



SIN CLASIFICAR



# Informe Código Dañino CCN-CERT ID-11/16

---

*Ransom.Petya*

Octubre 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

|                                                            |           |
|------------------------------------------------------------|-----------|
| <b>1. SOBRE CCN-CERT .....</b>                             | <b>4</b>  |
| <b>2. RESUMEN EJECUTIVO .....</b>                          | <b>5</b>  |
| <b>3. INFORMACIÓN DE VERSIONES DEL CÓDIGO DAÑINO .....</b> | <b>5</b>  |
| 3.1 EXTENSIONES A CIFRAR .....                             | 5         |
| 3.2 EXTENSIÓN AÑADIDA A LOS ARCHIVOS CIFRADOS .....        | 5         |
| 3.3 ARCHIVOS DE RESCATE .....                              | 5         |
| 3.4 PRIMERA VERSIÓN .....                                  | 5         |
| 3.4.1 SEGUNDA VERSIÓN .....                                | 6         |
| <b>4. CARACTERÍSTICAS DEL CÓDIGO DAÑINO .....</b>          | <b>7</b>  |
| <b>5. DETALLES GENERALES .....</b>                         | <b>7</b>  |
| <b>6. PROCEDIMIENTO DE INFECCIÓN.....</b>                  | <b>8</b>  |
| <b>7. CARACTERÍSTICAS TÉCNICAS .....</b>                   | <b>8</b>  |
| 7.1 FASE I: INFECCIÓN .....                                | 8         |
| 7.2 FASE II: CIFRADO .....                                 | 10        |
| 7.3 FASE III: DESCIFRADO.....                              | 11        |
| <b>8. CIFRADO Y OFUSCACIÓN .....</b>                       | <b>11</b> |
| <b>9. PERSISTENCIA EN EL SISTEMA .....</b>                 | <b>12</b> |
| <b>10.DETECCIÓN .....</b>                                  | <b>12</b> |
| 10.1 POWERTOOL .....                                       | 12        |
| 10.2 MANDIANT.....                                         | 13        |
| <b>11.DESINFECCIÓN.....</b>                                | <b>14</b> |
| <b>12.INFORMACIÓN DEL ATACANTE .....</b>                   | <b>15</b> |
| <b>13.REGLAS DE DETECCIÓN.....</b>                         | <b>17</b> |
| 13.1 INDICADOR DE COMPROMISO – IOC.....                    | 17        |
| 13.2 YARA .....                                            | 17        |

## 1. SOBRE CCN-CERT

El CCN-CERT ([www.ccn-cert.cni.es](http://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.Petya", el cual ha sido diseñado para leer la unidad primaria en la que se haya instalado el sistema operativo del equipo, extraer su sector de arranque y los sectores pertenecientes a las tablas del sistema de archivos para cifrarlos, imposibilitando el acceso al sistema y a los datos.

El objetivo del código dañino es extorsionar a la víctima para que pague un rescate por recuperar el sistema comprometido.

## 3. INFORMACIÓN DE VERSIONES DEL CÓDIGO DAÑINO

Dicho binario solo tiene dos versiones que datan de abril y mayo de 2016.

### 3.1 EXTENSIONES A CIFRAR

El código dañino, en lugar de cifrar los archivos del sistema como otro *ransomware*, cifra determinados sectores del disco en el que se haya instalado el sistema operativo, impidiendo el acceso al sistema y a los datos almacenados en él.

### 3.2 EXTENSIÓN AÑADIDA A LOS ARCHIVOS CIFRADOS

El código dañino no modifica ni los archivos del sistema comprometido, ni sus nombres.

### 3.3 ARCHIVOS DE RESCATE

### 3.4 PRIMERA VERSIÓN

El código dañino muestra una pantalla en los arranques del sistema posteriores a la infección con una calavera y la siguiente información:



Ilustración 1. Carga dañina visual en el reinicio del equipo

### 3.4.1 SEGUNDA VERSIÓN

La segunda versión del código dañino tiene la misma interfaz que la primera versión cambiando únicamente el color del mensaje a verde:



Ilustración 2. Carga dañina visual en el reinicio del equipo de la segunda versión

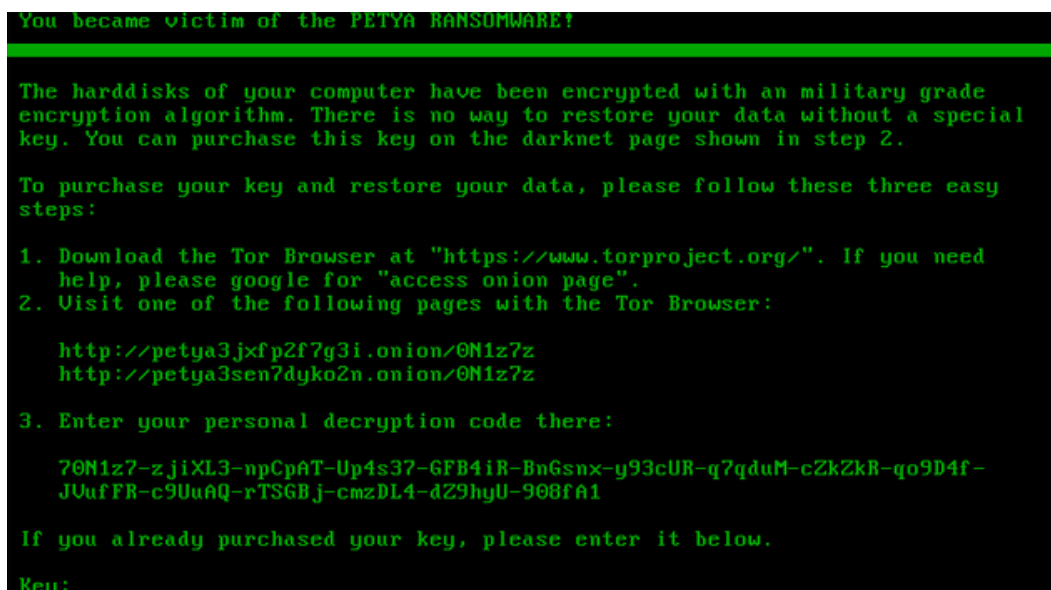


Ilustración 3. Información acerca del secuestro del sistema operativo

## 4. CARACTERÍSTICAS DEL CÓDIGO DAÑINO

El binario examinado posee las siguientes características:

- Carga el código dañino en el sistema.
- El código dañino se encuentra embebido en un "dropper".
- Utiliza técnicas anti-depuración y anti-análisis.
- Cifra el sector de arranque (*Master Boot Record* - MBR) y los sectores de la *Master File Table* (MFT).
- En cada arranque del equipo se muestra información sobre el secuestro del sistema operativo y el procedimiento a seguir para recuperar el mismo.

## 5. DETALLES GENERALES

Las muestras analizadas se corresponden con las siguientes firmas MD5:

```
af2379cc4d607a45ac44d62135fb7015  
8a241cfcc23dc740e1fadc7f2df3965e
```

Los binarios tienen formato *Portable Executable* (PE), es decir, son ejecutables para sistemas operativos Windows, concretamente para 32 bits. En las muestras analizadas se ha podido observar que la fecha interna de creación del programa data del 9 de enero de 2016 y del 27 de marzo de 2016.

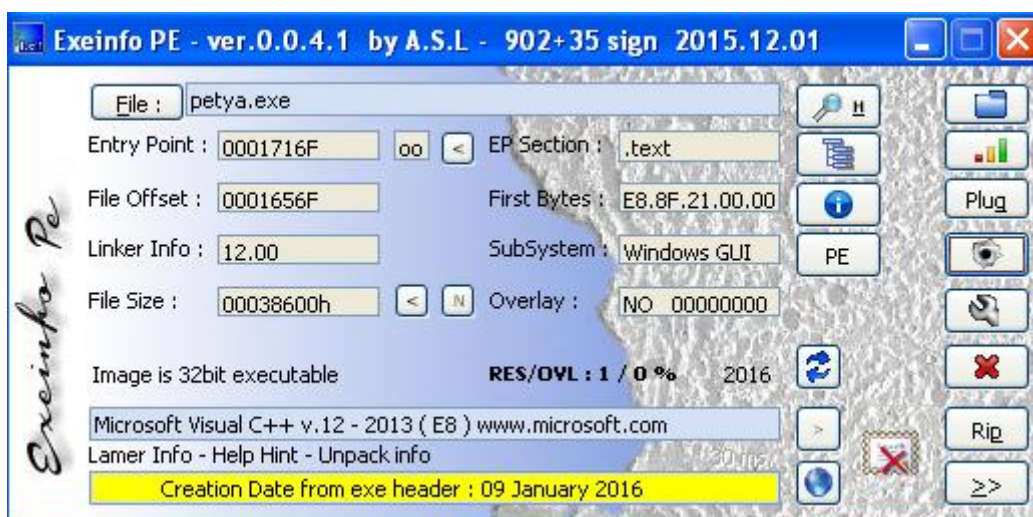


Ilustración 4. Detalles de uno de los binarios

## 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:

- El "dropper" pone en memoria el código dañino y lo ejecuta.
- Este código cifra determinados sectores del disco principal.
- Se fuerza a reiniciar el equipo de forma que el usuario no interviene en ello.
- En los arranques posteriores del sistema se muestra un mensaje sobre el secuestro del sistema y el procedimiento a seguir para recuperarlo.

## 7. CARACTERÍSTICAS TÉCNICAS

El código dañino actúa en tres fases: en la primera, realiza la infección y reinicia el sistema; en la segunda, cifra la MFT; y en la tercera, si se ha pagado el rescate, se recupera el sistema con una clave.

### 7.1 FASE I: INFECCIÓN

El código dañino posee dos capas. La primera es un "dropper" que es el encargado de descifrar en memoria el verdadero código dañino y ejecutarlo. El "dropper" intenta simular ser una aplicación legítima haciendo llamadas a funciones inocuas. Una vez descifrado en memoria el código dañino, se asegura de alterar sus secciones de datos y exportaciones para que solo pueda ser ejecutado en memoria y bajo su contexto.

Cuando el código dañino se ejecuta, genera un valor único como identificador de la víctima mediante valores aleatorios usando la función "CryptGenRandom". Una vez generado este identificador, lo cifra con Criptografía de Curva Elíptica (ECC)<sup>1</sup>.

Tras crear el identificador, procede a recopilar las propiedades del disco duro con la función "DeviceloControl" para así obtener el sector de arranque del disco. Posteriormente, el código dañino realiza las siguientes operaciones en el disco duro:

- Copia a un buffer de memoria el sector de arranque (MBR) que reside en el sector 0 del disco duro afectado y lo cifra en su totalidad con una simple operación XOR con el valor 0x37. Tras esta operación, copia ese sector al sector 56 (0x38) del disco.
- Los sectores comprendidos entre el 1 y el 33 (0x21) son cifrados mediante una operación XOR con el valor 0x37. Estos sectores, por defecto, no poseen ninguna información, siendo todos sus bytes nulos.

---

<sup>1</sup> [https://es.wikipedia.org/wiki/Criptografía\\_de\\_curva\\_elíptica](https://es.wikipedia.org/wiki/Criptografía_de_curva_elíptica)

- Copia su carga dañina entre el sector 34 (0x22) y el 53 (0x35), ambos inclusive. Este código será el que se ejecute tras el código de arranque en el disco comprometido.
- En el sector 54 (0x36) copia la clave que se utilizará para cifrar el disco en el primer reinicio tras la infección, tal y como se explica en el apartado [7.2 FASE II: CIFRADO](#). En este sector también reside un vector de inicialización (IV), las direcciones de TOR para poder efectuar el pago del secuestro y el identificador único que genera el código dañino.
- El sector 55 (0x37) se rellena con una serie de bytes, que son generados utilizando la clave de cifrado para ese disco. Este sector será usado posteriormente para comprobar si la clave introducida es correcta o no.
- En el sector 56 (0x38), tal y como se indicó, reside el sector de arranque original cifrado con el valor 0x37 mediante una operación XOR mientras que en el sector 57 (0x39) solo aparecen valores nulos.
- Por último, sobrescribe el sector de arranque con un arranque modificado (MBR) que tiene la función de copiar en la memoria los sectores de la carga dañina - del 34 (0x22) al 53 (0x35) - y ejecutarlos.

Tras realizar esta serie de operaciones en los sectores del disco, el código dañino produce un error en el sistema que provoca un "pantallazo azul" (*Blue Screen of Death* - BSOD) al utilizar la función "NtRaiseHardError<sup>2</sup>" de la librería "ntdll.dll".

Para ello se da el privilegio de poder apagar el equipo a través de la función "SeShutdownPrivilege" modificando el token del propio proceso. Una vez asignado ese privilegio, busca la dirección de la función "NtRaiseHardError" mediante "GetProcAddress". Esta función, "NtRaiseHardError", no está documentada por parte de Microsoft y recibe seis parámetros siendo, en este caso, los más importantes el primero y el quinto. El código dañino indica siempre en el primer parámetro el código de error "0xc0000350" y en el quinto el valor "6" que indica al sistema que hay que reiniciar la máquina.

|                                 |                                             |
|---------------------------------|---------------------------------------------|
| <code>push esi</code>           |                                             |
| <code>push eax</code>           |                                             |
| <code>push 28</code>            |                                             |
| <code>call [92A058]</code>      | <code>kernel32.GetCurrentProcess</code>     |
| <code>push eax</code>           |                                             |
| <code>call [92A004]</code>      | <code>ADVAPI32.OpenProcessToken</code>      |
| <code>test eax, eax</code>      |                                             |
| <code>jnz short 00928FFA</code> |                                             |
| <code>xor eax, eax</code>       |                                             |
| <code>jmp short 00929062</code> |                                             |
| <code>lea eax, [ebp-14]</code>  |                                             |
| <code>xor esi, esi</code>       |                                             |
| <code>push eax</code>           |                                             |
| <code>push 92A7A0</code>        | <code>ASCII "SeShutdownPrivilege"</code>    |
| <code>push esi</code>           |                                             |
| <code>call [92A000]</code>      | <code>ADVAPI32.LookupPrivilegeValueA</code> |

Ilustración 5. Añadiendo privilegio para poder reiniciar el equipo

<sup>2</sup> <http://undocumented.ntinternals.net/index.html?page=UserMode%2FUndocumented%20Functions%2FError%2FNtRaiseHardError.html>

## 7.2 FASE II: CIFRADO

Una vez que la máquina se reinicia comienza la segunda fase en la que se ejecuta código de 16 bits en "modo real"<sup>3</sup>. Lo primero que se ejecuta es el sector de arranque modificado por el código dañino. Este código tiene la función de copiar a la memoria RAM, en la dirección 0x8000, los sectores del disco comprendidos entre el 34 (0x22) y el 62(0x3E). Una vez copiados en la memoria, se procede a ejecutar ese código.

```

sub_7C00      proc near
cli
xor          eax, eax
mov         ss, ax
mov         es, ax
mov         ds, ax
mov         sp, 7C00h      ; sp points to this code in RAM
sti
mov         ds:byte 7C93, dl
mov         eax, 32        ; max sector number that Petya will copy into RAM
mov         ebx, 34        ; initial sector to read
mov         cx, 8000h      ; address to put the code
_petya_copy_boot_sectors:      ; CODE XREF: sub_7C00+2A1j
call        PetyaCopyCodeFromSectorsToRAM
dec         eax
cmp         eax, 0
jnz         short _petya_copy_boot_sectors
mov         eax, ds:8000h    ; 0x8000 have Petya Boot Code now
jmp         far ptr 0:8000h  jmp to it!!
sub_7C00      endp

```

Ilustración 6. Ejecución del MBR y copia de sectores a la RAM

Una vez que se comienza a ejecutar el código con la carga dañina, se procede a comprobar si el sistema tiene ya la MFT cifrada o si es el primer re-arranque y debe ser cifrada. Esto lo hace a través de un determinado byte en el sector 54, que puede tener dos valores: "0" o "1".

En el caso de que ese byte esté a "0", lo que significa que no ha cifrado todavía la MFT, el código dañino pone el valor a "1" y muestra en pantalla un comprobador de disco falso ("chkdsk"). En ese momento se procede a cifrar la MFT del sistema de archivos volviéndolo inutilizable con la clave almacenada en el sector 54. Tras ese cifrado, el código dañino borra la clave del disco y reinicia el equipo perdiendo la posibilidad de recuperarla.

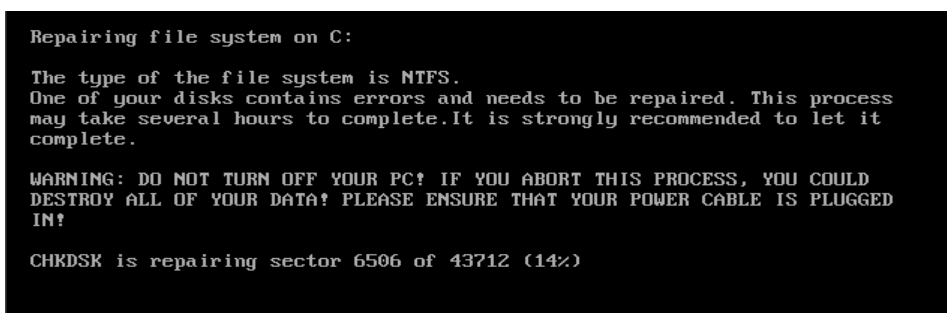


Ilustración 7. Cifrando la Master File Table

En el caso de que el valor de ese byte esté a 1, lo que indica que ya se ha cifrado la MFT, el código dañino procede a mostrar la pantalla gráfica sobre el secuestro del sistema y el procedimiento a seguir para efectuar el pago.

<sup>3</sup> [https://es.wikipedia.org/wiki/Modo\\_real](https://es.wikipedia.org/wiki/Modo_real)

### 7.3 FASE III: DESCIFRADO

A partir del final de la fase II, el sistema permanece a la espera de que se introduzca desde el teclado la clave válida para poder descifrar los sectores.

```

mov     [bp+di+var_4C], 0
inc     [bp+var_1]
cmp     [bp+var_1], 4Ah
jb      short loc_85FE
push    49h
lea     ax, [bp+var_4C]
push    ax
call    PetyaCheckInputedKey
add     sp, 4
push    ax
lea     ax, [bp+var_4C]
push    ax
mov     al, [bp+arg_2]
push    ax
push    si
call    PetyaCheckDecryptionKey
add     sp, 8
dec     al
jz      short _exit
push    offset aIncorrectKeyPleaseTryAgain_ ; "\r\n Incorrect key! Please try again!
call    PetyaWriteString
pop     bx
jmp     short loc_85F3

```

**Ilustración 8. Comprobación de la clave introducida**

Según se introduce la clave se verifica sobre el sector 55 (0x37) si puede convertir todos sus bytes al valor 0x37. En el caso de que todo el sector quede con el valor 0x37, se considera que la clave es correcta y, en caso contrario, la clave será mostrada como no válida y se volverá a preguntar por ella. En la segunda versión del código dañino el valor esperado en todos sus bytes es 0x07.

En el caso de que sea correcto, el código dañino procederá a descifrar los sectores del sistema de archivos. Tras ello, mostrará otra pantalla que, al pulsar una tecla, reiniciará el equipo dejándolo operativo de nuevo.

## 8. CIFRADO Y OFUSCACIÓN

El código dañino genera el identificador único del sistema víctima mediante funciones de la librería criptográfica de Windows como, por ejemplo, "CryptGenRandom".

El algoritmo usado es una variante del "Salsa20"<sup>4</sup>. Este algoritmo originalmente es un código de 32 bits y, por lo tanto, se diseñó para ser usado en múltiples plataformas. Sin embargo, al tener que ejecutarse en un entorno de 16 bits, los creadores del código dañino modificaron el algoritmo para adaptarlo. En la conversión del código de 32 bits a 16 bits, se dejó el código funcional pero con algunos fallos de seguridad que fueron usados para crear un descifrador gratuito en la primera versión.

En la segunda versión del código dañino los fallos de seguridad fueron corregidos haciendo que el algoritmo utilizara una versión en modo 16 bits. A pesar de ello, esta versión no está exenta de fallos de seguridad. Pese a que la clave para descifrar los

<sup>4</sup> <https://github.com/alexwebr/salsa20>

sectores es de 16 caracteres, solo 8 se computan para comprobar si la clave es válida o no, lo que rebaja la seguridad de la clave considerablemente y abre la puerta a nuevas formas de romper la cifra.

El código dañino pasa tres fases en el proceso de cifrado: en la primera, el código dañino se carga en memoria desde el "dropper"; en la segunda desde el código de arranque emulando un comprobador de disco falso ("chkdsk"); y en la tercera se procede al descifrado. Los algoritmos utilizados para cada fase son:

- En la primera fase, una simple operación XOR con el valor 0x37 para ciertos sectores del disco, como el sector de arranque o el sector de comprobación de la clave. Además, para guardar la clave de cifrado se utiliza el algoritmo ECC en la primera versión, mientras que en la segunda se almacena en texto plano.
- En la segunda fase se utiliza una versión modificada del algoritmo "Salsa20" para cifrar la MFT.
- En la tercera fase, se utiliza de nuevo el "Salsa20" para el descifrado de los sectores iniciales del disco modificados previamente.

## 9. PERSISTENCIA EN EL SISTEMA

El código dañino no crea entradas de registro ni crea nuevos archivos. Su persistencia se basa en la modificación del MBR.

## 10. DETECCIÓN

El código dañino puede ser detectado en el momento del arranque del equipo comprometido y, dependiendo de la fase en la que se encuentre, mostrará una pantalla falsa de comprobación de disco o el texto acerca del secuestro del sistema y el procedimiento a seguir para poder recuperarlo.

En un equipo afectado que no se haya reiniciado, se puede detectar el código dañino utilizando herramientas de detección a bajo nivel, como por ejemplo PowerTool<sup>5</sup>.

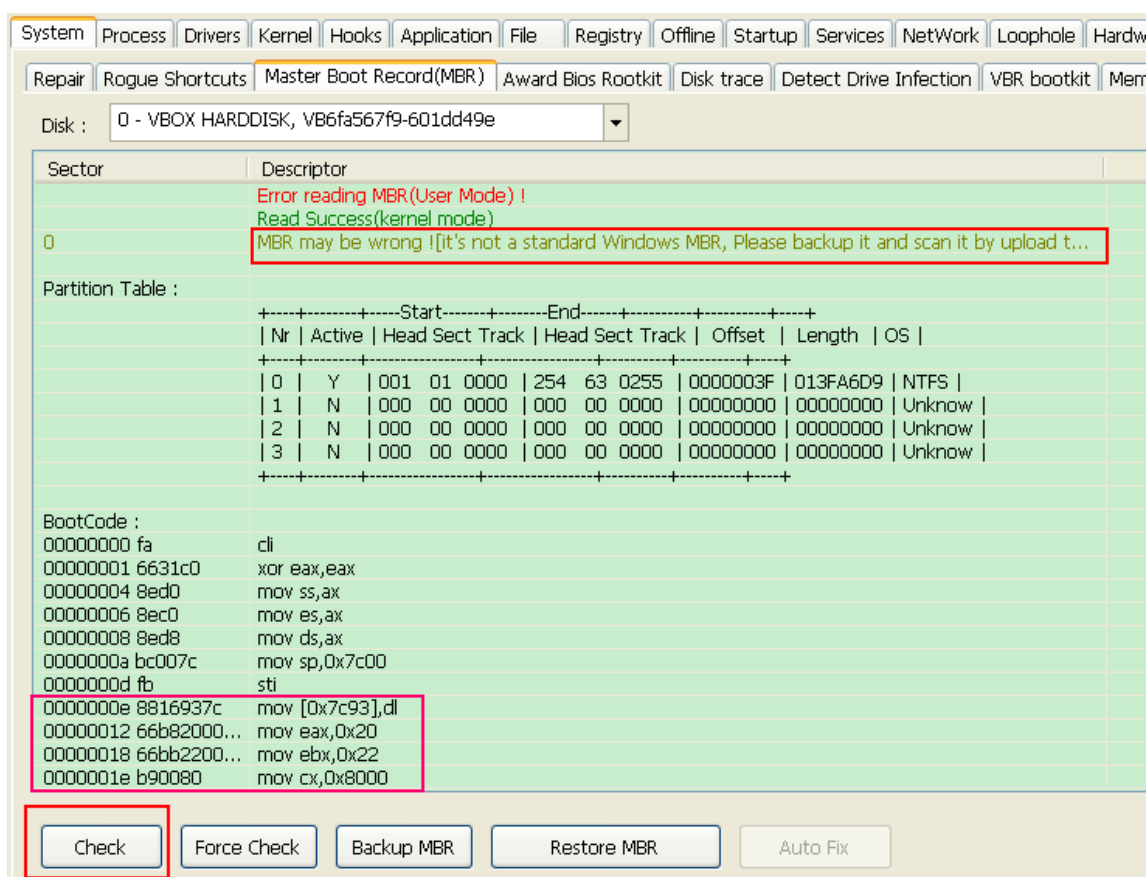
### 10.1 POWERTOOL

Con la herramienta PowerTool se puede analizar el MBR del equipo comprometido, ya sea desde el propio equipo antes de que se haya reiniciado, desde otra partición si el disco duro afectado fue puesto en otra máquina, o si se usa un adaptador que permita leer un disco duro interno desde otro sistema.

Para ello hay que arrancar la herramienta y, en la pestaña "System -> Master Boot Record (MBR)", se seleccionará el disco duro que se quiera comprobar para posteriormente pulsar el botón "Check". El resultado en un disco comprometido se puede observar en la siguiente ilustración.

---

<sup>5</sup> <http://d-h.st/users/powertool>



**Ilustración 9. Detección de modificación del MBR en disco comprometido**

La herramienta detectará que el código de arranque no es el habitual, si bien no lo reporta como infectado. Este método puede ser usado como un posible indicador de compromiso del disco. En este caso se recomienda realizar una copia de seguridad del código de arranque usando el botón "Backup MBR" y realizar su posterior análisis para confirmar que pertenece al código dañino.

## 10.2 MANDIANT

Se ha generado un nuevo archivo indicador de compromiso. El nombre del indicador generado es con GUID "8701c982-c7a9-4503-a794-1bf54ee4e02d".

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.

## 11. DESINFECCIÓN

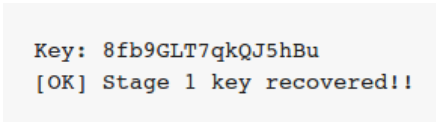
La desinfección se realizará a través de la herramienta "Antipetya" que funciona en todas las fases de la ejecución del código dañino para la primera versión del código dañino. En la segunda versión del código dañino solo se puede obtener la clave de cifrado si se encuentra en la primera fase.

En el caso de que la infección se encuentre entre la primera y la segunda fase, se puede recuperar la clave del sector 54 (0x36) que se utilizará en el siguiente reinicio del sistema para cifrar el sistema de archivos. En el caso de que el código dañino se encuentre en la segunda y la tercera fase, la utilidad informará de ello y procederá a calcular la clave mediante fuerza bruta.

Los pasos para usar esta herramienta son los siguientes:

- Descargar la imagen de disco desde <https://drive.google.com/file/d/0Bzb5kQFOXkiSTUJZQ1J1aDJxaEE/view?usp=sharing><sup>6</sup>
- Una vez descargada proceder a grabarla en un CD-ROM o en una unidad extraíble que sea usada como CD-ROM.
- Introducir el disco o la unidad extraíble en el sistema y reiniciar indicando previamente en el menú de arranque de la BIOS que se desea arrancar desde esa unidad. Cada BIOS es distinta por lo que se recomienda consultar el manual correspondiente en el caso de que se necesite más información de cómo acceder y proceder en este menú.
- Seleccionar en el arranque la unidad CD-ROM o el dispositivo extraíble usado.

La utilidad arrancará sola y en pocos segundos indicará en pantalla la clave de cifrado en el caso de que se encuentre entre la primera y la segunda fase.



```
Key: 8fb9GLT7qkQJ5hBu  
[OK] Stage 1 key recovered!!
```

### Ilustración 10. Ejemplo de la recuperación de la clave en la primera fase

En el caso de que se encuentre entre la segunda y la tercera fase, informará del suceso y procederá a calcular la clave lo cual puede durar unos minutos.

<sup>6</sup> El hash MD5 del archivo es: 5002daca5ccdd68573e2206caedd4ca6

```
[+] Trying to decrypt... Please be patient...
ugxwErH4 89
hiSwhrau 77
ugdWErH4 74
hiSwhra4 69
ugdPERH4 67
hiSwlra4 62
hgSPERH4 59
hiSwlraB 56
gAf31aib 51
hcfwlraB 48
hAf31aib 42
XqfJl15b 38
XPgKl15b 37
Xac4l15b 35
XaFFlA5e 32
AaFDlQ5B 28
xa8DlQ5B 26
xaM5lQ5B 25
x4GulQ5B 24
xbGulQ5F 22
xbG4lQlr 21
xbGtlQuB 18
8bGTqQ5B 0
[+] Key generation finished
[+] Validation passed
[+] YOUR KEY: 8xbxGxTxqxQx5xBx
```

Ilustración 11. Ejemplo de cálculo de la clave

Con esta clave se podrá reiniciar el equipo normalmente y una vez salga la pantalla de información del secuestro del sistema, se debe introducir la clave obtenida de forma que el código dañino descifre el equipo, para así arreglar MBR. Al finalizar, se reiniciará el equipo ya limpio de la amenaza.

## 12. INFORMACIÓN DEL ATACANTE

El código dañino no establece ninguna conexión con un servidor C2 (Mando y Control). Sin embargo, en la dirección web indicada en el mensaje de información del secuestro se puede encontrar la siguiente información:

### News

24.03.2015

#### WARNING

Do not restore the MBR with the Windows Recovery Tools. This could destroy your data completely!

There are a lot of wrong informations online. If you are looking for reliable informations, please visit <https://blog.gdata.de/2016/03/28222-ransomware-petya-verschluselt-die-festplatte>

---

16.12.2015

#### Petya launched

Today we launched the Petya Ransomware Project.

Copyright © 2016 Janus Cybercrime Solutions™

Ilustración 12. Información de la creación del código dañino

Como se puede apreciar en la ilustración anterior, el equipo encargado de desarrollar el código dañino se autodenomina "Janus Cybercrime Solutions"<sup>7</sup>.

En la segunda versión los autores poseen una nueva web<sup>8</sup>, en la que además de realizar el cobro de los secuestros, muestran información para futuros distribuidores del código dañino. En la web se muestran los índices de pago e información sobre de servicios gratuitos de cifrado de binarios entre otras cosas.



**PROFIT FROM PETYA & MISCHA!**

|                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>HIGH INFECTION RATES</b></p> <p>PETYA comes bundled with his little brother MISCHA. Since PETYA can't do his evil work without administrative privileges, MISCHA launches when those can't be obtained.</p> <p>PETYA does a low level encryption of the disk, which is a completely new technique in ransomware. MISCHA acts as an traditional file-based ransomware. For more informations see our FAQ.</p> | <p><b>PROVABLY FAIR</b></p> <p>As professional cybercriminals, we know that you can't trust anyone. So we developed a payment system based on multisig addresses, where no one (including us) can rip you off.</p> <p>For more informations see our FAQ.</p> | <p><b>FREE CRYPTING SERVICE</b></p> <p>We provide you FUD crypted binarys, and that 24/7. No need to buy shitty crypters or waste your money on expensive crypting services.</p> <p>Additionally, for our distributors with the highest volume, we provide a private stub. That means a even more stable infection rate. For more informations see our FAQ.</p> | <p><b>EASY ADMINISTRATION</b></p> <p>Administrative Tasks like view the latest infections, setting the ransom price or decrypting your binary can be done with an cli and simple web-interface.</p> <p>We also have an qualified support, which will help you with any problems. Since this project is still in beta, we are open for bug-report or feature-request.</p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Ilustración 13. Nueva web con servicios

<sup>7</sup> <http://www.bleepingcomputer.com/tag/janus-cybercrime-solutions>

<sup>8</sup> <http://janusaqado2zx75el.onion/start>

## 13. REGLAS DE DETECCIÓN

### 13.1 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="8701c982-c7a9-4503-a794-1bf54ee4e02d"
  xmlns="http://schemas.mandiant.com/2010/ioc"
  last-modified="2016-04-29T12:25:36"
  <short_description>Ransom.Petya</short_description>
  <description>IOC para detectar la muestra de Ransom.Petya con hash MD5
  AF2379CC4D607A45AC44D62135FB7015</description>
  <authored_by>CCN-CERT</authored_by>
  <authored_date>2016-04-29T12:22:51</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="60e82384-1a5a-4b1b-ac99-f7ec7906c63b">
      <IndicatorItem id="1e92e169-e05b-4f17-ad4b-775b7bcfa2e9" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">AF2379CC4D607A45AC44D62135FB7015</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
```

### 13.2 YARA

```
rule Ransom.Petya {
  meta:
    description = "Regla para detectar Ransom.Petya con md5
    AF2379CC4D607A45AC44D62135FB7015"
    author = "CCN-CERT"
    version = "1.0"
  strings:
    $ = { C1 C8 14 2B F0 03 F0 2B F0 03 F0 C1 C0 14 03 C2 }
    $ = { 46 F7 D8 81 EA 5A 93 F0 12 F7 DF C1 CB 10 81 F6 }
    $ = { 0C 88 B9 07 87 C6 C1 C3 01 03 C5 48 81 C3 A3 01 00 00 }
  condition:
    all of them
}
```