



SIN CLASIFICAR



Informe Código Dañino CCN-CERT ID-02/17

Ransom.Bart

Febrero de 2017

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	4
2. RESUMEN EJECUTIVO	5
3. INFORMACIÓN DE VERSIONES DEL CÓDIGO DAÑINO	5
3.1 EXTENSIONES A COMPRIMIR	5
3.2 EXTENSIÓN AÑADIDA A LOS ARCHIVOS COMPRIMIDOS	6
3.3 ARCHIVOS DE RESCATE	7
4. CARACTERÍSTICAS DEL CÓDIGO DAÑINO	8
5. DETALLES GENERALES	8
6. PROCEDIMIENTO DE INFECCIÓN	9
7. CARACTERÍSTICAS TÉCNICAS	9
8. CIFRADO Y OFUSCACIÓN	11
8.1 CIFRADO	11
8.2 OFUSCACIÓN	11
9. PERSISTENCIA EN EL SISTEMA	12
10. CONEXIONES DE RED	12
11. ARCHIVOS RELACIONADOS	13
12. DETECCIÓN	13
12.1 HERRAMIENTAS DEL SISTEMA	13
12.2 MANDIANT	13
13. DESINFECCIÓN	14
14. REGLAS DE DETECCIÓN	15
14.1 INDICADOR DE COMPROMISO – IOC	15
14.2 YARA	15

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 (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas clasificados**, del **Sector Público** 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.Bart**", el cual ha sido diseñado para enumerar todas las unidades del sistema, ya sean locales como remotas, enumerar archivos y comprimir en un archivo ".zip" con contraseña todos aquellos que tengan ciertas extensiones en su nombre.

También crea archivos en el sistema comprometido con la información de lo ocurrido y los pasos a proceder para la recuperación de los archivos, al igual que modifica el fondo del escritorio con información acerca del secuestro de los archivos y los pasos a seguir para recuperarlos.

El código dañino se cree que es de los mismos autores del código dañino "**Ransom.Locky**" o en su defecto una versión basada en su código fuente.

Existe una herramienta de descifrado gratuita para el código dañino desarrollada por el antivirus AVG la cual, aunque no da garantías del 100% de recuperación, si que puede recuperar gran parte de los archivos comprimidos.

3. INFORMACIÓN DE VERSIONES DEL CÓDIGO DAÑINO

El código dañino sólo tiene una versión.

3.1 EXTENSIONES A COMPRIMIR

El código dañino comprime los archivos que posean cualquiera de las siguientes extensiones:

.n64	.svg	.SQLITE3	.slk
.m4u	.bmp	.asc	.xlw
.m3u	.png	.lay6	.xlt
.mid	.gif	.lay	.xlm
.wma	.raw	.ms11(Security copy)	.xlc
.flv	.cgm	.ms11	.dif
.3g2	.jpeg	.sldm	.stc
.mkv	.jpg	.sldx	.sxc
.3gp	.tif	.ppsm	.ots
.mp4	.tiff	.ppsx	.ods
.mov	.NEF	.ppam	.hwp
.avi	.psd	.docb	.602
.asf	.cmd	.sxm	.dotm
.mpeg	.bat	.otg	.dotx
.vob	.class	.odg	.docm
.mpg	.jar	.uop	.docx

.wmv	.java	.potx	.DOT
.fla	.asp	.potm	.3dm
.swf	.brd	.pptx	.max
.wav	.sch	.pptm	.3ds
.mp3	.dch	.std	.txt
.qcow2	.dip	.sxd	.CSV
.vdi	.vbs	.pot	.uot
.vmdk	.asm	.pps	.RTF
.vmx	.pas	.sti	.pdf
.gpg	.cpp	.sxi	.XLS
.aes	.php	.otp	.PPT
.ARC	.ldf	.odp	.stw
.PAQ	.mdf	.wb2	.sxw
.tar.bz2	.ibd	.123	.ott
.tbk	.MYI	.wks	.odt
.bak	.MYD	.wk1	.DOC
.tar	.frm	.xltx	.pem
.tgz	.odb	.xltn	.p12
.rar	.dbf	.xlsx	.csr
.zip	.mdb	.xlsm	.crt
.djv	.SQLITEDB	.xlsb	.key
.djvu			

3.2 EXTENSIÓN AÑADIDA A LOS ARCHIVOS COMPRIMIDOS

El código dañino añade la siguiente extensión al archivo comprimido:

.bart.zip

Un ejemplo de archivo comprimido con la extensión añadida sería el siguiente:

fichero.txt.bart.zip

En el caso de que el archivo comprimido ya fuera un archivo ".zip", se añade la extensión ".zip" nuevamente y se comprime el archivo de nuevo.

3.3 ARCHIVOS DE RESCATE

El código dañino crea un archivo de texto con el nombre:

recover.txt

Este fichero contiene información acerca del secuestro de los archivos y los pasos a seguir para poder recuperarlos. El código dañino puede crear el archivo en distintos idiomas, siendo el inglés el idioma usado por defecto. Un ejemplo de dicho archivo sería el siguiente:

```

!!! IMPORTANT INFORMATION !!!

All your files are encrypted.
Decrypting of your files is only possible with the private key, which is on our secret server.
To receive your private key follow one of the links:
  1.
http://khh5cmzh5q7yp7th.tor2web.org/?id=Ar8ac%2bFNHnVx4fWkaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d
  2.
http://khh5cmzh5q7yp7th.onion.to/?id=Ar8ac%2bFNHnVx4fWkaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d
  3.
http://khh5cmzh5q7yp7th.onion.cab/?id=Ar8ac%2bFNHnVx4fWkaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d
  4.
http://khh5cmzh5q7yp7th.onion.link/?id=Ar8ac%2bFNHnVx4fWkaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d
If all addresses are not available, follow these steps:
  1. Download and install Tor Browser: https://torproject.org/download/download-easy.html
  2. After successfull installation, run the browser and wait for initialization.
  3. Type in the address bar:
    khh5cmzh5q7yp7th.onion/?id=Ar8ac%2bFNHnVx4fWkaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d
  4. Follow the instructions on the site.
!!! Your personal identification ID:
Ar8ac+FNHnVx4fWkaWbhX76y9NhKByokZXy1JXWEFFOfA== !!!

```

El código dañino también cambia el fondo del escritorio con información del secuestro de los archivos y los pasos a seguir para poder recuperarlos. Dicha modificación se realiza mediante el archivo "recover.bmp" creado dinámicamente y que reside en el Escritorio del sistema afectado.

recover.bmp

Un ejemplo de dicho archivo es el siguiente:

!!! IMPORTANT INFORMATION !!!

All your files are encrypted.

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

To receive your private key follow one of the links:

- ☐ 1. <http://khh5cmzh5q7yp7th.tor2web.org/?id=Ar8ac%2bFNHnVlx4fWKaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d>
- ☐ 2. <http://khh5cmzh5q7yp7th.onion.to/?id=Ar8ac%2bFNHnVlx4fWKaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d>
- ☐ 3. <http://khh5cmzh5q7yp7th.onion.cab/?id=Ar8ac%2bFNHnVlx4fWKaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d>
- ☐ 4. <http://khh5cmzh5q7yp7th.onion.link/?id=Ar8ac%2bFNHnVlx4fWKaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d>

If all addresses are not available, follow these steps:

- ☐ 1. Download and install Tor Browser: <https://torproject.org/download/download-easy.html>
- ☐ 2. After successful installation, run the browser and wait for initialization.
- ☐ 3. Type in the address bar:
- ☐ khh5cmzh5q7yp7th.onion/?id=Ar8ac%2bFNHnVlx4fWKaWbhX76y9NhKByokZXy1JXWEFFOfA%3d%3d
- ☐ 4. Follow the instructions on the site.

☐ !!! Your personal identification ID: Ar8ac+FNHnVlx4fWKaWbhX76y9NhKByokZXy1JXWEFFOfA== !!!

Ilustración 1. Ejemplo de fondo de escritorio modificado por el código dañino

4. CARACTERÍSTICAS DEL CÓDIGO DAÑINO

El código dañino examinado posee las siguientes características:

- Carga el código dañino en el sistema.
- Enumera las unidades del sistema tanto de disco duro como de unidades de red.
- Enumera los archivos de cada una de las unidades, buscando los que cumplan un patrón de extensión.
- Comprime archivos que cumplan ese patrón en formato ".zip" con contraseña.
- Crea archivos de texto y de imagen en el sistema, acerca del secuestro de los archivos y el procedimiento a seguir para poder recuperarlos.
- Modifica el fondo de pantalla del escritorio con una imagen con información acerca del secuestro de los archivos y el procedimiento a seguir.

5. DETALLES GENERALES

La muestra analizada se corresponde con la siguiente firma MD5:

65535f2b1ecee54718233e40e3f333b2

El binario tiene formato *Portable Executable* (PE), es decir, es un ejecutable para sistemas operativos Windows, concretamente para 32 bits.

En la muestra analizada se ha podido observar que la fecha interna de creación del programa data del 24 de junio de 2016.

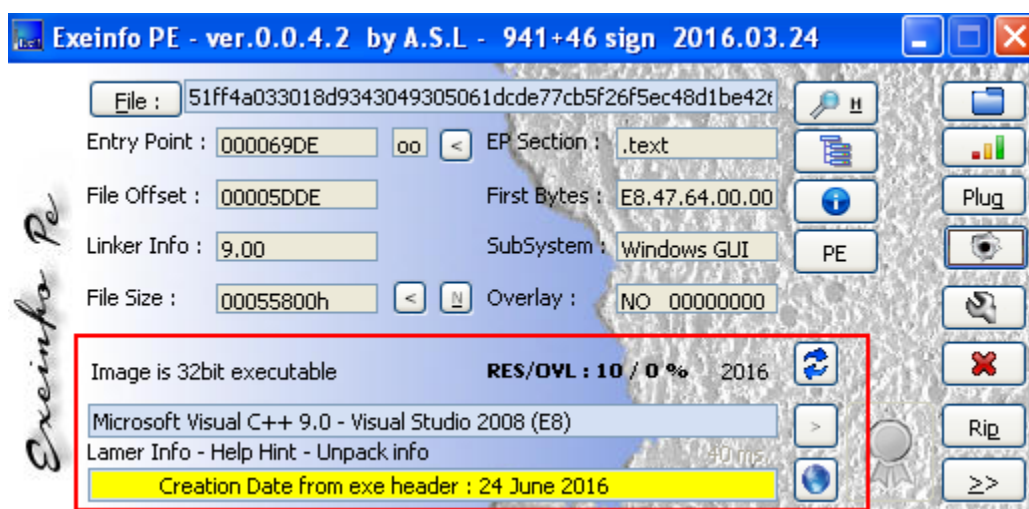


Ilustración 2. Detalles del binario

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 código dañino está embebido en un cargador ("loader") propio, el cual es el encargado de crear en memoria el código dañino final y ejecutarlo.
- Una vez ejecutado obtiene el idioma del sistema.
- Enumera todas las unidades de discos duros y de red.
- Por cada una de esas unidades encontradas y accesibles procede a enumerar todos los archivos y busca aquellos que cumplan un patrón de extensión.
- Comprime dichos archivos en formato ".zip" con contraseña.
- Muestra al usuario información visual de lo sucedido y modifica el fondo de pantalla del escritorio.
- Crea archivos de texto con información acerca del secuestro de los archivos, en todas las rutas donde haya podido comprimir archivos.

7. CARACTERÍSTICAS TÉCNICAS

El código dañino pertenece a la familia de códigos dañinos de tipo "ransomware". La primera característica es que va embebido en un cargador, "loader", el cual es el encargado de ponerlo en memoria y ejecutarlo sin dejar en disco ningún otro binario salvo el propio lanzador.

La primera acción que el código dañino realiza es asignar el modo de errores a "0x8003" lo cual permite que si el código dañino produce un error no se muestre ningún tipo de mensaje al usuario de lo ocurrido. Posteriormente, accede a su propio

token como proceso y deshabilita la virtualización en caso de que esté activa en el sistema.

A continuación, obtiene el idioma del sistema. Si lenguaje es ruso, ucraniano o bielorruso el código dañino finaliza su ejecución sin realizar ningún tipo de actividad dañina en el sistema.

Después procede a guardar el lenguaje del sistema en una variable si es:

Italiano
Francés
Alemán
Español
Árabe
Inglés

Esta acción la realiza para, posteriormente, crear los archivos con información del secuestro en el mismo idioma del sistema. En el caso de que el idioma del sistema no esté en la tabla anterior, asumirá que el idioma es el inglés.

```
jz     short _exit
push   10h           ; italian language
pop    ecx
cmp    edi, ecx
jz     short _set_language_special_var
cmp    esi, ecx
jz     short _set_language_special_var
cmp    eax, ecx
jz     short _set_language_special_var
push   0Ch           ; french language
pop    ecx
cmp    edi, ecx
jz     short _set_language_special_var
cmp    esi, ecx
jz     short _set_language_special_var
cmp    eax, ecx
jz     short _set_language_special_var
xor    ecx, ecx
inc    ecx           ; arabian language
cmp    edi, ecx
jz     short _set_language_special_var
```

Ilustración 3. Detectando lenguaje del sistema y guardando resultado en variable

A continuación, el código dañino comienza con la ofuscación. Este paso se comenta con más detalle en el apartado [8.2 OFUSCACIÓN](#) del presente informe.

El código dañino genera un identificador único con un algoritmo propietario y procede a obtener un valor aleatorio seguro usando la función "CryptGenRandom" de la librería criptográfica de Microsoft. Ese valor obtenido será la clave usada para comprimir los archivos en ".zip".

Seguidamente, obtiene todas las unidades del sistema y su tipo, quedándose solo con las de tipo disco duro, recursos de red y extraíbles. Sobre cada una de esas unidades enumera los archivos, seleccionando para cifrar aquellos que cumplan el

patrón de extensiones, indicado en el apartado de [3.1 EXTENSIONES A COMPRIMIR](#) del presente informe, y que no contengan alguna de las siguientes cadenas de texto en su nombre:



recover
bart

La explicación de que no posea ninguna de las cadenas indicadas en la anterior tabla es, en el primer caso, para no comprimir el archivo de texto con la información del secuestro de los archivos y, en segundo caso, para no volver a cifrar archivos ya cifrados.

El código dañino no utiliza ninguna librería embebida de creación de archivos ".zip". En su lugar, crea el archivo de forma manual escribiendo su cabecera byte a byte, junto con todo su contenido, incluyendo la clave para poder ser descifrado. Pese a que este proceso no usa librerías, el archivo puede ser abierto con cualquier programa que pueda abrir archivos ".zip".

Una vez que el código dañino ha finalizado de comprimir los archivos de todas las unidades disponibles, procede a cambiar el fondo del escritorio con la imagen acerca del secuestro de los archivos y los pasos a seguir para recuperarlos.

Tras esta acción finaliza sin borrarse del sistema.

8. CIFRADO Y OFUSCACIÓN

8.1 CIFRADO

A diferencia de otros "ransomware" que cifran los archivos con diversos algoritmos tanto propios como públicos (RSA, AES, RC4 por ejemplo), el código dañino usa el formato de compresión ".zip" con una contraseña generada aleatoriamente para que el usuario no pueda extraer el contenido.

La contraseña es generada con un algoritmo propietario desde un valor aleatorio obtenido con la función "CryptGenRandom" de Microsoft. Esta clave es utilizada como contraseña en todos los archivos del sistema y posee caracteres no imprimibles por lo que se necesita un programa que sea el encargado de abrir el archivo con la clave.

8.2 OFUSCACIÓN

El código dañino posee una fuerte ofuscación en su código la cual dificulta el proceso del análisis.

```

var_4          = dword ptr -4

                push    ebp
                mov     ebp, esp
                sub     esp, 0A0h
                mov     eax, __security_cookie
                xor     eax, ebp
                mov     [ebp+var_4], eax
                jmp     near ptr loc_42A827+4
sub_40BE30      endp

```

Ilustración 4. Ejemplo de ofuscación usada por el código dañino

La ofuscación incorpora varios niveles de complejidad pudiendo ejecutar funciones que ofusquen lo ya ofuscado:

```

loc_417D17:          ; CODE XREF: sub_4023DD+20Tj
                    push    1E240h
                    push    esi
                    pushf
                    push    ebx
                    push    ecx
                    push    edx
                    push    edi
                    push    ebp
                    push    eax
                    mov     ebx, 12345678h
                    mov     ebp, esp
                    sub     esp, 0C8h
                    mov     edi, esp
                    call    $+5
                    pop     esi
                    add     esi, 0FFFFFFD5D0h
                    jmp     loc_414EF5
; END OF FUNCTION CHUNK FOR sub_4023DD

```

Ilustración 5. Distintos niveles de ofuscación

Esta ofuscación proviene de la herramienta WProtect¹. Se utiliza para proteger esa parte que crea una sección en el código dañino. Todo el código de ofuscación es una máquina virtual la cual realiza acciones según sus propios comandos emulando una máquina real. Sin embargo, pese a toda la ofuscación, en algún momento las funciones del propio sistema operativo serán utilizadas. De esa forma se puede saber el funcionamiento y lógica del código dañino.

9. PERSISTENCIA EN EL SISTEMA

El código dañino no crea ninguna entrada en el registro, ni modifica nada en el sistema comprometido para obtener persistencia.

10. CONEXIONES DE RED

El código dañino no establece ninguna comunicación de red con ningún servidor C2. Toda la información que necesita la tiene embebida en el propio binario.

¹ <https://github.com/xiaoweime/WProtect>

11. ARCHIVOS RELACIONADOS

Los archivos relacionados con el código dañino son los siguientes:

<cualquier_ruta_con_archivos_comprimidos> - %DESKTOP%			
Nombre	Fecha creación	Tamaño bytes	Hash SHA1
recover.txt	<varía>	<varía>	<varía>
%DESKTOP%			
Nombre	Fecha creación	Tamaño bytes	Hash SHA1
recover.bmp	<varía>	<varía>	<varía>

12. DETECCIÓN

Para detectar si un equipo se encuentra, o ha estado infectado, se ejecutará alguna de las herramienta de Mandiant como el "Mandiant IOC Finder" o el colector generado por RedLine con los indicadores de compromiso generados para su detección o utilizando Herramientas del Sistema como el Gestor de Tareas de Windows o el propio Explorador de Windows.

12.1 HERRAMIENTAS DEL SISTEMA

Para detectar el código dañino utilizando las herramientas del sistema se puede ejecutar el Gestor de Tareas de Windows y buscar el proceso del código dañino si se está ejecutando en ese momento. En el caso de que ya se haya ejecutado el código no queda persistente con lo que no se encontraría ningún proceso.

La presencia en carpetas de archivos con la extensión indicada en el apartado de [3.2 EXTENSIÓN AÑADIDA A LOS ARCHIVOS COMPRIMIDOS](#) del presente informe, es un claro indicador de compromiso por parte del código dañino.

Si se encuentran archivos ".zip" que antes no existían y que solicitan una contraseña al abrirlos, es un indicador de compromiso del sistema al igual que la aparición de archivos de texto en numerosos directorios con el nombre indicado en la tabla de abajo.

recover.txt

Por último, el cambio de fondo del escritorio y la aparición en él de dos archivos, uno de texto indicado en la tabla anterior y otro ".bmp" con el mismo nombre, es un claro indicador de compromiso. Se debe de tener cuidado de no confundir el código dañino con el código "Ransom.Locky" que tiene un fondo de escritorio muy similar.

12.2 MANDIANT

Se ha generado un nuevo archivo indicador de compromiso. El indicador generado tiene el GUID "39fa5841-df9e-47ac-830e-1695704f067b".

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

El código dañino no se elimina tras su ejecución con lo que la primera tarea de desinfección sería eliminar al propio binario del código dañino que coincida con el hash indicado en el apartado de [4. CARACTERÍSTICAS DEL CÓDIGO DAÑINO](#) del presente informe.

El código dañino no crea ninguna entrada de registro que deba ser eliminada pero sí múltiples archivos de información acerca del secuestro de los archivos. Todos estos archivos de texto deben ser eliminados al igual que realizar el cambio de la imagen de fondo de escritorio.

Los archivos comprimidos en formato "zip" con clave pueden ser descomprimidos con la herramienta gratuita realizada por el antivirus AVG llamada "AVG's Bart Decryptor"². Esto es posible debido a que la estructura del archivo "zip" requiere almacenar la clave para poder validar la contraseña introducida.

En su funcionamiento, la herramienta necesita que se aporte dos archivos: uno no comprimido y otro comprimido por el código dañino para poder calcular esa clave y poder descomprimir todos los ficheros.

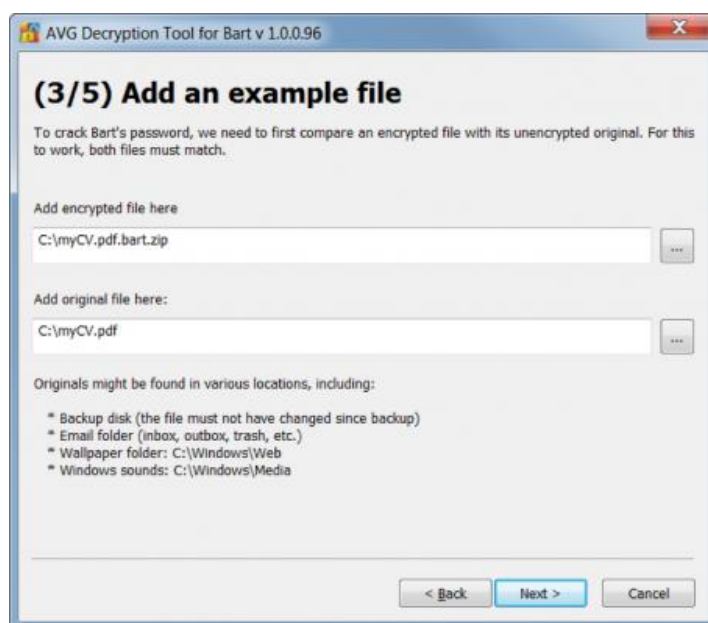


Ilustración 6. Herramienta para descomprimir archivos

² <http://now.avg.com/barts-shenanigans-are-no-match-for-avg/>

14. REGLAS DE DETECCIÓN

14.1 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="39fa5841-df9e-47ac-830e-
1695704f067b" last-modified="2016-08-31T09:59:03"
xmlns="http://schemas.mandiant.com/2010/ioc">
  <short_description>Ransom.Bart</short_description>
  <description>Reglas de compromiso que indican de la presencia del código
Ransom.Bart</description>
  <authored_by>CCN-CERT</authored_by>
  <authored_date>2016-08-31T09:54:54</authored_date>
  <links />
  <definition>
    <Indicator operator="OR" id="776d7c46-22a2-426b-9fab-6829441783ae">
      <IndicatorItem id="7845b07a-3bc6-4c20-8de1-d3d9baa7a3ae" condition="is">
        <Context document="FileItem" search="FileItem/Md5sum" type="mir" />
        <Content type="md5">65535f2b1ecce54718233e40e3f333b2</Content>
      </IndicatorItem>
    </Indicator>
  </definition>
</ioc>
```

14.2 YARA

```
rule Regla_Ransom_Bart_Memory
{
  /*
    Regla para detectar el código Ransom.Bart en la memoria del sistema.
  */
  meta:
    description = "Regla para detectar el código Ransom.Bart en memoria"
    author      = "CCN-CERT"
    version     = "1.0"

  strings:
    $a = { 6B 68 68 35 63 6D 7A 68 35 71 37 79 70 37 74 68 00 }
    $b = { 2E 62 61 72 74 00 }
    $c = { 2E 72 65 63 6F 76 65 72 2E 00 }

  condition:
    all of them
}
```