

Informe Código Dañino

CCN-CERT ID-13/22

ALPHV_Win ransomware



Diciembre 2022

Edita:



© Centro Criptológico Nacional, 2019

Fecha de Edición: diciembre de 2022

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. DETALLES GENERALES	6
4. CARACTERÍSTICAS TÉCNICAS.....	12
5. MITIGACIÓN	20
6. REGLAS DE DETECCIÓN	21
6.1 REGLA YARA	21
7. REFERENCIAS	22
ANEXO.....	23
FICHERO DE CONFIGURACIÓN	23

1. SOBRE CCN-CERT

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN) del 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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

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 identificada por la firma SHA1 7ca911dbcc159b30e7d71db30a889780e57b6c02 compilada para plataformas Windows (x32) y desarrollada en lenguaje Rust. El binario analizado pertenece a la familia de *ransomware* apodada como ALPHV también conocido como Noberus o BlackCat (debido a la existencia de un icono de un gato negro en el sitio web Tor ligado al grupo cibercriminal).

ALPHV surgió a mediados de noviembre de 2021, publicitado en determinado foro *underground*, y siguiendo el modelo de negocio RaaS (*Ransomware as a Service*) basado en una estructura de marketing de afiliados en donde éstos pueden llegar a conseguir el 80-90% del rescate ^[1]. Según información del FBI ^[2] BlackCat está ligado con miembros del ransomware BlackMatter (sucesor de DarkSide) cuya actividad tuvo gran impacto a partir de julio de 2021 llegando a afectar a diversas infraestructuras críticas en EEUU^[3].

Junto con LockBit y Black Basta, BlackCat^[4] se sitúa en el ranking de los ransomware más agresivos durante los Q2 y Q3 de 2022. Aunque la muestra actual ha sido compilada para entornos Windows, BlackCat dispone de variantes para sistemas operativos basados en Linux (Debian, Ubuntu, ReadyNAS, Synology) así como VMWare ESXi. Durante el 2022 las víctimas incluyen organizaciones en prácticamente todo el mundo dentro de los siguientes sectores: productos farmacéuticos, construcción e ingeniería, comercio minorista, transporte, servicios comerciales, seguros, maquinaria, telecomunicaciones, componentes de automóviles, etc.

ALPHV se puede configurar ^[5] para cifrar archivos utilizando los algoritmos AES o ChaCha20 y tiene capacidad para eliminar *volume shadow copies*, detener procesos y servicios, detener máquinas virtuales en servidores ESXi y auto propagarse a otros hosts de la red.

El ransomware dispone de un fichero de configuración embebido en donde se establecen los parámetros de infección que guiarán la lógica de ejecución del mismo: servicios/procesos que se deben detener, una lista blanca con los directorios/archivos/extensiones a excluir, un listado de credenciales robadas del entorno de la víctima con los que hacer movimientos laterales y/o escalar privilegios, etc. En otras versiones de BlackCat ^[6] este fichero de configuración se encuentra cifrado y requiere que el binario sea ejecutado con cierto argumento a partir del cual se deriva una *key* con la que descifrar el mismo. Sin dicho argumento el *ransomware* no se ejecutará en el sistema dificultando de este modo la labor del analista, así como su

análisis en entornos automatizados. La muestra actual, sin embargo, se corresponde con una versión previa en donde el fichero de configuración se encuentra en claro.

A fecha de realización del presente informe el sitio oficial del grupo criminal, dentro del dominio “.onion” (accesible vía TOR), presenta un total de 49 víctimas en 2022.

3. DETALLES GENERALES

El fichero analizado se corresponde con una muestra de ransomware para plataformas Windows (x32) de la familia BlackCat/ALPHV cuya firma se muestra a continuación:

MD5	93f34fb60a180a3a80ca758b97c2e551
SHA1	7ca911dbcc159b30e7d71db30a889780e57b6c02
SHA256	1048a41107f4d9a68c1f5fc0b99ac75dc198047f18bb6e50f3d462f262b8f6cd

El *sample* ha sido remitido, por primera vez, a la plataforma de análisis de malware el 18 de mayo de 2022 y actualmente muestra una tasa de detección de 57 sobre 69 motores antivirus. La mayor parte de soluciones de seguridad, así como el elevado número de *code gens* (95,31%) y *strings* reportados evidencia la relación del binario con BlackCat.

El binario no se encuentra empaquetado, presenta un tamaño de 3.068.931 bytes y ha sido compilado (*statically linked*) para arquitecturas de 32 bit el 7 de diciembre de 2021 según información de su *File Header*. A partir de las múltiples referencias al gestor de paquetes “Cargo” en los *strings* del binario (“*.cargo/registry/src*”) se puede inferir que Rust ha sido el lenguaje empleado por los atacantes para su desarrollo. Dichos *paths* reflejan las dependencias externas requeridas por el código (obsérvese, por ejemplo, la referencia a la implementación de AES en Rust).

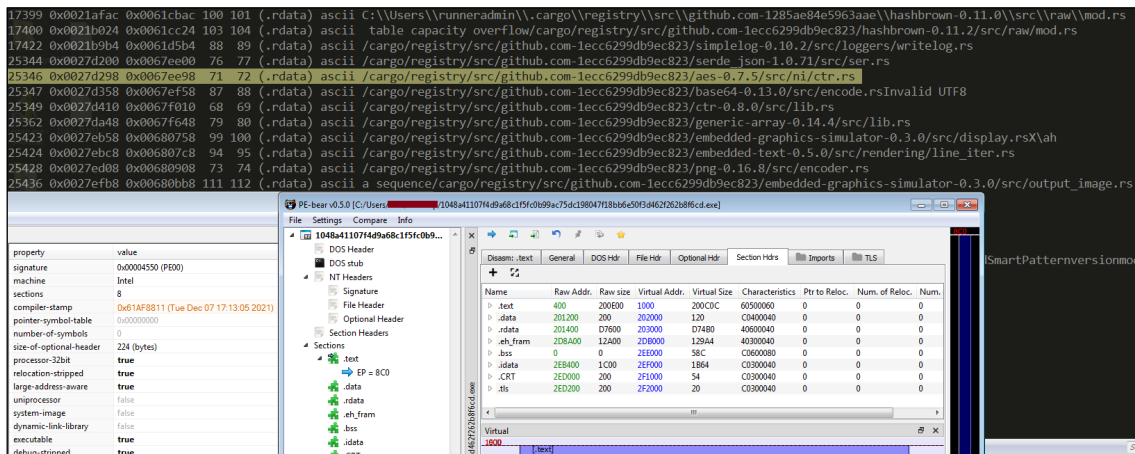


Figura 1. Propiedades estáticas: Section Headers / Strings (Rust)

El binario requiere de cierto argumento para su ejecución, en concreto el parámetro “**--access-token <ACCESS_TOKEN>**” pudiendo especificar para la muestra actual cualquier valor; únicamente se utilizará dicho parámetro para confirmar el proceso de cifrado (a diferencia de otras versiones de BlackCat en donde dicho *token* será necesario para descifrar el fichero de configuración).

Desde la línea de comandos se puede especificar el argumento ‘-h’ para ver el menú de ayuda y conocer las opciones de ejecución. Como se observa en la siguiente imagen, el ransomware tiene capacidad para hacer descubrimiento y propagarse a otras máquinas, excluir directorios, finalizar VMs en entornos ESXi, eliminar *snaphosts*, etc. Algunas de estas opciones se detallarán en el siguiente punto.

```

c:\
λ blackcat_v1.exe -h

USAGE:
    [OPTIONS] [SUBCOMMAND]

OPTIONS:
    --access-token <ACCESS_TOKEN>    Access Token
    --bypass <BYPASS>...              Run as child process
    --child                             Invoked with drag and drop
    --drag-and-drop                    Drop drag and drop target batch file
    --drop-drag-and-drop-target        Print help information
    -h, --help                         Enable logging to specified file
    --log-file <LOG_FILE>              Do not discover network shares on Windows
    --no-net                           Do not self propagate(worm) on Windows
    --no-prop                          Do not propagate to defined servers
    --no-prop-servers <NO_PROP_SERVERS>... Do not stop VMs on ESXi
    --no-vm-kill                       Do not stop defined VMs on ESXi
    --no-vm-kill-names <NO_VM_KILL_NAMES>... Do not wipe VMs snapshots on ESXi
    --no-vm-snapshot-kill              Do not update desktop wallpaper on Windows
    --no-wall                           Only process files inside defined paths
    -p, --paths <PATHS>...             Run as propagated process
    --propagated                       Show user interface
    --ui                               Log to console
    -v, --verbose
  
```

Figura 2. Menú ayuda (BlackCat)

El *flag --verbose* mostrará por STDOUT el proceso de cifrado en *runtime* (errores, ficheros afectados, etc.) además de reflejar las directivas establecidas en el fichero de configuración. En la siguiente imagen se muestra, por ejemplo, los servicios que se finalizarán antes de comenzar con el cifrado de ficheros.

```

21:56:17 MASTER [INFO] locker:core:os:windows:cmd: enum_servers_sync:start
21:56:17 MASTER [INFO] locker:core:os:windows:shadow_copy: shadow_copy:remove_all-1
21:56:17 MASTER [INFO] encrypt_app:windows: Cleaning event log
21:56:17 MASTER [INFO] encrypt_app:windows: Waiting for kills to complete
21:56:17 MASTER [INFO] encrypt_app:windows: Killing Processes
21:56:17 MASTER [INFO] locker:core:os:windows:service: kill_all("mepcs", "montas", "veean", "suc6", "backup", "sql", "vss", "msexchange", "sql")1,5s
21:56:17 MASTER [INFO] locker:core:os:windows:service: enum_services:ok=48
21:56:17 MASTER [INFO] locker:core:os:windows:service: service:stop_recursive:vss,5s
21:56:17 MASTER [INFO] locker:core:os:windows:service: enum_dependent_services:"vss"
21:56:17 MASTER [INFO] locker:core:os:windows:service: enum_dependent_services:ok=0
21:56:17 MASTER [INFO] locker:core:os:windows:service: stop_vss:5s
21:56:17 MASTER [INFO] locker:core:os:windows:service: try_stop_vss
21:56:17 MASTER [INFO] locker:core:os:windows:service: try_stop:ok=vss_3
21:56:17 MASTER [INFO] locker:core:os:windows:service: query_status_process:ok=1
21:56:17 MASTER [INFO] locker:core:attach: rpa: 200p
21:56:17 MASTER [INFO] encrypt_app:windows: Trying to mount hidden partitions
21:56:17 MASTER [INFO] locker:core:os:windows:hidden_partitions: mount_all:mounting-Z:\,Some('Z')
21:56:17 MASTER [INFO] encrypt_app:windows: Discovering local drives
21:56:17 MASTER [INFO] locker:core:discoverer: Recv Path -> C:\
21:56:17 MASTER [INFO] encrypt_app:windows: Cleaning up Recycle Bin
21:56:17 MASTER [INFO] locker:core:discoverer: Recv Path -> D:\
21:56:17 MASTER [INFO] locker:core:discoverer: Recv Path -> Z:\
21:56:17 MASTER [INFO] locker:core:discoverer: Recv Path -> C:\Users\
21:56:17 MASTER [ERROR] Can't read metadata -> C:\pagefile.sys, err=0x<code> 32, kind: Uncategorized, message: "The process cannot access the file because it is being used by another process." >
21:56:17 MASTER [INFO] locker:core:discoverer: Fixing Permissions -> C:\Users\Default User
21:56:17 MASTER [ERROR] Can't open file -> C:\Users\NeoNtuser.dat.LOCAL, err=0x<code> 32, kind: Uncategorized, message: "The process cannot access the file because it is being used by another pro
21:56:17 MASTER [ERROR] Can't open file -> C:\Users\NeoNtuser.dat.LOCAL, err=0x<code> 32, kind: Uncategorized, message: "The process cannot access the file because it is being used by another pro
21:56:17 MASTER [ERROR] Can't open file -> C:\Users\NeoNtuser.DAT(016808bd-6c6f-11de-8d1d-001e0bde3ec).IMB, err=0x<code> 32, kind: Uncategorized, message: "The process cannot access the file

```

Figura 3. Opción --verbose

Mediante el argumento *--log-file <LOG_FILE>* será posible guardar toda la información en un fichero de texto. La opción *--ui (user interface)* proporcionará otra vista que permitirá también mostrar el progreso de la infección de manera gráfica ofreciendo información sobre el número de ficheros afectados, el número de ficheros escaneados, así como la velocidad de procesamiento (MB/s).



Figura 4. User Interface (--ui)

A diferencia de las versiones más recientes de BlackCat la muestra analizada presenta el fichero de configuración en claro (formato *json*) dentro de la sección *“.rdata”*. En la siguiente imagen se puede observar la clave pública empleada para el proceso de cifrado, así como la extensión a la que se renombrará cada fichero afectado.

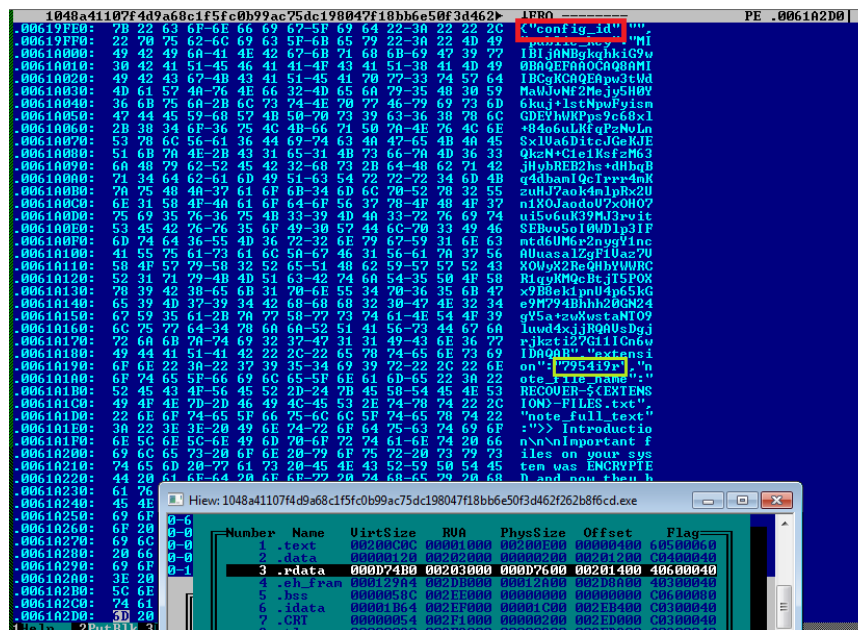


Figura 5. Fichero de configuración (.rdata)

Herramientas como *blackCatConf* [7] permiten extraer fácilmente el fichero de configuración y mostrar cada una de sus directivas.

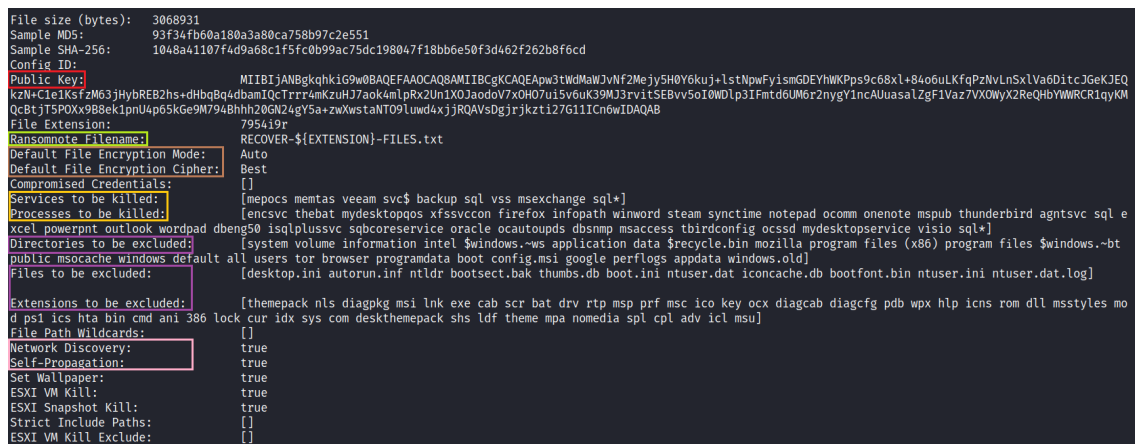


Figura 6. Extracción configuración (blackCatConf)

Obsérvese que en dicho *json* se configuran muchos parámetros que afectarán al comportamiento del ransomware; por ejemplo:

- Los **servicios y procesos** que serán finalizados.
- **Ficheros, directorios y extensiones** que serán excluidos del proceso de cifrado.
- La **clave pública RSA** codificada en base 64.
- Extensión de los ficheros renombrados que serán cifrados (*7954i9r*).

- Un *array* con credenciales comprometidas empleadas para escalar y propagar la infección (en la muestra actual se encuentra vacío).
- Formato del fichero con las **instrucciones de recuperación**: *RECOVER-{\$EXTENSION}-FILES.txt*.
- **Descubrimiento y propagación** a nuevos equipos.
- El **algoritmo y modo de cifrado**. El valor “Best” en la directiva “Default File Encryption Cipher” instruye al código dañino a emplear el conjunto de instrucciones AES-NI. Si la víctima no tiene soporte AES-NI empleará ChaCha20^[10] en su lugar. Por otro lado, el modo “Auto”, especificado por la directiva “Default File Encryption Mode”, establece la estrategia más óptima para cifrar los ficheros en función de la extensión y el tamaño del mismo. Otras opciones, como “SmartPattern”, dividen cada fichero en un número determinado de bloques cifrando un porcentaje de los mismos. El investigador Aleksandar Milenkoski realizó un análisis detallado de cada uno de los modos soportados por BlackCat (*Full, HeadOnly, DotPattern, SmartPattern*). Para más información consúltese la referencia adjunta ^[9].

El funcionamiento y características del ransomware son detallados en el propio anuncio del grupo criminal en el foro ruso *underground* RAMP (*Russian Anonymous MarketPlace*). Su contenido ^[10], traducido en inglés, se muestra a continuación:

INTRO

We are glad to welcome you to our affiliate program.

*We have taken into account all the advantages and disadvantages of previous partner programs and are proud to bring you **ALPHV** – the next generation of ransomware.*

All software is written from scratch, the decentralization of all web resources is architecturally laid down. A unique onion domain is generated for each new company. For each advertiser, an entrance is provided through its own unique onion domain (hello LockBit). Own datacenter for hosting leak files over 100 TB.

We are already cooperating with top recovery companies that worked with darks, revils, etc.

There is a support on chats, which sits 24 by 7, but if you wish, you can negotiate yourself.

SECURITY

We are in every possible way ready for existence in modern conditions, meeting all the requirements for the security of infrastructure and advertisements. In the affiliate program all possible links with forums are architecturally excluded (hello revil), algorithms for self-deletion of data upon expiration of the limitation period are laid down, a built-in mixer is integrated with a real break in the chain (not to be confused with Wasabi, BitMix and others), because you get completely clean coins from foreign exchanges. The wallets to which your coins were sent are unknown for our backend. The infrastructure is fragmented into the so-called. nodes that are interconnected through a whole network of pads within the onion network and are located behind NAT + FW. Even when receiving a full-fledged cmdshell, the attacker will not be able to reveal the real IP address of the server. (hi Conti)

SOFTWARE

The software is written from scratch without using any templates or previously leaked source codes of other ransomware. The choice is offered:

4 encryption modes:

-Full – full file encryption. The safest and slowest.

-Fast – encryption of the first N megabytes. Not recommended for use, the most unsafe possible solution, but the fastest.

-DotPattern – encryption of N megabytes through M step. If configured incorrectly, Fast can work worse both in speed and in cryptographic strength.

*-Auto. Depending on the type and size of the file, the locker (both on windows and *nix / esxi) chooses the most optimal (in terms of speed / security) strategy for processing files.*

-SmartPattern – encryption of N megabytes in percentage steps. By default, it encrypts 10 megabytes every 10% of the file starting from the header. The most optimal mode in the ratio of speed / cryptographic strength.

2 encryption algorithms:

-ChaCha20

-AES

In auto mode, the software detects the presence of AES hardware support (exists in all modern processors) and uses it. If there is no AES support, the software encrypts files ChaCha20.

Cross-platform software, i.e. if you mount Windows disks in Linux or vice versa, the decryptor will be able to decrypt the files.

Supported OS:

– All line of Windows from 7 and higher (tested by us on 7, 8.1, 10, 11; 2008r2, 2012, 2016, 2019, 2022); XP and 2003 can be encrypted over SMB.

– ESXI (tested on 5.5, 6.5, 7.0.2u)

– Debian (tested on 7, 8, 9);

– Ubuntu (tested on 18.04, 20.04)

– ReadyNAS, Synology

Since recently binaries have been leaking to analysts, and premium VT allows you to download samples and receive readme in chats, random people may appear who can disrupt negotiations (hello darkside), when launching the software it is MANDATORY to use the –access-token flag. The cmdline arguments are not passed to the Avers, which will keep the privacy of the correspondence with the victim. For the same reason, each encrypted computer generates its own unique ID used to separate chats.

There is a function of automatic downloading of files from the MEGA service, you give a link to the files, they are automatically downloaded to our servers.

You can get a full description of all functionality in the FAQ section.

Siguiendo la misma operativa que la mayor parte de ransomware, ALPHV creará en cada directorio afectado un fichero “.txt” con las instrucciones de recuperación (para la muestra actual, *RECOVER-7954i9r-FILES.txt*) en donde pueden encontrarse diversas referencias a direcciones “.onion” vinculadas con el grupo criminal.

Por un lado, una URL para acceder a un *preview* de los datos exfiltrados (<http://alphvmmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion>) previo a la ejecución de BlackCat y, por otro, un enlace a cierta URL para proceder con el rescate (<http://sty5r4hhb5oihbq2mwevrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd.onion>).

```
Short Ransomnote:
Important files on your system was ENCRYPTED.
Sensitive data on your system was DOWNLOADED.
To recover your files and prevent publishing of sensitive information follow instructions in "${NOTE_FILE_NAME}" file.

Full Ransomnote:
>> Introduction
Important files on your system was ENCRYPTED and now they have have "${EXTENSION}" extension.
In order to recover your files you need to follow instructions below.

>> Sensitive Data
Sensitive data on your system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank statements.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more ...

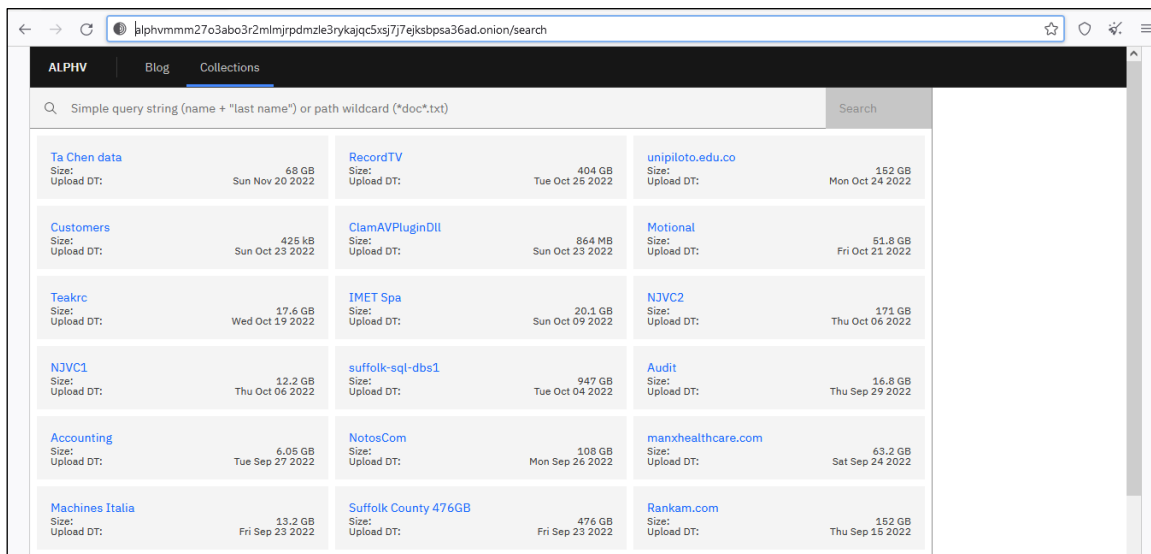
Private preview is published here: http://alphvmmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/336eb50d-ebf8-436b-937d-ec075de46e7f/419ef3f950d9f346cf86db56db453539dcd51567ea871728e78dbc9918c7efeb

>> CAUTION
DO NOT MODIFY FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.
YOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER KEY.

>> Recovery procedure
Follow these simple steps to get in touch and recover your data:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://sty5r4hhb5oihbq2mwevrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd.onion/?access-key=${ACCESS_KEY}
```

Figura 7. Mensaje de recuperación

A fecha de realización del presente informe, el portal de ALPHV recoge un total de 49 entidades comprometidas durante el año 2022.



ALPHV		
Simple query string (name + "last name") or path wildcard (*.doc*.txt)		
Ta Chen data Size: 68 GB Upload DT: Sun Nov 20 2022	RecordTV Size: 404 GB Upload DT: Tue Oct 25 2022	unipiloto.edu.co Size: 152 GB Upload DT: Mon Oct 24 2022
Customers Size: 425 kB Upload DT: Sun Oct 23 2022	ClamAVPluginDll Size: 864 MB Upload DT: Sun Oct 23 2022	Motional Size: 61.8 GB Upload DT: Fri Oct 21 2022
Teakrc Size: 17.6 GB Upload DT: Wed Oct 19 2022	IMET Spa Size: 20.1 GB Upload DT: Sun Oct 09 2022	NJVC2 Size: 171 GB Upload DT: Thu Oct 06 2022
NJVC1 Size: 12.2 GB Upload DT: Thu Oct 06 2022	suffolk-sql-dbs1 Size: 947 GB Upload DT: Tue Oct 04 2022	Audit Size: 16.8 GB Upload DT: Thu Sep 29 2022
Accounting Size: 6.05 GB Upload DT: Tue Sep 27 2022	NotosCom Size: 108 GB Upload DT: Mon Sep 26 2022	manxhealthcare.com Size: 63.2 GB Upload DT: Sat Sep 24 2022
Machines Italia Size: 13.2 GB Upload DT: Fri Sep 23 2022	Suffolk County 476GB Size: 476 GB Upload DT: Fri Sep 23 2022	Rankam.com Size: 152 GB Upload DT: Thu Sep 15 2022

Figura 8. Entidades afectadas por ALPHV (2022)

4. CARACTERÍSTICAS TÉCNICAS

ALPHV se ha caracterizado por haber sido uno de los primeros ransomware implementados en Rust. Este lenguaje no solo ofrece a los atacantes notables ventajas desde un punto de vista de seguridad y rendimiento (mejor gestión de la concurrencia y la memoria, gran velocidad de cifrado, etc.) sino que dificulta significativamente la ingeniería inversa por parte de los analistas. Este hecho está relacionado con la forma en la que Rust gestiona los errores y la gran cantidad de *checks* de seguridad que se añaden al código durante el proceso de compilación para garantizar un uso seguro de la memoria. La carencia de una ABI estable, el uso de determinados *flags* de compilación (por ejemplo, *link-time optimization*) así como otras características del propio lenguaje complican en gran medida la comprensión del código generado.

Pese a elegir Rust como lenguaje para su desarrollo, el binario no está empaquetado facilitando en gran medida la comprensión de su código. Para instruir al binario que comience con el proceso de cifrado de ficheros es necesario proporcionar, por medio de su *command-line*, el argumento “**--access-token <TOKEN>**” donde el *token* puede ser cualquier cadena para la muestra actual (en otras versiones de BlackCat este *token* será necesario para poder continuar con la infección al corresponderse con una cadena a partir de la cual se genera una clave AES con la que descifrar su fichero de configuración).

BlackCat puede eludir UAC abusando de la interfaz COM CMSTPLUA^[11] generando un nuevo proceso secundario bajo *"dllhost.exe"* con permisos elevados con los que cifrar la mayor cantidad posible de ficheros en el sistema.

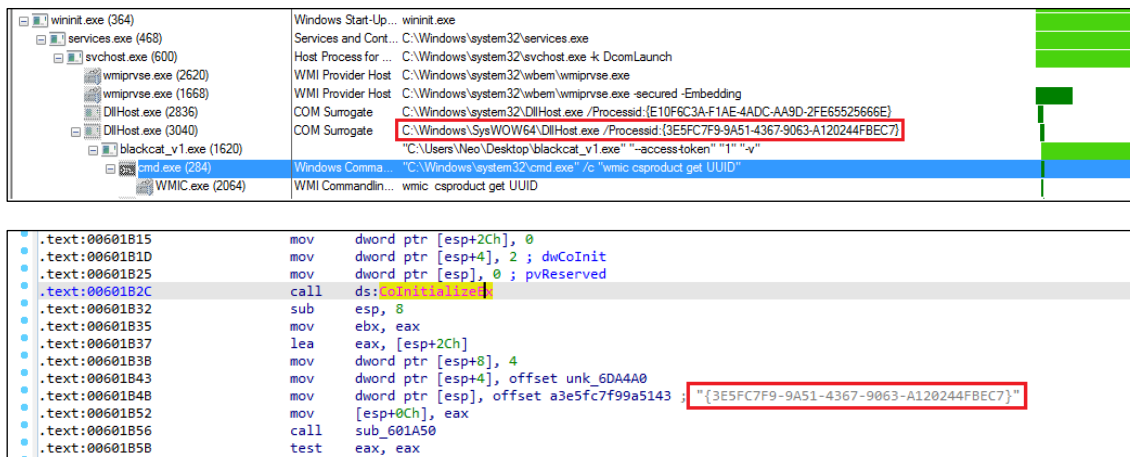


Figura 9. UAC Bypass

El ransomware habilitará los enlaces simbólicos locales y remotos posiblemente para asegurarse de que pueda seguir los accesos directos y localizar los ficheros originales. Para habilitar dicha funcionalidad ejecutará los siguientes procesos vía *CreateProcessW*:

- *fsutil behavior set SymlinkEvaluation R2L:1*
- *fsutil behavior set SymlinkEvaluation R2R:1*

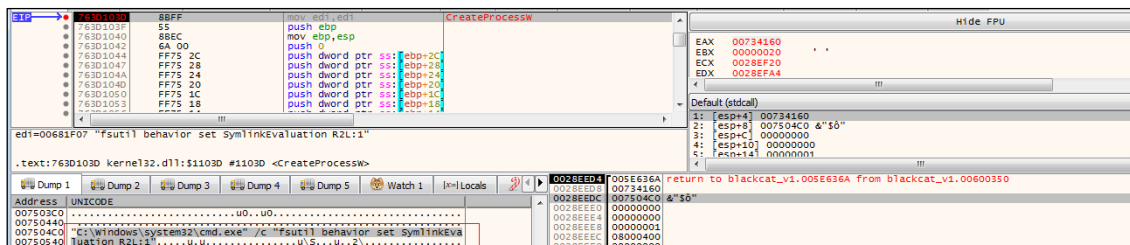


Figura 10. Enlaces simbólicos locales y remotos

También recuperará el UUID (identificador único universal) de la máquina mediante la ejecución de un comando WMI (*wmic csproduct get UUID*) que se utilizará para generar cierto *access-token* que formará parte de la URI de recuperación en el sitio Tor que se incluirá en la nota de rescate:

(<http://sty5r4hbb5oihbq2mwefrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd.onion/?access-key={access-token}>):

```
.text:005E635E push    0  
.text:005E6360 push    dword ptr [esp+58h]  
.text:005E6364 push    eax  
[.text:005E6365 call     CreateProcess] ; kernel32.dll:kernel32_CreateProcessInternalW+DA9  
.text:005E636A test     eax, eax  
.text:005E636C jz      loc_5F6453  
.text:005E6372 push    dword ptr [esp+24h]  
.text:005E6376 call     CloseHandle  
.text:005E637B movsd   xmm1, qword ptr [esp+104h]
```

Figura 11. Obtención UUID vía WMIC

Como es habitual en el proceso de infección en la gran mayoría de *ransomware*, ALPHV intentará eliminar las *Volume Shadow Copy Service* (VSS) para dificultar las tareas de recuperación de ficheros.

[illegible]

Figura 12. Eliminación Volume Shadow Copy

Asimismo, el ransomware eliminará todos los *event logs* haciendo uso de wevtutil:

```
for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1\""
```

76301039	90	nop				EAX	0028EFD0	
7630103A	90	nop				EDX	0028EF84	
7630103B	90	nop				ESP	0028F3F8	
7630103C	90	nop				ESP	0028EE84	
7630103D	90	nop				EIP	00000000	
7630103E	90	nop				EDI	0060E050	
7630103F	55	push esp	CreateProcessW			EIP	7630103D	
76301040	8BFF	mov edi,edi				EFLAGS	00000035	
76301041	88EC	mov ebp,esp				ZF	0	PF
76301042	6A 00	push 0				OF	0	SF
76301043	FF75 2C	push dword ptr [ebp+2C]				CF	1	TF
76301044	FF75 18	push dword ptr [ebp+18]						
76301045	FF75 14	push dword ptr [ebp+14]						
76301046	FF75 24	push dword ptr [ebp+24]						
76301047	FF75 20	push dword ptr [ebp+20]						
76301048	FF75 1C	push dword ptr [ebp+1C]						
76301049	FF75 10	push dword ptr [ebp+10]						
7630104A	FF75 0C	push dword ptr [ebp+0C]						
7630104B	FF75 08	push dword ptr [ebp+08]						
7630104C	FF75 04	push dword ptr [ebp+04]						
7630104D	FF75 00	push dword ptr [ebp+00]						
7630104E	6A 00	push 0						
7630104F	FF75 08	push dword ptr [ebp+08]						
76301050	6A 00	push 0						
76301051	CALL	kernel32.CreateProcessW						
76301052	EB	push ebx						
76301053	EB	push ebx						
76301054	EB	push ebx						
76301055	EB	push ebx						
76301056	EB	push ebx						
76301057	EB	push ebx						
76301058	EB	push ebx						
76301059	EB	push ebx						
7630105A	EB	push ebx						
7630105B	EB	push ebx						
7630105C	EB	push ebx						
7630105D	EB	push ebx						
7630105E	EB	push ebx						
7630105F	EB	push ebx						
76301060	EB	push ebx						
76301061	EB	push ebx						
76301062	EB	push ebx						
76301063	EB	push ebx						
76301064	EB	push ebx						
76301065	EB	push ebx						
76301066	EB	push ebx						
76301067	EB	push ebx						
76301068	EB	push ebx						
76301069	EB	push ebx						
7630106A	EB	push ebx						
7630106B	EB	push ebx						
7630106C	EB	push ebx						
7630106D	EB	push ebx						
7630106E	EB	push ebx						
7630106F	EB	push ebx						
76301070	EB	push ebx						
76301071	EB	push ebx						
76301072	EB	push ebx						

Figura 13. Eliminación de event logs vía wevtutil

Posteriormente modificará el parámetro TCP/IP **MaxMpxCt** del registro para incrementar el número de peticiones salientes permitidas (esto facilitará la distribución del *ransomware* a otras máquinas de la red). Para realizar dicho cambio se apoyará en el binario *reg.exe*:

```
reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v  
MaxMpxCt /d 65535 /t REG_DWORD /f
```

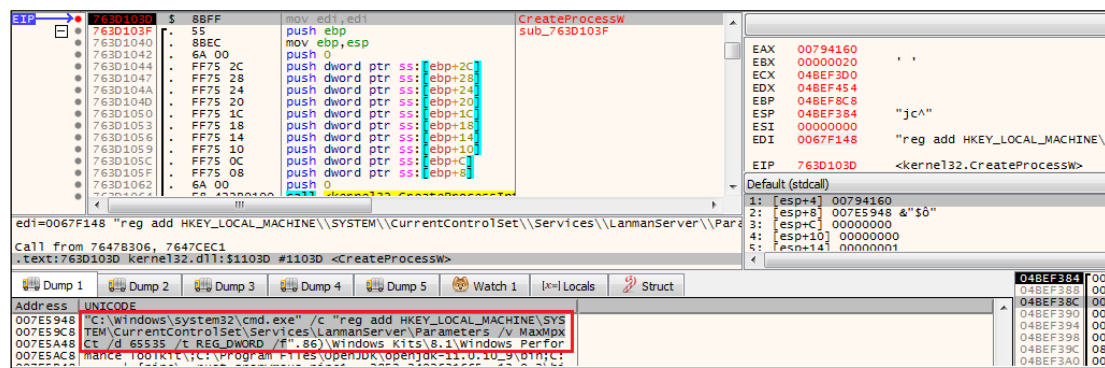


Figura 14. Eliminación de event logs via wevtutil

El ransomware tiene capacidad para propagarse a otros equipos de la red utilizando NetBIOS y SMB incluyendo también el uso del protocolo de resolución de direcciones (ARP) para recopilar las direcciones IP y MAC de la tabla ARP (y obtener así la lista de hosts conocidos por el host de la víctima). También hará uso de la API *NetServerEnum* para enumerar todos los servidores del dominio (SV_TYPE_ALL = 0xFFFFFFF) y de *NetShareEnum* para descubrir recursos compartidos de red.

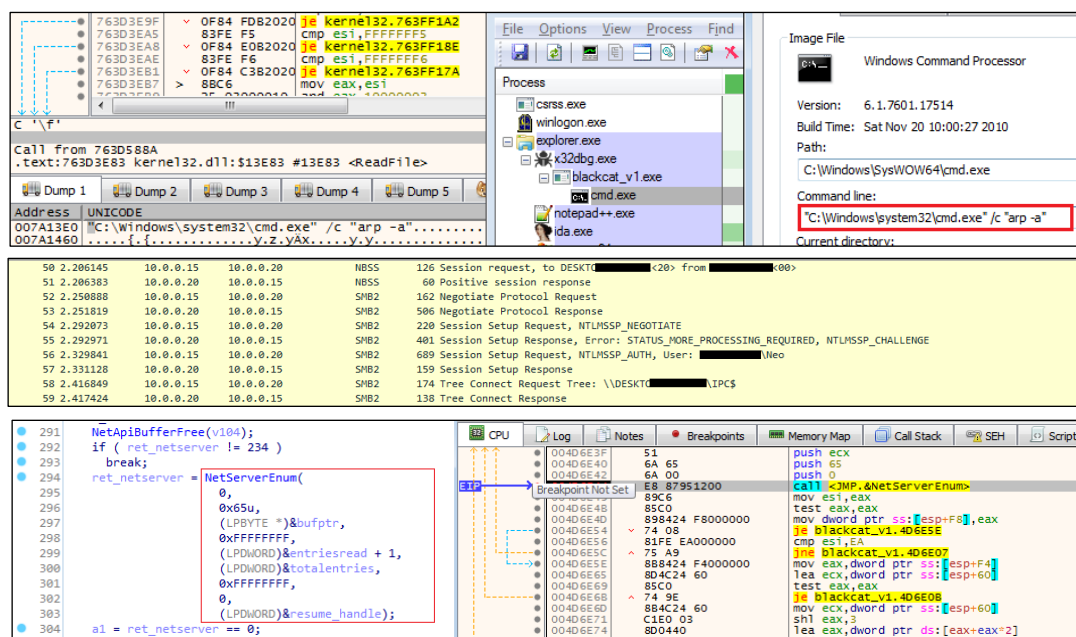
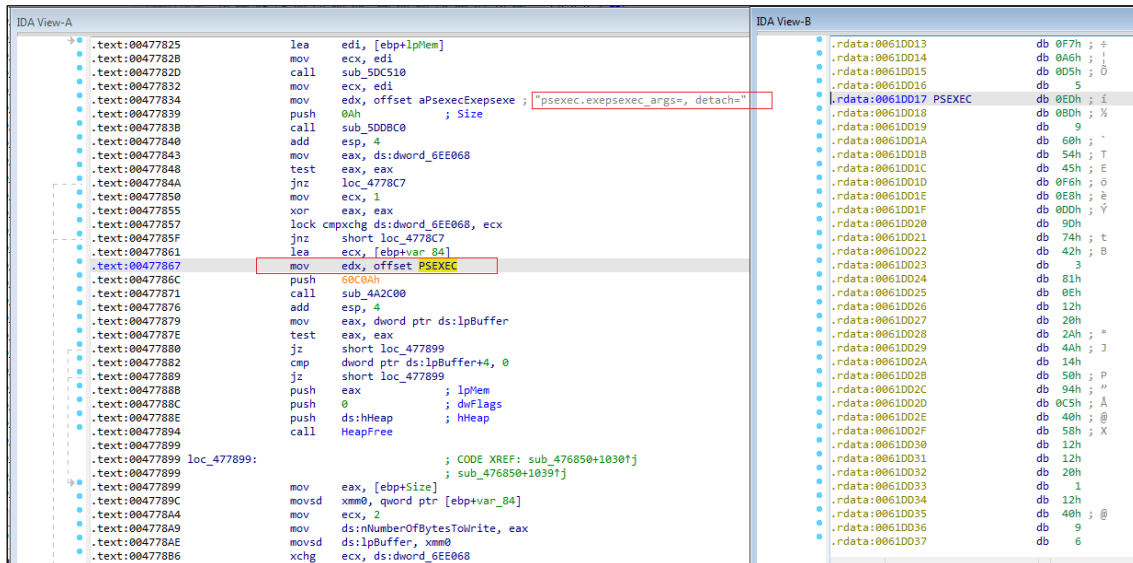


Figura 15. Propagación ARP/NetBIOS

La versión actual dispone de una versión comprimida de PsExec^[12] para poder moverse lateralmente a otros equipos de la red:



IDA View-A:

```

.text:00477825 lea edi,[ebp+lpMem]
.text:00477828 mov ecx,edi
.text:0047782D call sub_50C510
.text:00477832 mov ecx,edi
.text:00477834 mov edx,offset aPsexecExepsex ; "psexec.exe"
.text:00477839 push 0Ah ; Size
.text:0047783B call sub_50D8C0
.text:00477840 add esp,4
.text:00477843 mov eax,ds:dword_6EE068
.text:00477848 test eax,eax
.text:0047784A jnz loc_4778C7
.text:00477850 mov ecx,1
.text:00477855 xor eax,eax
.text:0047785F lock cmpxchg ds:dword_6EE068,ecx
.text:00477861 jnz short loc_4778C7
.text:00477863 lea ecx,[ebp+var_84]
.text:00477865 mov edx,offset PSEXEC
.text:00477867 push 60C0Ah
.text:00477871 call sub_4A2C00
.text:00477876 add esp,4
.text:00477879 mov eax,dword ptr ds:lpBuffer
.text:0047787E test eax,eax
.text:00477880 jz short loc_477899
.text:00477882 cmp dword ptr ds:lpBuffer+4,0
.text:00477885 jz short loc_477899
.text:00477888 push eax ; lpMem
.text:0047788C push 0 ; dwFlags
.text:0047788E push ds:hHeap ; hHeap
.text:00477894 call HeapFree
.text:00477899 loc_477899: ; CODE XREF: sub_476850+1030fj
; sub_476850+1039fj
.text:00477899 mov eax,[ebp+Size]
.text:0047789C movsd xmm0,qword ptr [ebp+var_84]
.text:004778A4 mov ecx,2
.text:004778A9 mov ds:NumberOfBytesToWrite,eax
.text:004778AE movsd ecx,ds:lpBuffer,xmm0
.text:004778B0 xchg ecx,ds:dword_6EE068
  
```

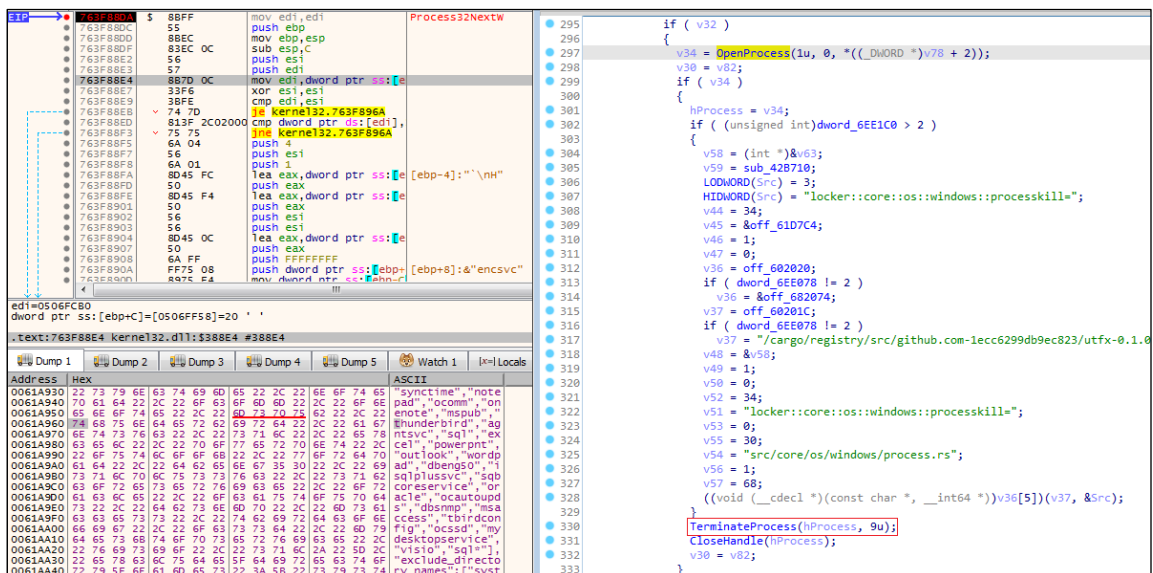
IDA View-B:

```

.rdata:00610D13 db 0F7h ; +
.rdata:00610D14 db 0A6h ; !
.rdata:00610D15 db 0D5h ; 0
.rdata:00610D16 db 5 ;
.rdata:00610D17 PSEXEC db 0EDh ; i
.rdata:00610D18 db 0Dh ; %
.rdata:00610D19 db 9 ;
.rdata:00610D1A db 60h ; '
.rdata:00610D1B db 54h ; T
.rdata:00610D1C db 45h ; E
.rdata:00610D1D db 0F6h ; 0
.rdata:00610D1E db 0E8h ; e
.rdata:00610D1F db 0Dh ; Y
.rdata:00610D20 db 9Dh ;
.rdata:00610D21 db 74h ; t
.rdata:00610D22 db 42h ; B
.rdata:00610D23 db 3 ;
.rdata:00610D24 db 81h ;
.rdata:00610D25 db 0Eh ;
.rdata:00610D26 db 12h ;
.rdata:00610D27 db 20h ;
.rdata:00610D28 db 2Ah ; "
.rdata:00610D29 db 4Ah ; J
.rdata:00610D2A db 14h ;
.rdata:00610D2B db 50h ; P
.rdata:00610D2C db 94h ; "
.rdata:00610D2D db 0C5h ; A
.rdata:00610D2E db 40h ; @
.rdata:00610D2F db 58h ; X
.rdata:00610D30 db 12h ;
.rdata:00610D31 db 12h ;
.rdata:00610D32 db 20h ;
.rdata:00610D33 db 1 ;
.rdata:00610D34 db 12h ;
.rdata:00610D35 db 40h ; @
.rdata:00610D36 db 9 ;
.rdata:00610D37 db 6 ;
  
```

Figura 16. PsExec embebido

El código dañino se asegurará de finalizar un conjunto de servicios y procesos que puedan interferir con el proceso de infección: herramientas de seguridad/monitorización, procesos/servicios que puedan tener abiertos ficheros, etc. Para recorrer los binarios en ejecución se apoyará en las API *CreateToolhelp32Snapshot* y *Process32NextW* finalizando aquellos (vía *TerminateProcess*) que coincidan con los definidos en el fichero de configuración.



Assembly code (left):

```

763F88D0 8BFF 0C mov edi,edi
763F88D1 8BEC 0C mov ebp,esp
763F88D2 56 0C sub esp,C
763F88D3 57 0C push edi
763F88D4 8B7D 0C mov edi,dword ptr ss:[ebp+edi]
763F88D5 3BF5 74 7D cmp edi,esi
763F88D6 813F 2C020000 cmp dword ptr edi:[edi],0
763F88D7 75 75 jnz short loc_763F88E4
763F88D8 6A 04 push 4
763F88D9 56 0C push esi
763F88DA 6A 01 push 1
763F88DB 6A 01 push 1
763F88DC 6A 01 push 1
763F88DD 6A 01 push 1
763F88DE 6A 01 push 1
763F88DF 6A 01 push 1
763F88E0 6A 01 push 1
763F88E1 6A 01 push 1
763F88E2 6A 01 push 1
763F88E3 6A 01 push 1
763F88E4 6A 01 push 1
763F88E5 6A 01 push 1
763F88E6 6A 01 push 1
763F88E7 6A 01 push 1
763F88E8 6A 01 push 1
763F88E9 6A 01 push 1
763F88EA 6A 01 push 1
763F88EB 6A 01 push 1
763F88EC 6A 01 push 1
763F88ED 6A 01 push 1
763F88EE 6A 01 push 1
763F88EF 6A 01 push 1
763F88F0 6A 01 push 1
763F88F1 6A 01 push 1
763F88F2 6A 01 push 1
763F88F3 6A 01 push 1
763F88F4 6A 01 push 1
763F88F5 6A 01 push 1
763F88F6 6A 01 push 1
763F88F7 6A 01 push 1
763F88F8 6A 01 push 1
763F88F9 6A 01 push 1
763F88FA 6A 01 push 1
763F88FB 6A 01 push 1
763F88FC 6A 01 push 1
763F88FD 6A 01 push 1
763F88FE 6A 01 push 1
763F88FF 6A 01 push 1
763F8900 6A 01 push 1
763F8901 6A 01 push 1
763F8902 6A 01 push 1
763F8903 6A 01 push 1
763F8904 6A 01 push 1
763F8905 6A 01 push 1
763F8906 6A 01 push 1
763F8907 6A 01 push 1
763F8908 6A 01 push 1
763F8909 6A 01 push 1
763F890A 6A 01 push 1
763F890B 6A 01 push 1
763F890C 6A 01 push 1
763F890D 6A 01 push 1
763F890E 6A 01 push 1
763F890F 6A 01 push 1
763F8910 6A 01 push 1
763F8911 6A 01 push 1
763F8912 6A 01 push 1
763F8913 6A 01 push 1
763F8914 6A 01 push 1
763F8915 6A 01 push 1
763F8916 6A 01 push 1
763F8917 6A 01 push 1
763F8918 6A 01 push 1
763F8919 6A 01 push 1
763F891A 6A 01 push 1
763F891B 6A 01 push 1
763F891C 6A 01 push 1
763F891D 6A 01 push 1
763F891E 6A 01 push 1
763F891F 6A 01 push 1
763F8920 6A 01 push 1
763F8921 6A 01 push 1
763F8922 6A 01 push 1
763F8923 6A 01 push 1
763F8924 6A 01 push 1
763F8925 6A 01 push 1
763F8926 6A 01 push 1
763F8927 6A 01 push 1
763F8928 6A 01 push 1
763F8929 6A 01 push 1
763F892A 6A 01 push 1
763F892B 6A 01 push 1
763F892C 6A 01 push 1
763F892D 6A 01 push 1
763F892E 6A 01 push 1
763F892F 6A 01 push 1
763F8930 6A 01 push 1
763F8931 6A 01 push 1
763F8932 6A 01 push 1
763F8933 6A 01 push 1
763F8934 6A 01 push 1
763F8935 6A 01 push 1
763F8936 6A 01 push 1
763F8937 6A 01 push 1
763F8938 6A 01 push 1
763F8939 6A 01 push 1
763F893A 6A 01 push 1
763F893B 6A 01 push 1
763F893C 6A 01 push 1
763F893D 6A 01 push 1
763F893E 6A 01 push 1
763F893F 6A 01 push 1
763F8940 6A 01 push 1
763F8941 6A 01 push 1
763F8942 6A 01 push 1
763F8943 6A 01 push 1
763F8944 6A 01 push 1
763F8945 6A 01 push 1
763F8946 6A 01 push 1
763F8947 6A 01 push 1
763F8948 6A 01 push 1
763F8949 6A 01 push 1
763F894A 6A 01 push 1
763F894B 6A 01 push 1
763F894C 6A 01 push 1
763F894D 6A 01 push 1
763F894E 6A 01 push 1
763F894F 6A 01 push 1
763F8950 6A 01 push 1
763F8951 6A 01 push 1
763F8952 6A 01 push 1
763F8953 6A 01 push 1
763F8954 6A 01 push 1
763F8955 6A 01 push 1
763F8956 6A 01 push 1
763F8957 6A 01 push 1
763F8958 6A 01 push 1
763F8959 6A 01 push 1
763F895A 6A 01 push 1
763F895B 6A 01 push 1
763F895C 6A 01 push 1
763F895D 6A 01 push 1
763F895E 6A 01 push 1
763F895F 6A 01 push 1
763F8960 6A 01 push 1
763F8961 6A 01 push 1
763F8962 6A 01 push 1
763F8963 6A 01 push 1
763F8964 6A 01 push 1
763F8965 6A 01 push 1
763F8966 6A 01 push 1
763F8967 6A 01 push 1
763F8968 6A 01 push 1
763F8969 6A 01 push 1
763F896A 6A 01 push 1
763F896B 6A 01 push 1
763F896C 6A 01 push 1
763F896D 6A 01 push 1
763F896E 6A 01 push 1
763F896F 6A 01 push 1
763F8970 6A 01 push 1
763F8971 6A 01 push 1
763F8972 6A 01 push 1
763F8973 6A 01 push 1
763F8974 6A 01 push 1
763F8975 6A 01 push 1
763F8976 6A 01 push 1
763F8977 6A 01 push 1
763F8978 6A 01 push 1
763F8979 6A 01 push 1
763F897A 6A 01 push 1
763F897B 6A 01 push 1
763F897C 6A 01 push 1
763F897D 6A 01 push 1
763F897E 6A 01 push 1
763F897F 6A 01 push 1
763F8980 6A 01 push 1
763F8981 6A 01 push 1
763F8982 6A 01 push 1
763F8983 6A 01 push 1
763F8984 6A 01 push 1
763F8985 6A 01 push 1
763F8986 6A 01 push 1
763F8987 6A 01 push 1
763F8988 6A 01 push 1
763F8989 6A 01 push 1
763F898A 6A 01 push 1
763F898B 6A 01 push 1
763F898C 6A 01 push 1
763F898D 6A 01 push 1
763F898E 6A 01 push 1
763F898F 6A 01 push 1
763F8990 6A 01 push 1
763F8991 6A 01 push 1
763F8992 6A 01 push 1
763F8993 6A 01 push 1
763F8994 6A 01 push 1
763F8995 6A 01 push 1
763F8996 6A 01 push 1
763F8997 6A 01 push 1
763F8998 6A 01 push 1
763F8999 6A 01 push 1
763F899A 6A 01 push 1
763F899B 6A 01 push 1
763F899C 6A 01 push 1
763F899D 6A 01 push 1
763F899E 6A 01 push 1
763F899F 6A 01 push 1
763F89A0 6A 01 push 1
763F89A1 6A 01 push 1
763F89A2 6A 01 push 1
763F89A3 6A 01 push 1
763F89A4 6A 01 push 1
763F89A5 6A 01 push 1
763F89A6 6A 01 push 1
763F89A7 6A 01 push 1
763F89A8 6A 01 push 1
763F89A9 6A 01 push 1
763F89AA 6A 01 push 1
763F89AB 6A 01 push 1
763F89AC 6A 01 push 1
763F89AD 6A 01 push 1
763F89AE 6A 01 push 1
763F89AF 6A 01 push 1
763F89B0 6A 01 push 1
763F89B1 6A 01 push 1
763F89B2 6A 01 push 1
763F89B3 6A 01 push 1
763F89B4 6A 01 push 1
763F89B5 6A 01 push 1
763F89B6 6A 01 push 1
763F89B7 6A 01 push 1
763F89B8 6A 01 push 1
763F89B9 6A 01 push 1
763F89BA 6A 01 push 1
763F89BB 6A 01 push 1
763F89BC 6A 01 push 1
763F89BD 6A 01 push 1
763F89BE 6A 01 push 1
763F89BF 6A 01 push 1
763F89C0 6A 01 push 1
763F89C1 6A 01 push 1
763F89C2 6A 01 push 1
763F89C3 6A 01 push 1
763F89C4 6A 01 push 1
763F89C5 6A 01 push 1
763F89C6 6A 01 push 1
763F89C7 6A 01 push 1
763F89C8 6A 01 push 1
763F89C9 6A 01 push 1
763F89CA 6A 01 push 1
763F89CB 6A 01 push 1
763F89CC 6A 01 push 1
763F89CD 6A 01 push 1
763F89CE 6A 01 push 1
763F89CF 6A 01 push 1
763F89D0 6A 01 push 1
763F89D1 6A 01 push 1
763F89D2 6A 01 push 1
763F89D3 6A 01 push 1
763F89D4 6A 01 push 1
763F89D5 6A 01 push 1
763F89D6 6A 01 push 1
763F89D7 6A 01 push 1
763F89D8 6A 01 push 1
763F89D9 6A 01 push 1
763F89DA 6A 01 push 1
763F89DB 6A 01 push 1
763F89DC 6A 01 push 1
763F89DD 6A 01 push 1
763F89DE 6A 01 push 1
763F89DF 6A 01 push 1
763F89E0 6A 01 push 1
763F89E1 6A 01 push 1
763F89E2 6A 01 push 1
763F89E3 6A 01 push 1
763F89E4 6A 01 push 1
763F89E5 6A 01 push 1
763F89E6 6A 01 push 1
763F89E7 6A 01 push 1
763F89E8 6A 01 push 1
763F89E9 6A 01 push 1
763F89EA 6A 01 push 1
763F89EB 6A 01 push 1
763F89EC 6A 01 push 1
763F89ED 6A 01 push 1
763F89EE 6A 01 push 1
763F89EF 6A 01 push 1
763F89F0 6A 01 push 1
763F89F1 6A 01 push 1
763F89F2 6A 01 push 1
763F89F3 6A 01 push 1
763F89F4 6A 01 push 1
763F89F5 6A 01 push 1
763F89F6 6A 01 push 1
763F89F7 6A 01 push 1
763F89F8 6A 01 push 1
763F89F9 6A 01 push 1
763F89FA 6A 01 push 1
763F89FB 6A 01 push 1
763F89FC 6A 01 push 1
763F89FD 6A 01 push 1
763F89FE 6A 01 push 1
763F89FF 6A 01 push 1
763F8A00 6A 01 push 1
763F8A01 6A 01 push 1
763F8A02 6A 01 push 1
763F8A03 6A 01 push 1
763F8A04 6A 01 push 1
763F8A05 6A 01 push 1
763F8A06 6A 01 push 1
763F8A07 6A 01 push 1
763F8A08 6A 01 push 1
763F8A09 6A 01 push 1
763F8A0A 6A 01 push 1
763F8A0B 6A 01 push 1
763F8A0C 6A 01 push 1
763F8A0D 6A 01 push 1
763F8A0E 6A 01 push 1
763F8A0F 6A 01 push 1
763F8A10 6A 01 push 1
763F8A11 6A 01 push 1
763F8A12 6A 01 push 1
763F8A13 6A 01 push 1
763F8A14 6A 01 push 1
763F8A15 6A 01 push 1
763F8A16 6A 01 push 1
763F8A17 6A 01 push 1
763F8A18 6A 01 push 1
763F8A19 6A 01 push 1
763F8A1A 6A 01 push 1
763F8A1B 6A 01 push 1
763F8A1C 6A 01 push 1
763F8A1D 6A 01 push 1
763F8A1E 6A 01 push 1
763F8A1F 6A 01 push 1
763F8A20 6A 01 push 1
763F8A21 6A 01 push 1
763F8A22 6A 01 push 1
763F8A23 6A 01 push 1
763F8A24 6A 01 push 1
763F8A25 6A 01 push 1
763F8A26 6A 01 push 1
763F8A27 6A 01 push 1
763F8A28 6A 01 push 1
763F8A29 6A 01 push 1
763F8A2A 6A 01 push 1
763F8A2B 6A 01 push 1
763F8A2C 6A 01 push 1
763F8A2D 6A 01 push 1
763F8A2E 6A 01 push 1
763F8A2F 6A 01 push 1
763F8A30 6A 01 push 1
763F8A31 6A 01 push 1
763F8A32 6A 01 push 1
763F8A33 6A 01 push 1
763F8A34 6A 01 push 1
763F8A35 6A 01 push 1
763F8A36 6A 01 push 1
763F8A37 6A 01 push 1
763F8A38 6A 01 push 1
763F8A39 6A 01 push 1
763F8A3A 6A 01 push 1
763F8A3B 6A 01 push 1
763F8A3C 6A 01 push 1
763F8A3D 6A 01 push 1
763F8A3E 6A 01 push 1
763F8A3F 6A 01 push 1
763F8A40 6A 01 push 1
763F8A41 6A 01 push 1
763F8A42 6A 01 push 1
763F8A43 6A 01 push 1
763F8A44 6A 01 push 1
763F8A45 6A 01 push 1
763F8A46 6A 01 push 1
763F8A47 6A 01 push 1
763F8A48 6A 01 push 1
763F8A49 6A 01 push 1
763F8A4A 6A 01 push 1
763F8A4B 6A 01 push 1
763F8A4C 6A 01 push 1
763F8A4D 6A 01 push 1
763F8A4E 6A 01 push 1
763F8A4F 6A 01 push 1
763F8A50 6A 01 push 1
763F8A51 6A 01 push 1
763F8A52 6A 01 push 1
763F8A53 6A 01 push 1
763F8A54 6A 01 push 1
763F8A55 6A 01 push 1
763F8A56 6A 01 push 1
763F8A57 6A 01 push 1
763F8A58 6A 01 push 1
763F8A59 6A 01 push 1
763F8A5A 6A 01 push 1
763F8A5B 6A 01 push 1
763F8A5C 6A 01 push 1
763F8A5D 6A 01 push 1
763F8A5E 6A 01 push 1
763F8A5F 6A 01 push 1
763F8A60 6A 01 push 1
763F8A61 6A 01 push 1
763F8A62 6A 01 push 1
763F8A63 6A 01 push 1
763F8A64 6A 01 push 1
763F8A65 6A 01 push 1
763F8A66 6A 01 push 1
763F8A67 6A 01 push 1
763F8A68 6A 01 push 1
763F8A69 6A 01 push 1
763F8A6A 6A 01 push 1
763F8A6B 6A 01 push 1
763F8A6C 6A 01 push 1
763F8A6D 6A 01 push 1
763F8A6E 6A 01 push 1
763F8A6F 6A 01 push 1
763F8A70 6A 01 push 1
763F8A71 6A 01 push 1
763F8A72 6A 01 push 1
763F8A73 6A 01 push 1
763F8A74 6A 01 push 1
763F8A75 6A 01 push 1
763F8A76 6A 01 push 1
763F8A77 6A 01 push 1
763F8A78 6A 01 push 1
763F8A79 6A 01 push 1
763F8A7A 6A 01 push 1
763F8A7B 6A 01 push 1
763F8A7C 6A 01 push 1
763F8A7D 6A 01 push 1
763F8A7E 6A 01 push 1
763F8A7F 6A 01 push 1
763F8A80 6A 01 push 1
763F8A81 6A 01 push 1
763F8A82 6A 01 push 1
763F8A83 6A 01 push 1
763F8A84 6A 01 push 1
763F8A85 6A 01 push 1
763F8A86 6A 01 push 1
763F8A87 6A 01 push 1
763F8A88 6A 01 push 1
763F8A89 6A 01 push 1
763F8A8A 6A 01 push 1
763F8A8B 6A 01 push 1
763F8A8C 6A 01 push 1
763F8A8D 6A 01 push 1
763F8A8E 6A 01 push 1
763F8A8F 6A 01 push 1
763F8A90 6A 01 push 1
763F8A91 6A 01 push 1
763F8A92 6A 01 push 1
763F8A93 6A 01 push 1
763F8A94 6A 01 push 1
763F8A95 6A 01 push 1
763F8A96 6A 01 push 1
763F8A97 6A 01 push 1
763F8A98 6A 01 push 1
763F8A99 6A 01 push 1
763F8A9A 6A 01 push 1
763F8A9B 6A 01 push 1
763F8A9C 6A 01 push 1
763F8A9D 6A 01 push 1
763F8A9E 6A 01 push 1
763F8A9F 6A 01 push 1
763F8AA0 6A 01 push 1
763F8AA1 6A 01 push 1
763F8AA2 6A 01 push 1
763F8AA3 6A 01 push 1
763F8AA4 6A 01 push 1
763F8AA5 6A 01 push 1
763F8AA6 6A 01 push 1
763F8AA7 6A 01 push 1
763F8AA8 6A 01 push 1
763F8AA9 6A 01 push 1
763F8AAA 6A 01 push 1
763F8AAB 6A 01 push 1
763F8AAC 6A 01 push 1
763F8AAD 6A 01 push 1
763F8AAE 6A 01 push 1
763F8AAF 6A 01 push 1
763F8AAG 6A 01 push 1
763F8AAH 6A 01 push 1
763F8AAI 6A 01 push 1
763F8AAJ 6A 01 push 1
763F8AAK 6A 01 push 1
763F8AAL 6A 01 push 1
763F8AAM 6A 01 push 1
763F8AAN 6A 01 push 1
763F8AAO 6A 01 push 1
763F8AAP 6A 01 push 1
763F8AAQ 6A 01 push 1
763F8AAR 6A 01 push 1
763F8AAS 6A 01 push 1
763F8AAT 6A 01 push 1
763F8AAU 6A 01 push 1
763F8AAV 6A 01 push 1
763F8AAW 6A 01 push 1
763F8AAX 6A 01 push 1
763F8AAY 6A 01 push 1
763F8AAZ 6A 01 push 1
763F8AB0 6A 01 push 1
763F8AB1 6A 01 push 1
763F8AB2 6A 01 push 1
763F8AB3 6A 01 push 1
763F8AB4 6A 01 push 1
763F8AB5 6A 01 push 1
763F8AB6 6A 01 push 1
763F8AB7 6A 01 push 1
763F8AB8 6A 01 push 1
763F8AB9 6A 01 push 1
763F8ABA 6A 01 push 1
763F8ABB 6A 01 push 1
763F8ABC 6A 01 push 1
763F8ABD 6A 01 push 1
763F8ABE 6A 01 push 1
763F8ABF 6A 01 push 1
763F8AC0 6A 01 push 1
763F8AC1 6A 01 push 1
763F8AC2 6A 01 push 1
763F8AC3 6A 01 push 1
763F8AC4 6A 01 push 1
763F8AC5 6A 01 push 1
763F8AC6 6A 01 push 1
763F8AC7 6A 01 push 1
763F8AC8 6A 01 push 1
763F8AC9 6A 01 push 1
763F8ACA 6A 01 push 1
763F8ACB 6A 01 push 1
763F8ACC 6A 01 push 1
763F8ACD 6A 01 push 1
763F8ACE 6A 01 push 1
763F8ACF 6A 01 push 1
763F8AD0 6A 01 push 1
763F8AD1 6A 01 push 1
763F8AD2 6A 01 push 1
763F8AD3 6A 01 push 1
763F8AD4 6A 01 push 1
763F8AD5 6A 01 push 1
763F8AD6 6A 01 push 1
763F8AD7 6A 01 push 1
763F8AD8 6A 01 push 1
763F8AD9 6A 01 push 1
763F8ADA 6A 01 push 1
763F8ADB 6A 01 push 1
763F8ADC 6A 01 push 1
763F8ADE 6A 01 push 1
763F8ADF 6A 01 push 1
763F8AE0 6A 01 push 1
763F8AE1 6A 01 push 1
763F8AE2 6A 01 push 1
763F8AE3 6A 01 push 1
763F8AE4 6A 01 push 1
763F8AE5 6A 01 push 1
763F8AE6 6A 01 push 1
763F8AE7 6A 01 push 1
763F8AE8 6A 01 push 1
763F8AE9 6A 01 push 1
763F8AEA 6A 01 push 1
763F8AEB 6A 01 push 1
763F8AEC 6A 01 push 1
763F8AED 6A 01 push 1
763F8AEE 6A 01 push 1
763F8AEF 6A 01 push 1
763F8AF0 6A 01 push 1
763F8AF1 6A 01 push 1
763F8AF2 6A 01 push 1
763F8AF3 6A 01 push 1
763F8AF4 6A 01 push 1
763F8AF5 6A 01 push 1
763F8AF6 6A 01 push 1
763F8AF7 6A 01 push 1
763F8AF8 6A 01 push 1
763F8AF9 6A 01 push 1
763F8AFA 6A 01 push 1
763F8AFB 6A 01 push 1
763F8AFC 6A 01 push 1
763F8AFD 6A 01 push 1
763F8AFE 6A 01 push 1
763F8AFF 6A 01 push 1
763F8B00 6A 01 push 1
763F8B01 6A 01 push 1
763F8B02 6A 01 push 1
763F8B03 6A 01 push 1
763F8B04 6A 01 push 1
763F8B05 6A 01 push 1
763F8B06 6A 01 push 1
763F8B07 6A 01 push 1
763F8B08 6A 01 push 1
76
```

“EnumServicesStatusExW”. Aquellos existentes en el fichero de configuración serán finalizados mediante una notificación SERVICE_CONTROL_STOP vía “ControlService”.

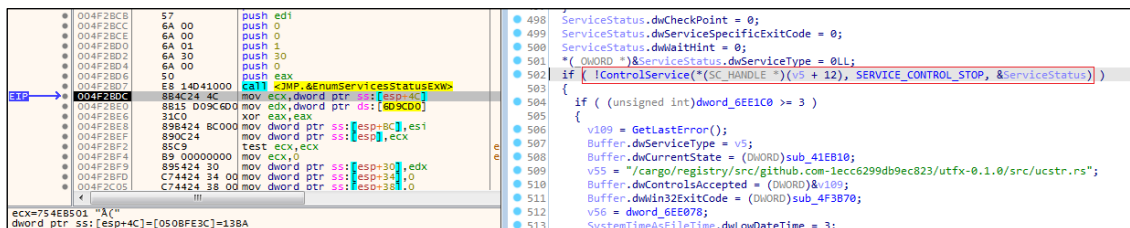


Figura 18. Finalización de servicios

BlackCat recorrerá todos los volúmenes existentes e intentará montar unidades actualmente desmontados utilizando las APIs:

GetDriveTypeW, GetVolumePathNamesForVolumeNameW, SetVolumeMountPointW

Estas acciones permitirán crear una lista con los dispositivos que se recorrerán posteriormente para proceder con el cifrado de ficheros.

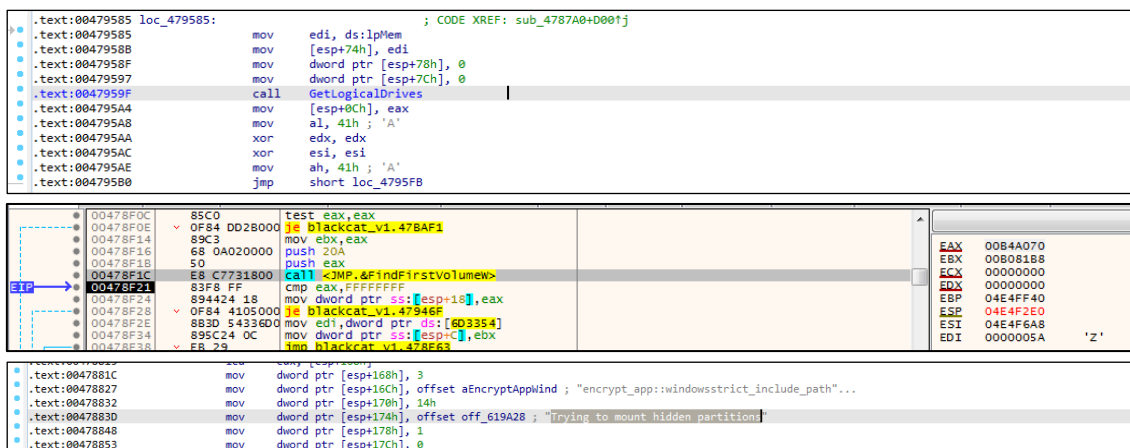


Figura 19. Identificación de unidades / volúmenes

El conjunto de acciones previamente descrito generará un árbol de procesos similar al mostrado en la siguiente imagen (el cual podrá variar en función de los permisos y los argumentos proporcionados por la línea de comandos).

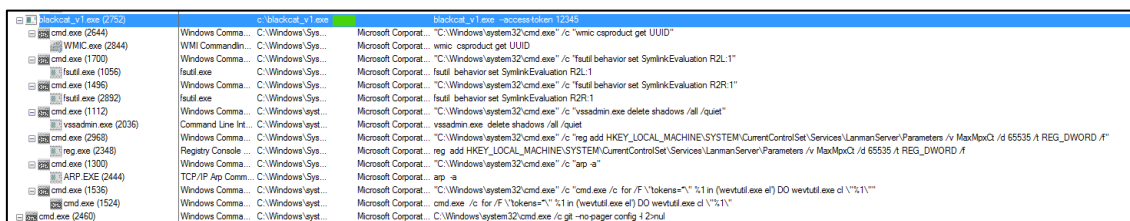


Figura 20. Proceso de infección

En cada directorio afectado por el código dañino se generará un fichero de texto (*RECOVER-<EXTENSION>-FILES.txt*) con las instrucciones para la recuperación de los ficheros cifrados y en donde se podrán encontrar las direcciones “.onion” vinculadas con el grupo criminal.

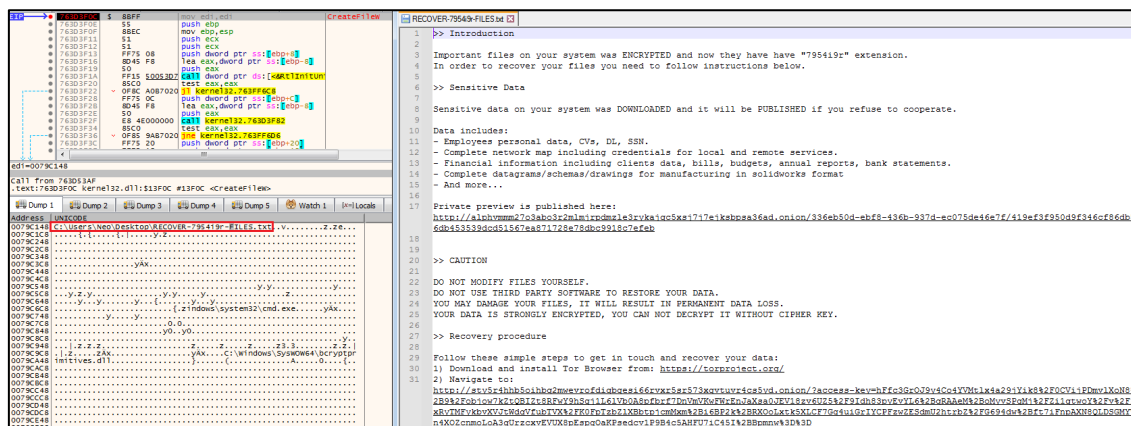


Figura 21. Fichero de recuperación

El código dañino recorre el sistema de archivos mediante las API *FindFirstFileW* y *FindNextFileW* excluyendo los directorios/ficheros y extensiones definidos en su fichero de configuración (por ejemplo: "desktop.ini", "autorun.inf", "ntldr", "bootsect.bak", "thumbs.db", "boot.ini", etc.). Durante el cifrado de ficheros, generará archivos intermedios bajo la sintaxis *checkpoint-<nombre de archivo cifrado>*. La extensión del mismo vendrá definida en el propio fichero de configuración ("7954i9r" para la muestra actual)

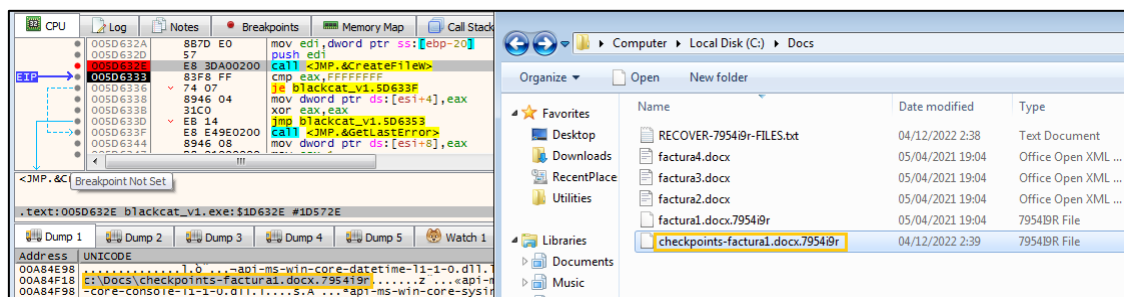


Figura 22. Generación ficheros intermedios

El valor "Best" en la directiva "Default File Encryption Cipher" del fichero de configuración instruye al código dañino a emplear el conjunto de instrucciones AES-NI 128 introducido en la familia de procesadores Intel® Core™ 2010. En la siguiente imagen se muestra la función que implementa dicha lógica para cifrar el contenido de los ficheros afectados:

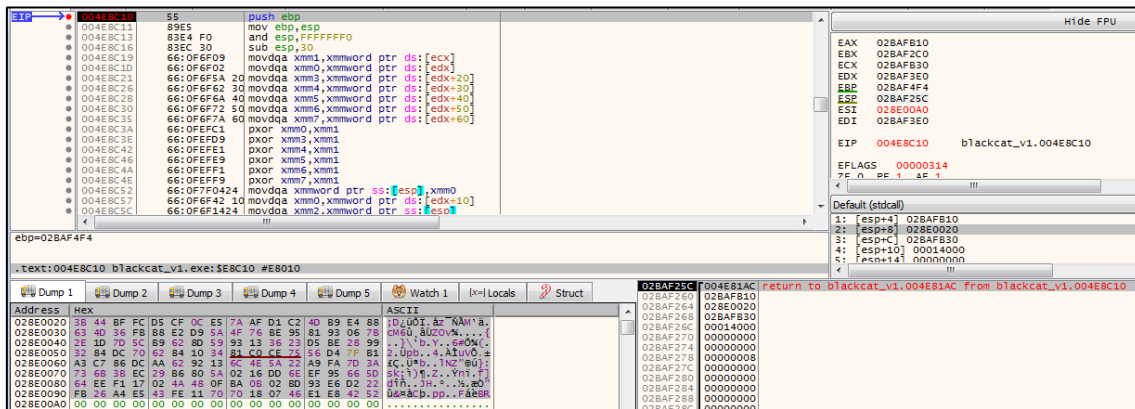


Figura 23. Instrucciones AES-NI (cifrado AES)

Los bloques de datos cifrados se irán escribiendo al fichero correspondiente vía `WriteFile`. La clave AES será posteriormente cifrada con la `public key` RSA 2048 (embebida en el fichero de configuración) e incorporada al final del fichero utilizando cierto delimitador de 4 bytes antes y después de dicho bloque ("19 47 BC C3").

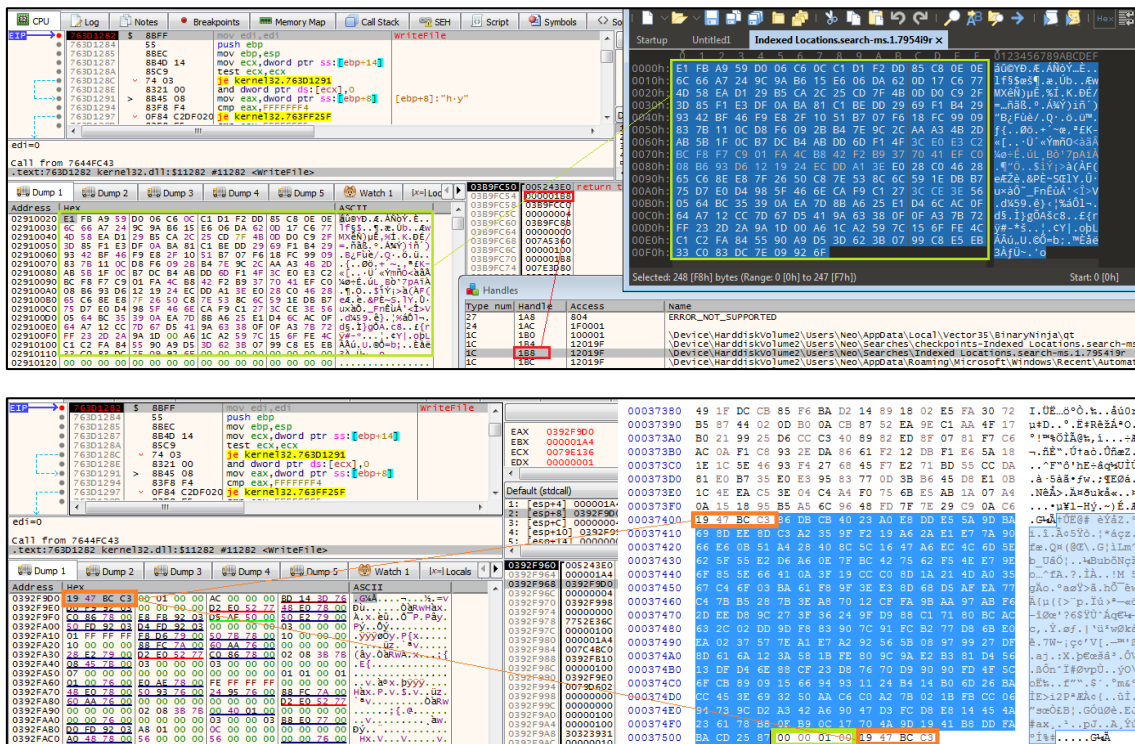


Figura 24. Clave AES cifrada con RSA / Delimitador "19 47 BC C3"

Estas acciones se llevarán a cabo de forma recursiva en todos los directorios del sistema (o los especificados por medio del parámetro `-p` o `-paths`).

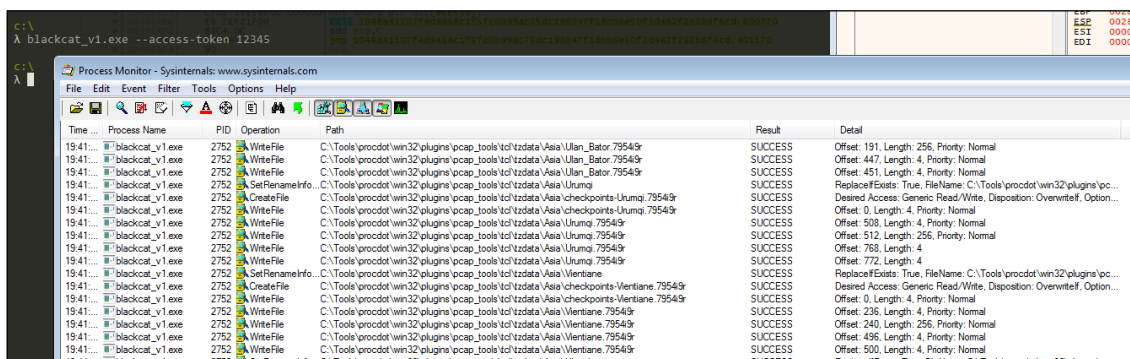


Figura 25. Proceso de cifrado

El ransomware podrá modificar el fondo de escritorio haciendo uso de la función `SystemParametersInfoW` con el parámetro `0x14` (`SPI_SETDESKWALLPAPER`):

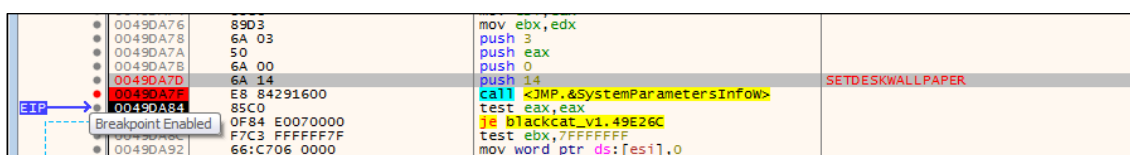


Figura 26. Cambio de fondo de escritorio

5. MITIGACIÓN

La manera más estratégica para contener y reducir el impacto del *ransomware* es trabajar de forma paralela en el aislado de redes/VLAN que conforman la entidad afectada (con el objetivo de contener los segmentos de red con equipos infectados y evitar su expansión) y en el rotado de contraseñas en el dominio. Dicho rotado debe incluir las cuentas locales de administrador (es importante que sean únicas para cada equipo) así como la cuenta KRBTGT del dominio (entornos Windows). Téngase en cuenta que estas medidas posiblemente interfieran con el correcto funcionamiento del dominio o redes afectadas y puedan causar diversos imprevistos (por ejemplo, el reinicio de máquinas); no obstante, permitiría contener la amenaza de una manera resolutive.

Desde un punto de vista preventivo es importante estar al día de las TTP (Tácticas Técnicas y Procedimientos) empleadas por este tipo de *Threat Actors* en las diversas fases del *kill Chain*. Consúltase el apartado de referencias para conocer^[13] las herramientas y técnicas más habituales empleadas por grupos criminales que emplean este ransomware para conseguir acceso a los sistemas y escalar sus ataques hasta comprometer prácticamente toda la organización. Estar al corriente de esta información e implementar medidas que mitiguen este tipo de estrategias ayudarán significativamente a prevenir y reducir el *dwell time* durante un incidente.

6. REGLAS DE DETECCIÓN

6.1 REGLA YARA

```
rule blackcat_v1{
  meta:
    description = "BlackCat/BlackCat"
    author = "CCN-CERT"
    version = "1.0"
    date = "2022-12-01"
    hash1 = "93f34fb60a180a3a80ca758b97c2e551"
  strings:
    $x1 = "${ACCESS_KEY}${EXTENSION}${NOTE_FILE_NAME}" ascii
    $x2 = "Follow these simple steps to get in touch and recover your data" ascii
    $x3 = "\"config_id\": \"\", \"public_key\": \"MIIBIjANBgkqhkiG9\" ascii
    $x4 = "psexec.exe psexec_args=, detach=" ascii
    $x5 = ".onion/?access-key=${ACCESS_KEY}" ascii
    $x6 = "access-tokenpathsno-netno-propno-wallno-vm-kill" ascii
    $x7 = "uac_bypass::shell_exec=" ascii
    $x8 = "--no-prop-servers--propagatedpropagate::server=" ascii
    $x9 = "service::stop_recursive=L" ascii
    $x10 = "KeyInvalid RSA Private KeyChaCha20Aes" ascii

  condition:
    uint16(0) == 0x5A4D and 1 of ($x*) and (pe.number_of_sections > 6) and filesize > 2MB and filesize < 5MB
}
```

Múltiples reglas referenciadas desde el servicio Malware Bazaar^[14] detectarían también la muestra actual; por ejemplo:

```
rule RAN_ALPHV_Dec_2021_1
{
  meta:
    description = "Detect AlphV ransomware (Nov and Dec 2021)"
    author = "Arkbird_SOLG"
    date = "2021-12-09"
    reference = "Internal Research"
    hash1 = "3d7cf20ca6476e14e0a026f9bdd8ff1f26995cdc5854c3adb41a6135ef11ba83"
    hash2 = "7e363b5f1ba373782261713fa99e8bbc35ddda97e48799c4eb28f17989da8d8e"
    hash3 = "cefea76dfdbb48cfe1a3db2c8df34e898e29bec9b2c13e79ef40655c637833ae"
    hash4 = "731adcf2d7fb61a8335e23dbee2436249e5d5753977ec465754c6b699e9bf161"
    tlp = "white"
    adversary = "BlackCat"
  strings:
    $s1 = { ff b4 24 [2] 00 00 6a 00 ff 35 ?? e1 ?? 00 e8 [3] 00 8d 8c 24 [2] 00 00 ba [3] 00 68 c0 1f 00 00 e8 [3] ff 83 c4 04 ?? bc 24 [2] 00 00 }
    $s2 = { 85 f6 74 47 8b 3d ?? e1 ?? 00 85 ff 0f 85 81 00 00 00 eb 60 68 [3] 00 6a 00 6a 00 e8 [2] 04 00 85 c0 0f 84 99 01 00 00 89 c1 31 c0 f0 0f b1 0d ?? e1 ?? 00 0f 84 f0 fe ff ff 89 c6 51 e8 [2] 04 00 89 f1 e9 e1 fe ff ff 68 [3] 00 ff 35 ?? e1 ?? 00 e8 [2] 04 00 85 c0 0f 84 32 03 00 00 89 c6 a3 ?? e1 ?? 00 8b 3d ?? e1 ?? 00 85 ff 75 1f 68 [3] 00 ff 35 ?? e1 ?? 00 e8 [2] 04 00 85 c0 0f 84 09 03 00 00 89 c7 a3 ?? e1 ?? 00 89 74 24 18 e8 [2] 04 00 8b 35 ?? e1 ?? 00 89 44 24 14 85 f6 75 1f 68 [3] 00 ff 35 ?? e1 ?? 00 e8 [2] 04 00 85 c0 0f 84 b8 01 00 00 89 c6 a3 ?? e1 ?? 00 8d 44 24 70 c7 44 24 64 00 00 00 00 c7 44 24 60 00 00 00 00 68 0c 01 00 00 6a 00 50 e8 [2] 04 00 83 }
    $s3 = { 8b 38 89 4d ec 89 55 ?? 74 34 a1 ?? e1 ?? 00 85 c0 75 0e e8 [3] 00 85 c0 74 14 a3 ?? e1 ?? 00 53 6a 00 50 e8 [3] 00 89 c6 85 c0 75 13 89 d9 ba 01 00 00 00 e8 [3] ff 0f 0b be 01 00 00 00 53 57 56 e8 [3] 00 83 c4 0c 8d 04 1e 8d 4d }
    $s4 = { 83 c4 0c c7 45 ?? 00 00 00 00 c7 45 ?? 02 00 00 89 89 75 ?? 8d 45 ?? c7 45 ?? 00 00 00 00 c7 45 ?? 00 00 00 00 6a 10 50 57 e8 [3] 00 83 f8 ff 0f 84 ?? 02 00 00 f6 45 9c ff }
  condition:
    uint16(0) == 0x5A4D and filesize > 300KB and all of ($s*)
}
```

7. REFERENCIAS

[1] Who Wrote the ALPHV/BlackCat Ransomware Strain?

<https://krebsonsecurity.com/2022/01/who-wrote-the-alphv-blackcat-ransomware-strain/>

[2] FBI: BlackCat/ALPHV Ransomware Indicators of Compromise

<https://www.ic3.gov/Media/News/2022/220420.pdf>

[3] BlackMatter Ransomware

https://www.cisa.gov/uscert/sites/default/files/publications/Joint-CISA-FBI-NSA_CSA_AA21-291A_BlackMatter_Ransomware.pdf

[4] Lockbit and Black Basta are the most active raas groups as victim count rises

<https://www.trendmicro.com/vinfo/us/security/news/ransomware-by-the-numbers/lockbit-and-black-basta-are-the-most-active-raas-groups-as-victim-count-rises-ransomware-in-q2-and-q3-2022>

[5] Malpedia: Blackcat

<https://malpedia.caad.fkie.fraunhofer.de/details/win.blackcat>

[6] BlackCat Ransomware: Tactics and Techniques from a Targeted Attack

<https://www.netskope.com/blog/blackcat-ransomware-tactics-and-techniques-from-a-targeted-attack>

[7] Github: blackCatConf

<https://github.com/f0wl/blackCatConf>

[8] Wikipedia: ChaCha20

https://en.wikipedia.org/wiki/Salsa20#ChaCha_variant

[9] Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection

<https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/>

[10] ALPHV ransomware gang analysis

<https://www.intrinsec.com/alphv-ransomware-gang-analysis/>

[11] Github: hfiref0x/akagi_41.c

<https://gist.github.com/hfiref0x/196af729106b780db1c73428b5a5d68d>

[12] Noberus: Technical Analysis Shows Sophistication of New Rust-based Ransomware

<https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-alphv-rust-ransomware>

[13] Ransomware Spotlight Blackcat

<https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat>

[14] Malware Bazaar: 93f34fb60a180a3a80ca758b97c2e551

<https://bazaar.abuse.ch/sample/1048a41107f4d9a68c1f5fc0b99ac75dc198047f18bb6e50f3d462f262b8f6cd/#yara>

ANEXO

FICHERO DE CONFIGURACIÓN

```
{
  "config_id": "",
  "public_key":
    "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApw3tWdMaWJvNf2Mejy5H0Y6kuj+IstNpwFyismGDEYhWKPps9c68xl+84o
    6uLKfqPzNvLnSxLVa6DitCjGeKJEQkzN+C1e1KsfzM63jHybREB2hs+dHbqBq4dbamlQcTrrr4mKzuHJ7aok4mlpRx2Un1XOJaodoV7xOH
    O7ui5v6uK39MJ3rvitSEBvv5oIOWDlp3IFmtd6UM6r2nygY1ncAUuasalZgF1Vaz7VXOWyX2ReQHbYWWRCR1qyKMqCbtjT5POXx9B8e
    k1pnU4p65kGe9M794Bhhh20GN24gY5a+zwXwstaNTO9luwd4xjJRQAVsDgjrjktzi27G11Cn6wIDAQAB",
  "extension": "7954i9r",
  "note_file_name": "RECOVER-#{EXTENSION}-FILES.txt",
  "note_full_text": ">> Introduction\n\nImportant files on your system was ENCRYPTED and now they have have \"#{EXTENSION}\"
  extension.\n\nIn order to recover your files you need to follow instructions below.\n\n>> Sensitive Data\n\nSensitive data on your
  system was DOWNLOADED and it will be PUBLISHED if you refuse to cooperate.\n\nData includes:\n- Employees personal data, CVs,
  DL, SSN.\n- Complete network map including credentials for local and remote services.\n- Financial information including clients
  data, bills, budgets, annual reports, bank statements.\n- Complete datagrams/schemas/drawings for manufacturing in solidworks
  format\n- And more...\n\nPrivate preview is published here:
  http://alphvmmm27o3abo3r2mlmjrpdmzle3rykajqc5xsj7j7ejksbpsa36ad.onion/336eb50d-ebf8-436b-937d-
  ec075de46e7f/419ef3f950d9f346cf86db56db453539dcd51567ea871728e78dbc9918c7efeb\n\n>> CAUTION\n\nDO NOT
  MODIFY FILES YOURSELF.\n\nDO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.\n\nYOU MAY DAMAGE YOUR FILES, IT
  WILL RESULT IN PERMANENT DATA LOSS.\n\nYOUR DATA IS STRONGLY ENCRYPTED, YOU CAN NOT DECRYPT IT WITHOUT CIPHER
  KEY.\n\n>> Recovery procedure\n\nFollow these simple steps to get in touch and recover your data:\n1) Download and install Tor
  Browser from: https://torproject.org/\n2) Navigate to:
  http://sty5r4hhb5oihbq2mwewrofdiqbgesi66rvxr5sr573xgvtuvr4cs5yd.onion/?access-key=#{ACCESS_KEY}",
  "note_short_text": "Important files on your system was ENCRYPTED.\nSensitive data on your system was DOWNLOADED. \n\nTo
  recover your files and prevent publishing of sensitive information follow instructions in \"#{NOTE_FILE_NAME}\" file.",
  "default_file_mode": "Auto",
  "default_file_cipher": "Best",
  "credentials": [],
  "kill_services": ["mepocs", "memtas", "veeam", "svc$", "backup", "sql", "vss", "msexchange", "sql*"],
  "kill_processes": ["encsvc", "thebat", "mydesktopqos", "xfssvccn", "firefox", "infopath", "winword", "steam",
  "synctime", "notepad", "ocomm", "onenote", "msspub", "thunderbird", "agntsvc", "sql", "excel", "powerpnt",
  "outlook", "wordpad", "dbeng50", "isqlplussvc", "sqbcoreservice", "oracle", "ocautoupds", "dbsnmp", "msaccess",
  "tbirdconfig", "ocssd", "mydesktopservice", "visio", "sql*"],
  "exclude_directory_names": ["system volume information", "intel", "$windows.~ws", "application data", "$recycle.bin",
  "mozilla", "program files (x86)", "program files", "$windows.~bt", "public", "msocache", "windows", "default", "all
  users", "tor browser", "programdata", "boot", "config.msi", "google", "perflogs", "appdata", "windows.old"],
  "exclude_file_names": [ "desktop.ini", "autorun.inf", "ntldr", "bootsect.bak", "thumbs.db", "boot.ini", "ntuser.dat",
  "iconcache.db", "bootfont.bin", "ntuser.ini", "ntuser.dat.log"],
  "exclude_file_extensions": [ "themepack", "nls", "diagpkg", "msi", "lnk", "exe", "cab", "scr", "bat", "drv", "rtp",
  "msp", "prf", "msc", "ico", "key", "ocx", "diagcab", "diagcfg", "pdb", "wpx", "hlp", "icns", "rom", "dll",
  "msstyles", "mod", "ps1", "ics", "hta", "bin", "cmd", "ani", "386", "lock", "cur", "idx", "sys", "com",
  "deskthemepack", "shs", "ldf", "theme", "mpa", "nomedia", "spl", "cpl", "adv", "icl", "msu"],
  "exclude_file_path_wildcard": [],
  "enable_network_discovery": true,
  "enable_self_propagation": true,
  "enable_set_wallpaper": true,
  "enable_esxi_vm_kill": true,
  "enable_esxi_vm_snapshot_kill": true,
  "strict_include_paths": [],
  "esxi_vm_kill_exclude": []
}
```