.exe.
- "rocex": process explorer, processxp.exe.
- "egedit": Editor del Registro, regedit.exe.
- "sconfi": Configuración del sistema, msconfig.exe.
- "cmd": Interpretador de comandos, cmd.exe

Por supuesto, no solo los procesos indicados con la cadena son los finalizados sino que cualquiera que posea una de esas cadenas en su nombre será finalizado también como, por ejemplo, "cmdcalc.exe".

El hilo de la eliminación de los "Shadow Volumes" ejecuta la aplicación Vssadmin³ para poder efectuar su borrado.

push	0	
push	edx	
call	0042C850	
push	0043B570	ASCII " delete "
lea	eax, [ebp-208]	
push	104	
push	eax	
call	00425A88	
push	0043B57C	ASCII " shadows "
lea	ecx, [ebp-208]	
push	104	
push	ecx	
call	00425A88	
add	esp, 48	
push	0043B588	ASCII " /all "
lea	edx, [ebp-208]	
push	104	
push	edx	
call	00425A88	
push	0043B590	ASCII " /Quiet "

Ilustración 4. Borrado de los "Shadow Volumes"

La última versión del código dañino, Teslacrypt 4.0 o versión 3.0.1 interna, no usa el comando "vssadmin" para realizar el borrado de los Shadow Volumes y en su lugar utiliza el comando "wmic".

El hilo de la búsqueda de archivos procede a enumerar todas las unidades de disco duro y extraíbles. En cada una de ellas busca recursivamente archivos que posean alguna de las siguientes extensiones.

Primeras versiones del código dañino:

³ [https://technet.microsoft.com/es-es/library/cc754968\(v=ws.10\).aspx](https://technet.microsoft.com/es-es/library/cc754968(v=ws.10).aspx)

```
7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .sc2save, .sie, .sum, .ibank, .t13, .t12,
.qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb, .icxs,
.hvpl, .hplg, .hkdb, .mdbbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb, .fos,
.mcgame, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .001, .vtf, .dazip,
.fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc,
.lrf, .m2, .mcmeta, .vfs0, .mpage, .kdb, .db0, .DayZProfile, .rofl, .hxx, .bar, .upk, .das,
.iwi, .litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak,
.big, .unity3d, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c,
.p7b, .p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf,
.nrw, .mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg,
.cdr, .indd, .ai, .eps, .pdf, .pdd, .psd, .dbfv, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst,
.accdb, .mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc,
.odb, .odc, .odm, .odp, .ods, .odt
```

AlphaCrypt y posteriores versiones a ella:

```
.sql, .mp4, .7z, .rar, .m4a, .wma, .avi, .wmv, .csv, .d3dbsp, .zip, .sie, .sum, .ibank, .t13,
.t12, .qdf, .gdb, .tax, .pkpass, .bc6, .bc7, .bkp, .qic, .bkf, .sidn, .sidd, .mddata, .itl, .itdb,
.icxs, .hvpl, .hplg, .hkdb, .mdbbackup, .syncdb, .gho, .cas, .svg, .map, .wmo, .itm, .sb,
.fos, .mov, .vdf, .ztmp, .sis, .sid, .ncf, .menu, .layout, .dmp, .blob, .esm, .vcf, .vtf, .dazip,
.fpk, .mlx, .kf, .iwd, .vpk, .tor, .psk, .rim, .w3x, .fsh, .ntl, .arch00, .lvl, .snx, .cfr, .ff, .vpp_pc,
.lrf, .m2, .mcmeta, .vfs0, .mpage, .kdb, .db0, .dba, .rofl, .hxx, .bar, .upk, .das, .iwi,
.litemod, .asset, .forge, .ltx, .bsa, .apk, .re4, .sav, .lbf, .slm, .bik, .epk, .rgss3a, .pak, .big,
.wallet, .wotreplay, .xxx, .desc, .py, .m3u, .flv, .js, .css, .rb, .png, .jpeg, .txt, .p7c, .p7b,
.p12, .pfx, .pem, .crt, .cer, .der, .x3f, .srw, .pef, .ptx, .r3d, .rw2, .rwl, .raw, .raf, .orf, .nrw,
.mrwref, .mef, .erf, .kdc, .dcr, .cr2, .crw, .bay, .sr2, .srf, .arw, .3fr, .dng, .jpe, .jpg, .cdr,
.indd, .ai, .eps, .pdf, .pdd, .psd, .dbf, .mdf, .wb2, .rtf, .wpd, .dxg, .xf, .dwg, .pst, .accdb,
.mdb, .pptm, .pptx, .ppt, .xlk, .xlsb, .xlsm, .xlsx, .xls, .wps, .docm, .docx, .doc, .odb,
.odc, .odm, .odp, .ods, .odt
```

En el caso de que se encuentre algún archivo con una extensión de la tabla, se procede a leer el archivo en la memoria, cifrar todo el contenido mediante AES256 y sobrescribir el archivo con la información cifrada.

El código dañino genera una clave maestra para cifrar todos los archivos seleccionados pero, para cada uno de ellos, utiliza un vector de inicialización diferente y aleatorio. La clave maestra, dependiendo de la versión, se puede encontrar en:

- En el archivo "%AppData%\key.dat".
- De forma cifrada en el archivo "%AppData%\key.dat".
- En el registro.
- Enviado al C2.

Cada archivo cifrado se almacena en disco con una cabecera cifrada con RSA, y cuya clave obtienen del C2, que incluye la información necesaria, según versiones, para el descifrado como puede ser el vector de inicialización, la ruta de origen en

El mensaje liberado por el código dañino abierto como HTML muestra la información siguiente:

NOT YOUR LANGUAGE? USE [Google Translate](#)

What happened to your files?
 All of your files were protected by a strong encryption with RSA
 More information about the encryption RSA can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?
 This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
 Especially for you, on our SERVER was generated the secret keypair RSA - public and private.
 All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
 Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program, which is on our Secret Server!!!

What do I do?
 Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
 If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. <http://kjsdfuo9ndskj4.flueymari.com/B43EBDB39A85C1>
2. <http://p5vnwj4nfszlk.chamablunk.com/B43EBDB39A85C1>
3. <http://q4nsjn45nldflef.polypdicot.com/B43EBDB39A85C1>

Ilustración 8. Información mostrada del rescate

A parte de los archivos creados de texto y el HTML las últimas versiones del código dañino proceden a cambiar el fondo de pantalla a un fondo con la información del secuestro de los archivos y los pasos a proceder a pagar el rescate.

8. CIFRADO Y OFUSCACION

El código dañino está empaquetado con algoritmos propios que pueden variar dependiendo de la muestra analizada. En otros casos se pueden encontrar muestras que no poseen ningún cifrado ni ofuscación.

El código dañino cifra todos los archivos que localice con cualquiera de las extensiones indicadas en el apartado de "Extensiones a cifrar" de este informe usando el algoritmo AES256. El algoritmo de cifrado AES, también llamado "Rijndael", es un esquema de cifrado por bloques simétrico de forma que la misma clave que se usa para cifrar, es la que se usa para descifrar.

Las últimas versiones del código dañino utilizan RSA en lugar de AES y, concretamente en las versiones 3.0.a y 3.0.1, se utilizan los algoritmos ECDH y AES para cifrar la clave maestra con la que se cifran los archivos en el sistema.

La última versión, Teslacrypt 4.0 o versión 3.0.1 interna, utiliza un cifrado asimétrico donde la clave pública va incrustada en el propio binario mientras que la clave privada está en manos de los autores de la extorsión. En base a esa clave pública se genera una clave maestra con la que cifrará los archivos en el sistema. Esta información es guardada en el registro de Windows, donde inicialmente comprueba que dicha información no exista para no crear volver a crear ninguna clave maestra.

9. PERSISTENCIA EN EL SISTEMA

El código dañino hace una copia de sí mismo en %APPDATA% con un nombre generado aleatoriamente usando la función "GetTickCount"⁴ y añadiendo un texto fijo, en una de las muestras analizadas es "he45.exe". Este nombre del archivo varía entre versiones y muestras del código dañino.

%APPDATA%\<valor aleatorio>he45.exe

El código dañino, con el fin de asegurarse su ejecución en cada reinicio del equipo, modifica el registro de Windows creando las siguientes entradas:

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

zsevice-34 = <%APPDATA%>\<valor_aleatorio>he45.exe

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]

zsevice-35 = <%APPDATA%>\<valor_aleatorio>he45.exe

Aparte de las dos entradas en el arranque del sistema, el código dañino crea las siguientes entradas:

[HKEY_CURRENT_USER\SOFTWARE\<valor_aleatorio>]

Data = <datos_binarios>

Los datos binarios almacenados son las direcciones de Bitcoin generadas para el sistema comprometido y donde se debe realizar el pago solicitado por el código dañino. Esta información almacenada aquí será usada posteriormente para enviarla al servidor C2 junto con más datos del sistema.

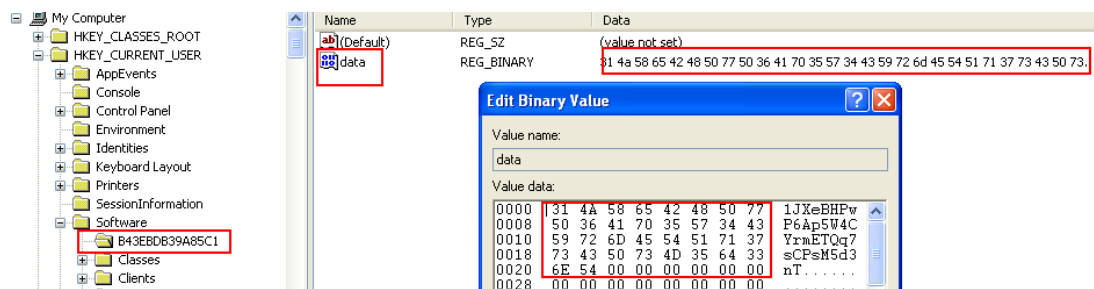


Ilustración 9. Direcciones Bitcoin guardadas en el registro

⁴[https://msdn.microsoft.com/es-es/library/windows/desktop/ms724408\(v=vs.85\).aspx](https://msdn.microsoft.com/es-es/library/windows/desktop/ms724408(v=vs.85).aspx)

10. CONEXIONES DE RED

El código dañino intenta establecer conexión con un dominio enviando la información necesaria para poder generar la clave de descifrado de los archivos del sistema comprometido en algunas versiones del código dañino.

En los análisis realizados se han obtenido los siguientes dominios con los que intentará establecer conexión:

santeserenitesucces.com
yalcingulten.com
deanza.californiadar.org
shreevishwakarmaengworks.com
residencialmontebello.com

El código dañino envía de forma cifrada información del equipo comprometido y del propio código dañino;



Ilustración 10. Envío de datos al dominio residencialmontebello.com

La información sin cifrar que envía el código dañino es la siguiente:

Sub=Ping&key=empty&dh=0494F73C6AA3789B9E3A84DF2812526C22875F84EA4E8E04B81E6D79CB80EF752807AEE6CEF13E6FC7F8F889C1A4C481574FC2341062F5E80F0C9412BB5EC1A014B8993D426BFCF6A569B36EC3F9475E6BAD4D7CEF27F3FE71C19BC2585B2AC4AB&addr=1MdE3QGGuPyLVVvhXdr2ZG8NRtCyz89HsAR&size=0&version=3.0.0a&OS=2600&ID=1433&gate=santeserenitesucces.com&ip=176.10.104.240&inst_id=723041921ABF5CC7

Los campos de la información son varios.

- Sub = Siempre con el texto "Ping".

- key = En antiguas versiones del código dañino en este campo se enviaba la clave maestra usada para cifrar los archivos del sistema. En las últimas versiones lleva el texto "empty". Para más información de las versiones consultar el [punto 3.1](#) del presente informe.
- dh = La EHDC⁵ Secret Key de la clave usada para cifrar y de la dirección bitcoin a la que realizar el pago.
- addr = La dirección bitcoin en la que se tendrá que efectuar el pago del rescate de los archivos.
- size = Con el valor a 0.
- version = La versión del código dañino siguiendo la numeración de los creadores del código dañino.
- OS = La versión del sistema operativo comprometido de forma numérica. Por ejemplo, 2600 para XP.
- ID = Identificador del código dañino.
- gate = Dominio C2 al que va a enviar la información.
- ip = La dirección IP del sistema comprometido.
- inst_id = El identificador de la instalación del código dañino.

10.1 USER-AGENT

El código dañino utiliza un campo *User-Agent* específico:

Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko

11. ARCHIVOS RELACIONADOS

Los archivos relacionados con el código dañino son los siguientes:

%APPDATA%\			
Nombre	Fecha Creación	Tamaño bytes	Hash SHA1
<nombre aleatorio>he45.exe	<varía>	<varía_según_muestra>	<varía_según_muestra>
<%DESKTOP%>			
Nombre	Fecha Creación	Tamaño bytes	Hash SHA1
help_recover_instructi ons.HTM	<varía>	<varía_según_muestra>	<varia_por_archivo>
help_recover_instructi ons.BMP	<varía>	<varía_según_muestra>	<varia_por_archivo>
<todas las rutas que tienen al menos un archivo cifrado>			
help_recover_instructi ons+<variable>.html	<varía>	<varía_según_muestra>	<varia_por_archivo>
help_recover_instructi ons+<variable>.txt	<varía>	<varía_según_muestra>	<varia_por_archivo>

⁵ https://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman (en inglés)

12. DETECCIÓN

Para detectar si un equipo se encuentra o ha estado infectado para cualquiera de sus usuarios, se empleará el editor de registro del sistema, *regedit.exe*. También se podrá emplear alguna de las herramientas de *Mandiant: Mandiant IOC Finder* o el colector generado por *RedLine@* con los indicadores de compromiso generados.

12.1 UTILIDAD DEL SISTEMA

Se iniciará editor del registro de Windows: *Inicio -> Ejecutar -> regedit.exe*. En el caso de que el Editor de Registro se cierre automáticamente, muy posiblemente querrá decir que el código dañino estaría cerrando la aplicación. Para evitar esto se procederá a crear una copia del archivo "regedit.exe" en la misma carpeta donde esté con el nombre "editor.exe", posteriormente se ejecutará.

Dentro de la herramienta se buscará la entrada:

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
zservice-34 = <%APPDATA%>\<valor_aleatorio>he45.exe

Si se encuentra la entrada indicada es una evidencia de la presencia presente o pasada del código dañino en el sistema. Esa entrada apunta al código dañino, por lo que hay que comprobar la ruta para intentar localizar archivos que tengan este formato:

%APPDATA%\<nombre_aleatorio>he45.exe

También se buscará la siguiente entrada en el registro, que asegura la persistencia para todos los usuarios del sistema comprometido pues la anterior sólo aseguraba persistencia para el usuario que instaló el código dañino:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
zservice-35 = <%APPDATA%>\<valor_aleatorio>he45.exe

La presencia de archivos llamados "help_recover_instructions <valor aleatorio de tres caracteres>" y con extensión "TXT" o "HTML" en muchas carpetas del sistema es un claro indicador de la presencia del código dañino en el sistema. También se pueden encontrar archivos llamados "help_recover_instructions" en el escritorio con las extensiones "TXT", "BMP" y "HTML".

Encontrar archivos con alguna de las extensiones indicadas en la tabla inferior indica un posible compromiso del sistema.

.ecc, .ezz, .exx, .xyz, .zzz, .aaa, .abc, .ccc, .xxx, .ttt, .micro y .MP3

En el caso de la extensión "MP3" es conocida por ser un formato de comprensión de audio y la última versión conocida del código dañino, *Teslacrypt 4.0*, añade esa extensión en cada archivo cifrado. Para poder descartar que no sea un "MP3" auténtico, se deberá comprobar que el nombre del archivo no posea dos extensiones, siendo la última la de "MP3": por ejemplo "informe.docx.MP3".

12.2 MANDIANT

Se ha generado un nuevo archivo indicador de compromiso. El nombre del indicador generado es con GUID "b1608a67-a9d2-47f7-baec-986ab42a17eb".

Se utilizará el indicador con alguna de las herramientas de las que dispone Mandiant como "Mandiant Ioc Finder" o para la confección de un recolector de evidencias mediante "Mandiant RedLine".

Se recomienda consultar la guía de seguridad CCN-STIC-423 Indicadores de Compromiso (IOC), donde se recoge qué es un indicador de compromiso, cómo crearlo y cómo identificar equipos comprometidos.

13. DESINFECCIÓN

Con el fin de eliminar el código dañino, hay que iniciar sesión con un usuario *Administrador* o que posea privilegios administrativos.

Se ejecutará el editor del Registro de Windows (*Inicio -> Ejecutar -> regedit.exe*). En el caso de que el Editor de Registro se cierre automáticamente, muy probablemente querrá decir que el código dañino estaría cerrando la aplicación. Para evitar esto se procederá a crear una copia del archivo "regedit.exe" en la misma carpeta donde esté con el nombre "editor.exe", posteriormente se ejecutará y se buscarán las entradas:

[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
zservice-34 = <%APPDATA%>\<valor_aleatorio>he45.exe

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
zservice-35 = <%APPDATA%>\<valor_aleatorio>he45.exe

[HKEY_CURRENT_USER\SOFTWARE\<valor_aleatorio>]
Data = <datos_binarios>

En el caso de que exista alguna de las entradas, deberá ser borrada y se deberá reiniciar el equipo posteriormente. Después del reinicio, se borrará el archivo indicado en la entrada previa del registro de la ruta:

%APPDATA%\<valor_aleatorio>he45.exe

Esta operación se deberá de realizar por cada usuario que exista en el sistema. Al finalizar, se reiniciará de nuevo el equipo y se comprobará que no existe ninguna entrada en el registro del código dañino ni archivo.

14. DESCIFRADO

Existen dos herramientas que permiten recuperar los archivos cifrados según la versión del código dañino. Para las versiones que van desde la primera a la décima, se puede utilizar "TeslaDecoder" mientras el resto de versiones, de la undécima a la decimoquinta, se puede utilizar "ESET Teslacrypt Decryptor".

14.1 TESLADECODER

Tras el borrado del código dañino, siguiendo el procedimiento indicado en el apartado anterior de "Desinfección", se procederá a observar qué extensión tienen los archivos cifrados y si están incluidas en la lista mostrada a continuación. Si así fuera, se procederá a utilizar la herramienta "TeslaDecoder"⁶:

.ecc, .ezz, .exx, .xyz, .zzz, .aaa, .abc, .ccc

Dicha herramienta puede encontrar la clave usada para cifrar los archivos en el disco del propio sistema comprometido. La interfaz del programa es simple:

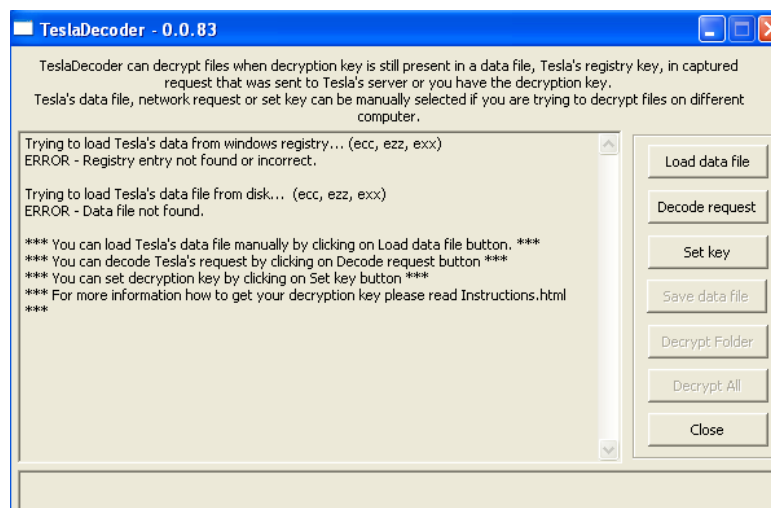


Ilustración 11. Interfaz de la herramienta "TeslaDecoder"

La herramienta detecta automáticamente en un sistema comprometido dónde encontrar la clave almacenada por el código dañino. En el caso de que no pueda encontrarla, o si se están descifrando archivos provenientes de otro sistema comprometido, se puede usar el botón "Load Data File" el cual carga la clave desde el archivo especificado.

Con la opción "Decode Request" se pueden descifrar los archivos utilizando la petición almacenada en el sistema comprometido que se realizó al servidor C2 del código dañino.

⁶ <http://download.bleepingcomputer.com/BloodDolly/TeslaDecoder.zip>

La opción "Set Key" permite indicar a mano una clave que un usuario avanzado haya podido capturar en el sistema comprometido o en la transferencia de datos por la red (en el caso de que sea una de las últimas versiones del código dañino).

El botón de descifrado "Decrypt Folder" permite descifrar todo el contenido de una carpeta especificada. Se recomienda usar esta opción inicialmente y comprobar que los archivos descifrados están intactos, ya que el programa procederá a borrar el archivo cifrado y crear el nuevo descifrado. Cualquier fallo en el proceso o la utilización de una clave errónea producirá que el archivo resultante sea corrupto y se pueda borrar el archivo cifrado. Es por ello que, a parte de utilizar la opción como prueba, es necesario realizar una copia de seguridad de los archivos antes de su descifrado.

La opción "Decrypt All" intenta descifrar todos los archivos cifrados en el sistema comprometido. Esta opción se recomienda una vez se ha comprobado con la opción anterior que una carpeta puede ser descifrada con la clave aportada de forma correcta.

Se deberán borrar todos los archivos llamados "help_recover_instructions_<valor_aleatorio>" con las extensiones "TXT", "HTM", "HTML" o "BMP" que se puedan encontrar en el sistema.

14.2 ESET TESLACRYPT DECRYPTOR

La compañía antivirus ESET desarrolló la herramienta TESLACRYPT DECRYPTOR⁷ para facilitar el descifrado de los archivos utilizando la clave maestra.

La herramienta tiene una serie de parámetros:

- /d : Se ejecuta el programa en modo desarrollo mostrando más información de las acciones realizadas.
- /s : Se ejecuta en modo silencioso, no reportando ninguna información al usuario.
- /f : Las acciones de limpieza se realizan de modo forzado sin importar que se detecte algún tipo de incongruencia en el archivo.
- /n : Sólo lista los archivos cifrados que encuentre sin descifrarlos.

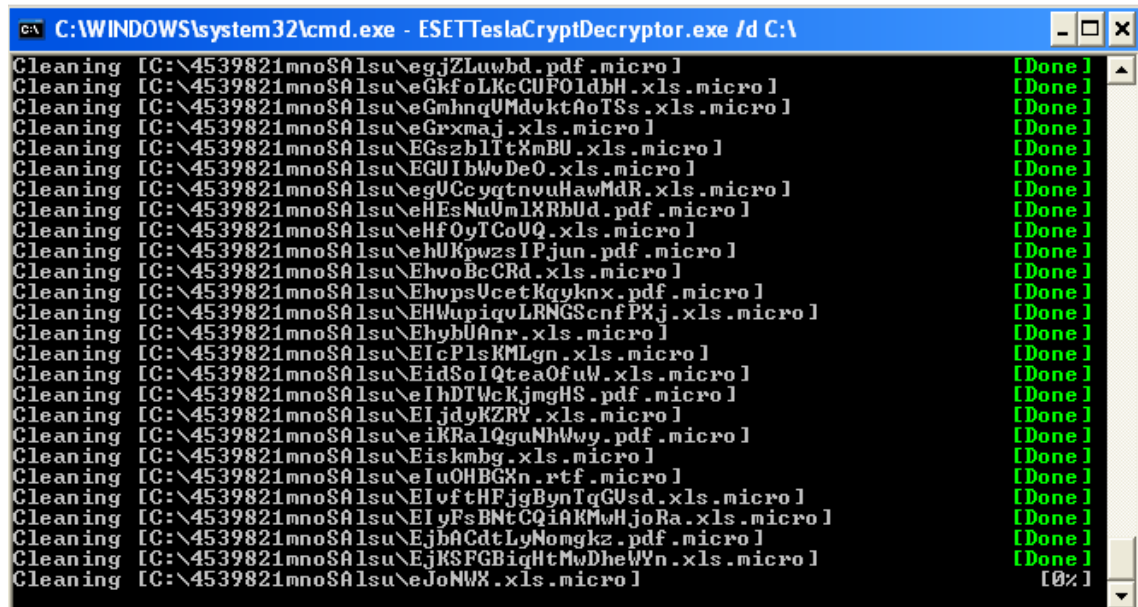
Para proceder al análisis y el descifrado de todos los archivos se lanzará la aplicación con el siguiente comando:

```
<ruta_al_ejecutable_de_ESET>\ESETTeslaCryptDecryptor.exe /d <raiz_del_disco>
```

El programa creará en su mismo directorio un archivo de texto donde guarda toda la información que muestra por pantalla. Dependiendo del tamaño del disco duro a analizar y del número de archivos afectados, el proceso podrá tardar más o menos tiempo.

⁷ <http://download.eset.com/special/ESETTeslaCryptDecryptor.exe>

Por cada archivo que se encuentre cifrado por el código dañino se procede a descifrarlo creando previamente una copia de seguridad del archivo cifrado con el mismo nombre y la extensión "*backup_X_by_eset*". Es por ello que se recomienda tener bastante espacio libre en el disco duro que se vaya a analizar.



```

C:\WINDOWS\system32\cmd.exe - ESETTeslaCryptDecryptor.exe /d C:\
Cleaning [C:\4539821mnoSAlsu\egjZLuwbd.pdf.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\GkfoLKcCUF0ldbH.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\GmhngUMdvtAoTss.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\Grxmaj.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EGszblTtXmBU.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EGUIbWuDeO.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\egUCcygtvnuuHawMdr.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EHesNuUmlXRbUd.pdf.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EHfOytCoUQ.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\ehUKpwzsIPjun.pdf.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EhvoBcCRd.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EhopsUcetKgyknx.pdf.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EHWupigvLRNGScnfPXj.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EhybUAnr.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EicPlsKMLgn.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EidSolQteaOfuW.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\ElhDTWcKjmgHS.pdf.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EIjdyKZRY.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\eiKRAlQguNhWwy.pdf.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\Eiskmbg.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EluOHBGXn.rtf.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EIofthPjgBynTqGUsd.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EIyFsBNtCQiAKMwHjoRa.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EjbACdtLyNongkz.pdf.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\EjKSFGBiqHtMwDheWYn.xls.micro] [Done]
Cleaning [C:\4539821mnoSAlsu\JoNWX.xls.micro] [Done]

```

Ilustración 12. Archivos descifrados usando la herramienta de ESET

Cuando finalice el proceso y se verifique que se han descifrado correctamente los archivos, se recomienda borrar todos los ficheros cifrados de *backup* creados por la herramienta.

Es recomendable, tras eliminar la amenaza del sistema, poner medidas preventivas en los sistemas críticos para evitar que códigos dañinos de tipo "ransomware" puedan volver a comprometer el entorno. Para más información consultar el informe:

<https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1384-ccn-cert-ia-01-16-medidas-de-seguridad-contr-ransomware/file.html>

15. INFORMACIÓN DEL ATACANTE

15.1 RESIDENCIALMONTEBELLO.COM

15.1.1 DIRECCIÓN IP

Según información obtenida en el mes de febrero de 2016, el dominio "residencialmontebello.com" se corresponde con la dirección IP 50.62.123.1.

Registrant Org	DISCEN IS ASSOCIATED WITH ~1 other domains	↗
Registrar	WILD WEST DOMAINS, LLC	
Registrar Status	clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited , clientRenewProhibited https://www.icann.org/epp#clientRenewProhibited , clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited , clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited	
Dates	Created on 2015-01-20 - Expires on 2017-01-20 - Updated on 2016-01-26	↗
Name Server(s)	NS33.DOMAINCONTROL.COM (has 39,975,896 domains) NS34.DOMAINCONTROL.COM (has 39,975,896 domains)	↗
IP Address	50.62.123.1 - 2,059 other sites hosted on this server	↗
IP Location	 - Arizona - Scottsdale - Godaddy.com Llc	
ASN	 AS26496 AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC (registered Oct 01, 2002)	
Domain Status	Registered And Active Website	
Whois History	10 records have been archived since 2015-01-20	↗
IP History	7 changes on 6 unique IP addresses over 12 years	↗
Registrar History	3 registrars with 2 drops	↗

Ilustración 13. Información WHOIS del dominio "residencialmontebello.com"

Comprobando el dominio en VirusTotal se puede observar que 4 motores antivirus reconocen el dominio como dañino.



URL: <http://residencialmontebello.com/dbsys.php>

Detecciones: **4 / 66**

Fecha de análisis: 2016-02-11 12:07:03 UTC (hace 0 minutos)

Análisis: [Ir al análisis del fichero descargado](#)

[Análisis](#)
[Información adicional](#)
[Comentarios](#)
[Votos](#)

Analizador	Resultado
ADMINUSLabs	Malicious site
BitDefender	Malware site
ESET	Malware site
Fortinet	Malware site

Ilustración 14. Análisis del dominio en VirusTotal

15.1.2 GEOLOCALIZACIÓN

Geolocalizando la dirección IP 50.62.123.1 se obtiene la siguiente información:



Ilustración 15. Geolocalización de la dirección IP 50.62.123.1

Dicha dirección IP muestra la siguiente información del dominio a fecha febrero de 2016:

Dirección IP:	50.62.123.1
AS Number (ASN):	AS26496 GoDaddy.com, LLC
Organización:	GoDaddy.com
Dominio:	secureserver.net
DNS:	50.62.123.1
País:	Estados Unidos
Código País:	us
Bandera:	
Nombre Región:	Arizona
País Original:	United States
Ciudad:	Scottsdale
Código ZIP:	85260
Diferencia Horaria:	-07:00
Ips vinculadas:	50.62.123.1
Whois IP - Dominio:	Ver Whois de 50.62.123.1

Ilustración 16. Datos de la dirección IP 50.62.123.1

15.2 SANTESERENITESUCCES.COM

15.2.1 DIRECCIÓN IP

Según información obtenida en el mes de febrero de 2016, el dominio "santeserenitesucces.com" se corresponde con la dirección IP 92.243.26.200.

Email	abuse@support.gandi.net is associated with ~889,106 domains 4abb71b1b2396cf603...@contact.gandi.net 75e766768a82012327...@contact.gandi.net	➔
Registrant Org	FREDERIC DELTOUR is associated with ~3 other domains	➔
Registrar	GANDI SAS	
Registrar Status	clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited	
Dates	Created on 2013-11-27 - Expires on 2016-11-27 - Updated on 2015-09-30	➔
Name Server(s)	A.DNS.GANDI.NET (has 603,794 domains) B.DNS.GANDI.NET (has 603,794 domains) C.DNS.GANDI.NET (has 603,794 domains)	➔
IP Address	92.243.26.200 - 17 other sites hosted on this server	➔
IP Location	 - Ile-de-france - Paris - Gandi Sas	
ASN	 AS29169 GANDI-AS GANDI SAS (registered Jun 20, 2003)	
Domain Status	Registered And Active Website	
Whois History	12 records have been archived since 2013-11-27	➔
IP History	4 changes on 3 unique IP addresses over 3 years	➔
Registrar History	1 registrar	➔

Ilustración 17. Información WHOIS del dominio "santeserenitesucces.com"

El historial de IP del dominio muestra una IP anterior: 217.70.184.38. El cambio de dirección IP se realizó el 31 de marzo del 2014.

Comprobando el dominio en VirusTotal se puede observar que 2 motores antivirus reconocen el dominio como dañino.

URL:

http://santeserenitesucces.com/

Detection ratio:

2 / 67

Analysis date:

2016-02-28 17:20:15 UTC (0 minutes ago)

Analysis

Additional information

Comments

Votes

URL Scanner	Result
BitDefender	Malware site
Fortinet	Malware site

Ilustración 18. Análisis del dominio en VirusTotal

15.2.2 GEOLOCALIZACIÓN

Geolocalizando la dirección IP 92.243.26.200 se obtiene la siguiente información:



IP Address	City	Country Flag	DMA Code
92.243.26.200	n/a		n/a
Provider	State (Code)	Latitude	Area Code
Gandi Dedicated Hosting Servers	n/a ()	48.86	n/a
Hostname	Country	Longitude	Postal Code
xvm-26-200.ghst.net	France	2.35	n/a
Timezone	Continent	TLD	GMT Offset
Europe/Paris	Europe	FR	1

Ilustración 19. Geolocalización de la dirección IP 92.243.26.200

15.3 YALCINGULTEN.COM

15.3.1 DIRECCIÓN IP

Según información obtenida en el mes de febrero de 2016, el dominio "yalcingulten.com" se corresponde con la dirección IP 94.73.146.233.

Email	abuse@nicproxy.com is associated with ~353,351 domains yalcin.gulten@gmail.com	↗
Registrar	NICS TELEKOMUNIKASYON TICARET LTD.STI.	
Registrar Status	ok https://www.icann.org/epp#OK	
Dates	Created on 2015-07-20 - Expires on 2016-07-20 - Updated on 2015-07-21	↗
Name Server(s)	NS1.NATROHOST.COM (has 248,810 domains) NS2.NATROHOST.COM (has 248,810 domains)	↗
IP Address	94.73.146.233 - 461 other sites hosted on this server	↗
IP Location	 - Famagusta - Famagusta - Cizgi Telekomunikasyon Anonim Sirketi	
ASN	 AS34619 CIZGI CIZGI TELEKOMUNIKASYON ANONIM SIRKETI (registered Feb 28, 2005)	
Domain Status	Registered And Active Website	
Whois History	6 records have been archived since 2015-07-20	↗
IP History	3 changes on 3 unique IP addresses over 1 years	↗
Registrar History	1 registrar	↗
Hosting History	1 change on 2 unique name servers over 1 year	↗
Whois Server	whois.nicproxy.com	

Ilustración 20. Información WHOIS del dominio "yalcingulten.com"

El historial de direcciones IP del dominio muestra una IP anterior: 94.73.149.90. El cambio de la dirección IP se produjo a fecha del 4 de agosto del 2015.

Comprobando el dominio en VirusTotal se puede observar que 3 motores antivirus reconocen el dominio como dañino.

URL: <http://yalcingulten.com/>

Detection ratio: **3 / 67**

Analysis date: 2016-02-28 18:17:41 UTC (0 minutes ago)

[Analysis](#)
[Additional information](#)
[Comments](#)
[Votes](#)

URL Scanner	Result
ADMINUSLabs	Malicious site
BitDefender	Malware site
Fortinet	Malware site

Ilustración 21. Análisis del dominio en VirusTotal

15.3.2 GEOLOCALIZACIÓN

Geolocalizando la dirección IP 94.73.146.233 se obtiene la siguiente información:

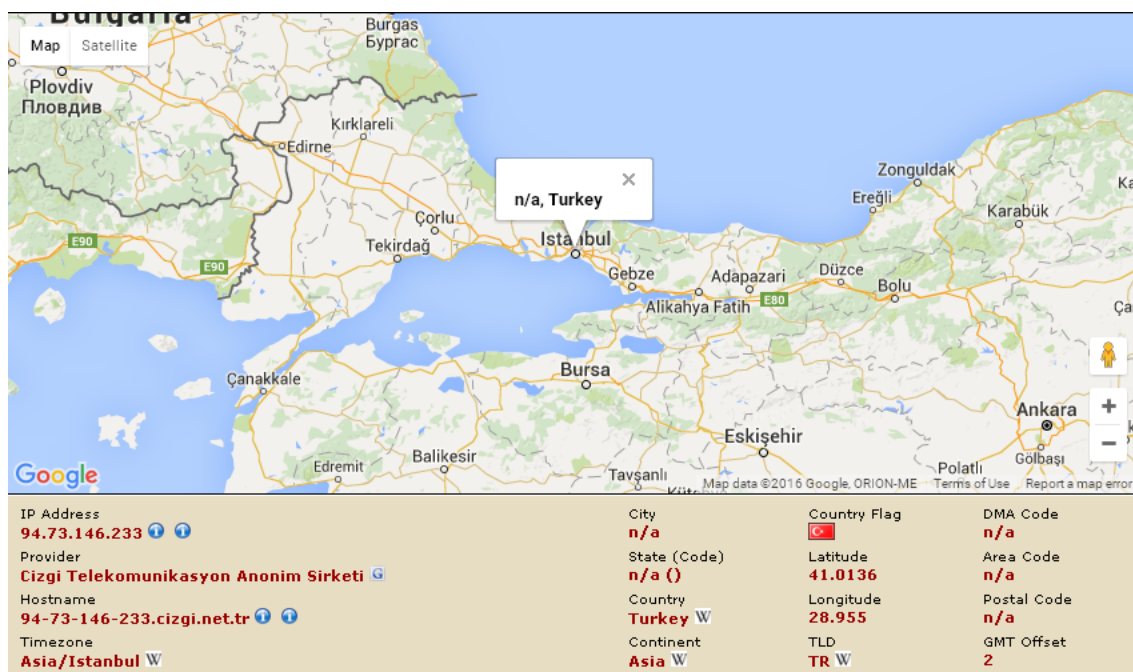


Ilustración 22. Geolocalización de la dirección IP 94.73.146.233

15.4 CALIFORNIADAR.ORG

15.4.1 DIRECCIÓN IP

Según información obtenida en el mes de febrero de 2016, el dominio "californiadar.org" se corresponde con la dirección IP 192.230.67.109. El historial de direcciones IP del dominio muestra las siguientes direcciones IP, desde la más nueva a la más antigua:

198.57.174.56
198.57.129.190
96.125.167.152
209.237.150.20
216.122.158.177

Las fechas de los cambios de IP son las siguientes desde la más actual a la más antigua:

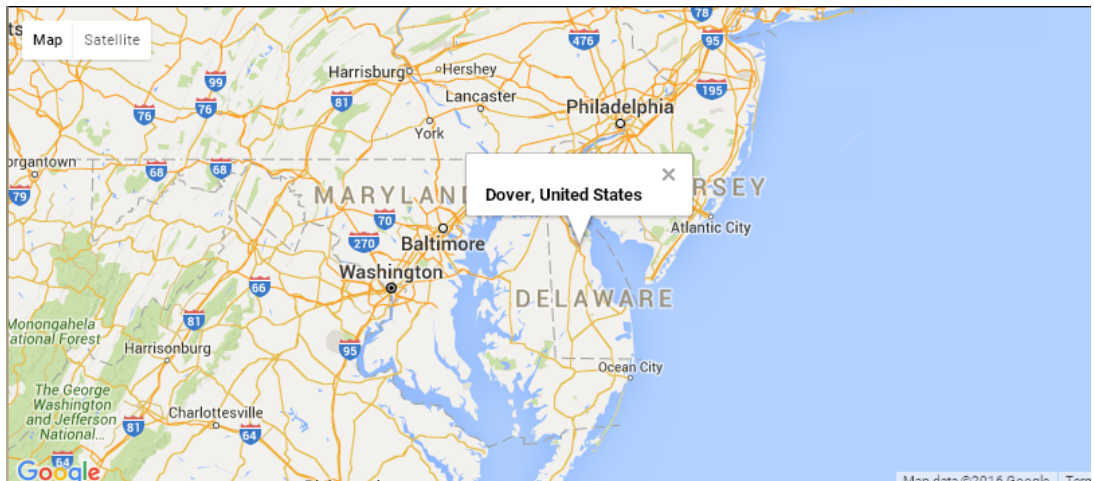
2008-10-26	Cambio	216.122.158.177	209.237.150.20
2012-08-10	Cambio	209.237.150.20	96.125.167.152
2012-10-20	Cambio	96.125.167.152	198.57.129.190
2014-12-31	Cambio	198.57.129.190	198.57.174.56
2016-01-29	Cambio	198.57.174.56	192.230.67.109

Email	webmaster@californiadar.org lizybh@earthlink.net is associated with ~2 domains hostmaster2@icom.com is associated with ~1,108 domains
Registrant Org	Daughters of the American Revolution is associated with ~3 other domains
Dates	Created on 2000-03-31 - Expires on 2017-03-31 - Updated on 2016-01-19
IP Address	192.230.67.109 - 195 other sites hosted on this server
IP Location	 - Washington - Seattle - Incapsula Inc
ASN	 AS19551 INCAPSULA - Incapsula Inc (registered Jan 12, 2011)
Domain Status	Registered And Active Website
Whois History	44 records have been archived since 2000-03-30
IP History	10 changes on 7 unique IP addresses over 10 years
Hosting History	5 changes on 4 unique name servers over 12 years
Whois Server	whois.pir.org

Ilustración 23. Información WHOIS del dominio "californiadar.org"

15.4.2 GEOLOCALIZACIÓN

Geolocalizando la dirección IP 192.230.67.109 se obtiene la siguiente información:



IP Address	City	Country Flag	DMA Code
192.230.67.109	Dover		504
Provider	State (Code)	Latitude	Area Code
Incapsula	Delaware (DE)	39.1588	302
Hostname	Country	Longitude	Postal Code
192.230.67.109.ip.incapsula.net	United States	-75.4941	19901
Timezone	Continent	TLD	GMT Offset
America/New_York	America	US	-5

Ilustración 24. Geolocalización de la dirección IP 192.230.67.109

15.5 SHREEVISWAKARMAENGWORKS.COM

15.5.1 DIRECCIÓN IP

Según información obtenida en el mes de febrero de 2016, el dominio "shreeviswakarmaengworks.com" corresponde a la IP 166.62.4.1.

— Whois & Quick Stats

Risk Score	16.65
Email	abuse@godaddy.com is associated with ~48,490,675 domains gajjarbirju@gmail.com is associated with ~5 domains
Registrant Org	cyninteltech is associated with ~1 other domains
Registrar	GODADDY.COM, LLC
Registrar Status	clientDeleteProhibited https://www.icann.org/epp#clientDeleteProhibited , clientRenewProhibited https://www.icann.org/epp#clientRenewProhibited , clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited , clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Dates	Created on 2013-10-06 - Expires on 2016-10-06 - Updated on 2015-09-15
Name Server(s)	NS65.DOMAINCONTROL.COM (has 40,138,382 domains) NS66.DOMAINCONTROL.COM (has 40,138,382 domains)
IP Address	166.62.4.1 - 2,212 other sites hosted on this server
IP Location	 - Arizona - Scottsdale - Godaddy.com Llc
ASN	 AS26496 AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC (registered Oct 01, 2002)
Domain Status	Registered And Active Website

Ilustración 25. Información WHOIS del dominio "shreeviswakarmaengworks.com"

El historial de direcciones IP del dominio muestra una IP anterior: 50.63.202.52. Comprobando el dominio en VirusTotal se puede observar que 2 motores antivirus reconocen el dominio como dañino.

URL:	http://shreevishwakarmaengworks.com/
Detecciones:	2 / 67
Fecha de análisis:	2016-03-04 08:10:58 UTC (hace 4 días, 6 horas)
Análisis Información adicional Comentarios 0 Votos	
Analizador	Resultado
BitDefender	Malware site
Fortinet	Malware site

Ilustración 26. . Análisis del dominio en VirusTotal

15.5.2 GEOLOCALIZACIÓN

Geolocalizando la dirección IP 166.62.4.1 se obtiene la siguiente información:



Ilustración 27. Geolocalización de la dirección IP 166.62.4.1

16. REFERENCIAS

- <http://www.bleepingcomputer.com/virus-removal/teslacrypt-alphacrypt-ransomware-information>
- <https://en.wikipedia.org/wiki/TeslaCrypt>
- <http://blog.talosintel.com/2016/03/teslacrypt-301-fores-from-crypto.html>
- https://en.wikipedia.org/wiki/Elliptic_curve_Diffie%E2%80%93Hellman
- <http://www.bleepingcomputer.com/news/security/teslacrypt-4-0-released-with-bug-fixes-and-stops-adding-extensions/>
- <http://download.bleepingcomputer.com/BloodDolly/TeslaDecoder.zip>

17. ANEXOS

ANEXO I: INDICADOR DE COMPROMISO – IOC

```
<?xml version="1.0" encoding="us-ascii"?>
<ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="b1608a67-a9d2-47f7-baec-986ab42a17eb"
last-modified="2016-02-12T14:24:47" xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>TeslaCrypt</short_description>
  <description>IOC para detectar TeslaCrypt</description>
  <authored_by>CCN-CERT</authored_by>
  <authored_date>2016-02-12T14:04:17</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="b777ca9e-1c19-49dc-9fcd-9a0318cde2a0">
      <IndicatorItem id="4c27c731-ca86-48e9-834c-5a27ef654f6e" condition="contains">
        <Context document="Network" search="Network/DNS" type="mir" />
        <Content type="string">residencialmontebello.com</Content>
      </IndicatorItem>
      <Indicator operator="OR" id="ed139c1b-1903-4f46-a669-f86fb243b6f1">
        <IndicatorItem id="15d031e3-7b7b-4fac-ae84-cb29e5e10bf9" condition="contains">
          <Context document="Network" search="Network/DNS" type="mir" />
          <Content type="string">shreevishwakarmaengworks.com</Content>
        </IndicatorItem>
      </Indicator>
      <Indicator operator="OR" id="885b1770-e6bb-40cc-9493-c193d372bcc3">
        <IndicatorItem id="74b44c22-2249-41db-8130-a12f15435b95" condition="contains">
          <Context document="Network" search="Network/DNS" type="mir" />
          <Content type="string">deanza.californiadar.org</Content>
        </IndicatorItem>
      </Indicator>
      <Indicator operator="OR" id="fcd35d48-e282-4eb5-a422-65f6edb657e9">
        <IndicatorItem id="4a55f883-dfe7-4ca7-ab30-1c681846ebde" condition="contains">
          <Context document="Network" search="Network/DNS" type="mir" />
          <Content type="string">santeserenitesucces.com</Content>
        </IndicatorItem>
      </Indicator>
      <Indicator operator="OR" id="456e3aba-6494-4461-a476-4ede30a0d7ad">
        <IndicatorItem id="39e4bd5e-6455-41fd-89a6-d413cfd372b" condition="contains">
          <Context document="Network" search="Network/DNS" type="mir" />
          <Content type="string">yalcingulten.com</Content>
        </IndicatorItem>
      </Indicator>
      <Indicator operator="OR" id="44b2ec1c-0fcf-4fec-a697-1d2b36e59b31">
        <IndicatorItem id="dcb633b0-088b-454c-bc40-a87093e69d84" condition="contains">
          <Context document="Network" search="Network/UserAgent" type="mir" />
          <Content type="string">Mozilla/5.0 ( Windows NT 6.3; WOW64; Trident/7.0;
Touch; rv:11.0) like Gecko</Content>
        </IndicatorItem>
      </Indicator>
      <Indicator operator="OR" id="6feae948-f0ec-405f-be67-427a63b89f91">
        <IndicatorItem id="21857f9a-63da-4e18-ae5d-26a01536ce83" condition="is">
          <Context document="RegistryItem" search="RegistryItem/Path" type="mir" />

```

```

    <Content
type="string">HKEY_CURRENT_USER\SOFTWARE\Microsoft\windows\CurrentVersion\Run</Content>
    </IndicatorItem>
    <Indicator operator="OR" id="c2146c46-8249-4f4a-bb3b-a59f3abdaa1e">
    <IndicatorItem id="edf81713-04f9-4622-a6b2-dc02cb6ed3b7" condition="is">
    <Context document="RegistryItem" search="RegistryItem/Path" type="mir" />
    <Content
type="string">HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\windows\CurrentVersion\Run</Content>
    </IndicatorItem>
    </Indicator>
    <Indicator operator="AND" id="d37fe1d3-9439-4cff-98f3-68e92a21fa60">
    <IndicatorItem id="22f52ddc-a496-4dfe-9b38-3e2820c57187" condition="contains">
    <Context document="RegistryItem" search="RegistryItem/Value" type="mir" />
    <Content type="string">zsevice-3</Content>
    </IndicatorItem>
    </Indicator>
    </Indicator>
    </Indicator>
    </definition>
</ioc>

```

ANEXO II: YARA

```

rule TeslaCrypt {
meta:
    description = "Regla para detectar Tesla con md5 eb4c18d2df9bb127ae0f51b2f2136938"
    author = "CCN-CERT"
    version = "1.0"
strings:
    $ = { 4E 6F 77 20 69 74 27 73 20 25 49 3A 25 4D 25 70 2E 00 00 00 76 61 6C 20 69
73 20 25 64 0A 00 00 }
condition:
    all of them
}

```