CONTEXTO DE LA AMENAZA WHISPERGATE

Autor:

Ángel Luis Rodríguez Martín-Palomino

Índice de contenidos

Términos y acrónimos **3**

Contexto de la amenaza **4**

Resumen Ejecutivo 4

Cadena de Ataque 5

Acceso inicial *5*

Entrega *6*

Instalación *6*

Ejecución y Evasión de Defensas *7*

Fases finales *8*

Acciones **9**

TTPs 9

Mitigación 11

Recomendaciones 12

Conclusiones 12

IoCs 13

Referencias **14**

Herramientas **14**

Índice de imágenes

Imagen 1. Diagrama de cadena de ataque de WhisperGate 5

Imagen 2. Mensaje de rescate de WhisperGate[3] 6

Imagen 3. Protección contra virus y amenazas de Windows Defender eliminada[3] 9

Términos y acrónimos

- **Beaconing Implant:** Tipo de malware que envía periódicamente señales a un servidor remoto para comprobar su estado (conectividad) y recibir instrucciones.
- **Cyber Kill-Chain:** Modelo desarrollado por *Lockheed Martin* para destacar las fases de un ciberataque desde su origen hasta su objetivo final. Las principales etapas son: reconocimiento, preparación, distribución, explotación, instalación, comando y control, persistencia.
- **Exploit:** Parte del malware que se aprovecha de una vulnerabilidad para provocar un comportamiento inesperado en el objetivo pudiendo así obtener acceso al mismo. Suele ser el encargado de inyectar el payload.
- **Malware:** Cualquier tipo de software que realiza acciones no deseadas con el objetivo de causar perjuicios económicos u otros contratiempos.
- **Payload:** También conocido como «*carga útil*», es la parte del malware que se ejecuta tras la explotación de la vulnerabilidad y causa acciones maliciosas no deseadas.
- **Wiper:** Programa malicioso que busca causar daños irreparables mediante el borrado completo del disco duro de la máquina comprometida.

- **CDN –** Content Delivery Network (*Red de Distribución de Contenidos*)
- **CMS –** Content Management System (*Sistema de Gestión de Contenidos*)
- **CVSS –** Common Vulnerability Scoring System (*Sistema de Puntuación de Vulnerabilidades Comunes*)
- **EDR –** Endpoint Detection and Response
- **GRU –** Departamento Central de Inteligencia de Rusia.
- **MBR –** Master Boot Record *(Registro de Arranque Principal)*
- **MFA –** Multifactor Authentication (*Autenticación Multifactor*)
- **PoC –** Proof of Concept (*Prueba de Concepto*)
- **TTP –** Tácticas, Técnicas y Procedimientos

Contexto de la amenaza

Resumen Ejecutivo

AMENAZA	WhisperGate
ACTOR	*Ember Bear* (APT28 – GRU)
SECTOR	Gubernamental
PAÍS ORIGEN	Rusia
PAÍS OBJETIVO	Ucrania
FECHA INICIAL	2022
MOTIVACIÓN	Ciberguerra
VECTOR ATAQUE	Vulnerabilidad Software
SISTEMA OBJETIVO	Windows
IMPACTO	**ALTO**

WhisperGate[1] es una variante de malware identificada por primera vez por el equipo de ciberinteligencia de amenazas de Microsoft, MSTIC (*Microsoft Threat Intelligence Center*), el 13 de enero de 2022 poco antes del estallido del conflicto bélico entre Rusia y Ucrania el 24 de febrero del 2022. Tras haber sido investigada, esta campaña se atribuye a un grupo cibercriminal financiado por el estado ruso conocido como *Ember Bear*[2], en concreto se le ubica dentro de APT28 (GRU) debido a su forma de operar. Su objetivo son principalmente organizaciones gubernamentales del estado ucraniano, así como algunas organizaciones sin ánimo de lucro o empresas dedicadas al sector de las TI. Mediante este ataque buscan principalmente causar daños irreparables en los equipos informáticos de Ucrania haciendo que estos queden inoperables.

WhisperGate se hace pasar por un ransomware imitando su comportamiento tradicional, pero sin llegar a proporcionar una clave de descifrado o método de recuperación de los archivos lo cual indica que su intención no es obtener un redito económico sino causar daños irreparables. Aunque al iniciar el sistema aparece una nota de rescate, realmente el malware se trata de un *Wiper* que elimina de manera irreversible la información del dispositivo afectado. Para lograr su objetivo se emplean técnicas como la sobreescritura del MBR, corrupción de archivos y directorios, evasión de defensas y destrucción del volumen `C:\`.

[1] WhisperGate, MITRE ATT&CK (https://attack.mitre.org/software/S0689/)
[2] Ember Bear, MITRE ATT&CK (https://attack.mitre.org/groups/G1003/)

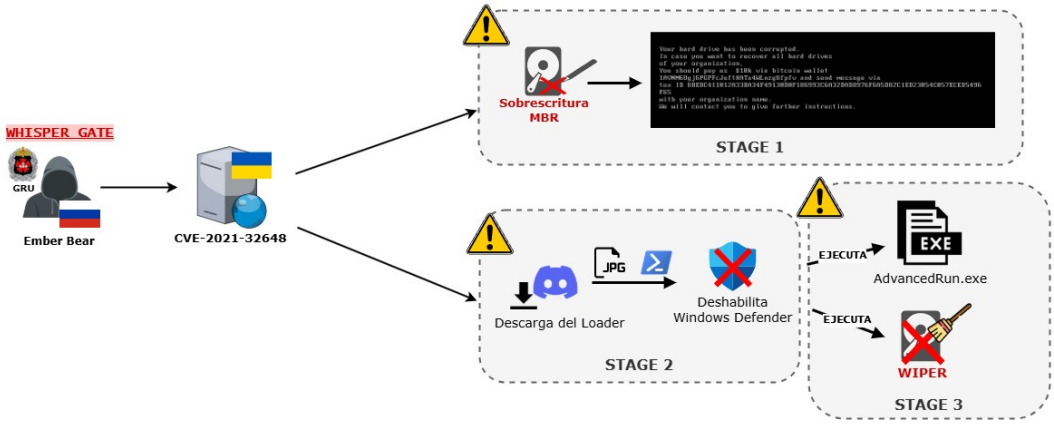
Cadena de Ataque

A alto nivel esta amenaza opera en tres grandes etapas. La primera consiste en la sobreescritura del MBR para mostrar la falsa nota de rescate, mientras que la segunda descarga contenido de un servidor aparentemente benigno como Discord para, posteriormente, en la tercera fase realizar acciones sobre el dispositivo tales como, añadirse a una lista de exclusión de Windows Defender para evitar ser detectado, realizar un descubrimiento del sistema para reconocer discos físicos y finalmente realizar el borrado de los datos del dispositivo de manera irreversible.

Los atacantes operan utilizando *Living Off The Land Binaries* (LOLBINs), es decir, programas ya instalados por defecto en la máquina objetivo (`powerhsell`, `reg`, `cmd`...), para realizar sus acciones de escalada de privilegios, persistencia y evasión de detección. También emplean distintas técnicas anti-forense para evitar que su forma de operar sea descubierta.

A continuación, se muestra un pequeño diagrama del flujo de esta amenaza y posteriormente se detallarán las fases del ataque de manera simplificada.

Imagen 1. *Diagrama de cadena de ataque de WhisperGate.*



Acceso inicial

Este actor de amenazas obtiene el acceso inicial a los sistemas generalmente explotando vulnerabilidades en los servidores web, CMS o Exchange de sus objetivos que a menudo se encuentran en la red perimetral o DMZ. Algunas de las vulnerabilidades que han sido explotadas por este actor son:

- **CVE-2021-26084:** Afecta a servidores de *Confluence* y es clasificada como critica con una puntuación de 9.8 en CVSS versión 3 por el NIST.
- **CVE-2022-4104:** Afecta a servidores de Exchange provocando bucles infinitos a través de una imagen JPEG.

- **CVE-2021-32648**: Afecta a un librería del CMS, OctoberCMS versión 1.0.471, provocando un cambio de contraseña en una cuenta objetivo sin validar correctamente los parámetros. Tiene una calificación crítica de 9.1 CVSS versión 3 por el NIST. Se cree que este último CVE fue utilizado para vulnerar los sitios web del gobierno ucraniano y solicitar el cambio de contraseña de un usuario administrador sin interacción del propio usuario, según informan algunos reportes[3,4].

Entrega

Una vez han adquirido el acceso en el sistema, los atacantes ejecutan el falso ransomware, conocido como `stage1.exe`, que sobrescribe el MBR para mostrar el siguiente mensaje de rescate.

Imagen 2. *Mensaje de rescate de WhisperGate[3].*



Una vez inutilizado el equipo y con la distracción del falso ransomware, se comienza la fase 2 (`stage2.exe`) que consiste en la creación de una conexión HTTPS para descargar un fichero JPG almacenado en el CDN de Discord (una plataforma legítima donde los usuarios, entre otras cosas, pueden crear archivos para compartir a través del CDN). El fichero en cuestión se obtiene de la siguiente dirección URL:

`hxxps://cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg`

La imagen `Tbopbh.jpg` resulta ser un *payload* en memoria utilizando MSIL (*Microsoft Intermidiate Language*) que entrega un *beaconing implant* que desata una serie de acciones maliciosas.

[3] Unit42, Palo Alto Networks (https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/)
[4] PoC CVE-2021-32648, GitHub (https://github.com/Immersive-Labs-Sec/CVE-2021-32648/blob/main/cve-2021-32648.py)

Instalación

Tras ejecutar el *payload* se desencadenan una serie de actividades y patrones los cuales se comentan a continuación.

1. Copia de un binario legítimo de Windows (`InstallUtil.exe`) al directorio `%TEMP%` de la máquina afectada. Por ejemplo, el directorio `C:\Users\[USERNAME]\AppData\Local\Temp`.
2. Se crean dos instancias de PowerShell con un comando codificado en base 64 que duerme el equipo 10 segundos para evadir detecciones.
   - `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==`
3. Se crea un fichero de Visual Basic Script (VBS) en `C:\Users\[USERNAME]\AppData\Local\Temp` nombrado: `Nmddfrqqrbyjeygggda.vbs`

Ejecución y Evasión de Defensas

Siguiendo con las acciones desencadenadas por la ejecución del *payload* y una vez se cuenta con el fichero de Visual Basic.

4. El proceso `wscript.exe` (un LOLBIN)[5] se utiliza para ejecutar el script de Visual Basic que llama a PowerShell para establecer una ruta de exclusión de Windows Defender, la raíz `C:\`. De manera efectiva, este comando de PowerShell desactiva la protección del antivirus de Microsoft para evadir defensas y evitar detecciones.
   - `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Set-MpPreference -ExclusionPath 'C:\'`
5. Una vez «desactivado» el antivirus, se crea el proceso AdvancedRun.exe[6] y se escribe en `C:\Users\[USERNAME]\AppData\Local\Temp`.
6. `AdvancedRun.exe` crea otro proceso de PowerShell para parar y eliminar definitivamente Windows Defender utilizando los siguientes parámetros.
   - `"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" /WindowState 0 /CommandLine "rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse" /StartDirectory "" /RunAs 8 /Run`
   - `"C:\Users\[USERNAME]\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\`

[5] Wscript, LOLBAS (https://lolbas-project.github.io/lolbas/Binaries/Wscript/)
[6] El proceso `AdvancedRun.exe` es una utilidad de NirSoft que permite ejecutar un programa de Windows con distintos usuarios, privilegios, configuraciones o variables de entorno.

```
sc.exe" /WindowState 0 /CommandLine "stop
WinDefend" /StartDirectory "" /RunAs 8 /Run
```

7. Eliminación de Windows Defender:
   - `C:\Windows\System32\WindowsPowerShell\v1.0\ powershell.exe rmdir 'C:\ProgramData\Microsoft\ Windows Defender' -Recurse`

Fases finales

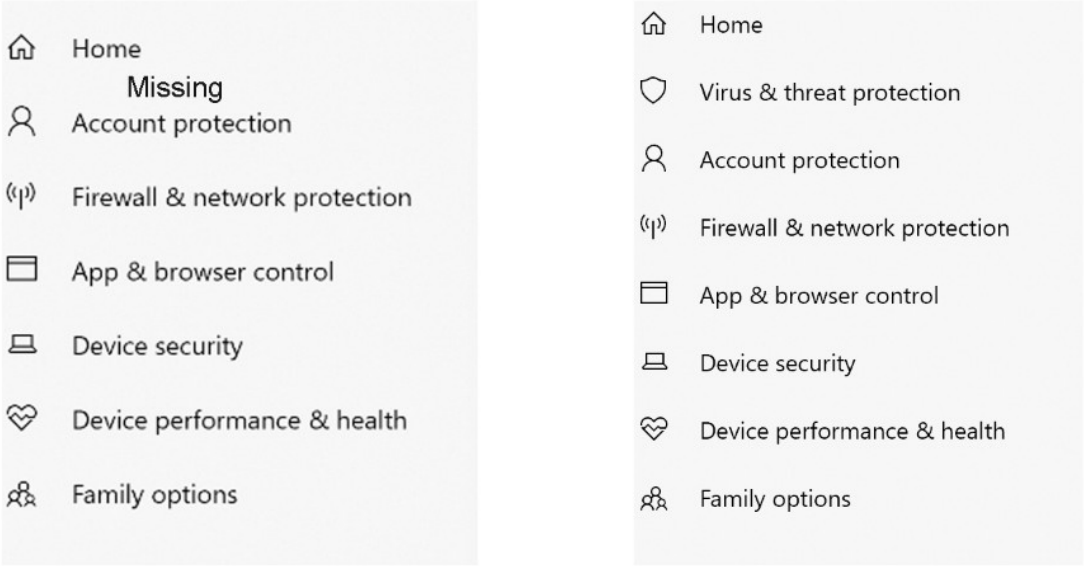
8. Varias instancias de `cmd.exe` llaman a `Ping.exe` y se elimina `InstallUtil.exe`.
   - `cmd.exe /min /C ping 111.111.111[.]111 -n 5 -w 10 > Nul & Del /f /q %TEMP%\InstallUtil.exe`
9. Se elimina `AdvancedRun.exe` del directorio temporal del usuario mediante `stage2.exe`.
10. Tráfico ICMP hacia la dirección `111.111.111[.]111`.
11. Todos los directorios y ficheros, incluyendo los montados a través de USB y red (sin contar con el volumen `A:`) se sobrescriben con el byte `0xCC` hasta el primer megabyte (1MB) si llevan alguna de las siguientes

```
.3DM .3DS .7Z .ACCDB .AI .ARC .ASC .ASM .ASP .ASPX .BACKUP
.BAK .BAT .BMP .BRD .BZ .BZ2 .CGM .CLASS .CMD .CONFIG .CPP
.CRT .CS .CSR .CSV .DB .DBF .DCH .DER .DIF .DIP .DJVU.SH .
DOC .DOCB .DOCM .DOCX .DOT .DOTM .DOTX .DWG .EDB .EML .FRM
.GIF .GO .GZ .HDD .HTM .HTML .HWP .IBD .INC .INI .ISO .JAR
.JAVA .JPEG .JPG .JS .JSP .KDBX .KEY .LAY .LAY6 .LDF .LOG
.MAX .MDB .MDF .MML .MSG .MYD .MYI .NEF .NVRAM .ODB .ODG .
ODP .ODS .ODT .OGG .ONETOC2 .OST .OTG .OTP .OTS .OTT .P12
.PAQ .PAS .PDF .PEM .PFX .PHP .PHP3 .PHP4 .PHP5 .PHP6 .PHP
7 .PHPS .PHTML .PL .PNG .POT .POTM .POTX .PPAM .PPK .PPS .
PPSM .PPSX .PPT .PPTM .PPTX .PS1 .PSD .PST .PY .RAR .RAW .
RB .RTF .SAV .SCH .SHTML .SLDM .SLDX .SLK .SLN .SNT .SQ3 .
SQL .SQLITE3 .SQLITEDB .STC .STD .STI .STW .SUO .SVG .SXC
.SXD .SXI .SXM .SXW .TAR .TBK .TGZ .TIF .TIFF .TXT .UOP .U
OT .VB .VBS .VCD .VDI .VHD .VMDK .VMEM .VMSD .VMSN .VMSS .
VMTM .VMTX .VMX .VMXF .VSD .VSDX .VSWP .WAR .WB2 .WK1 .WKS
.XHTML .XLC .XLM .XLS .XLSB .XLSM .XLSX .XLT .XLTM .XLTX .
XLW .YML .ZIP
```

extensiones. Los ficheros más grandes de 1MB se truncan antes de ser sobrescritos.

12. Se renombran los ficheros con una extensión aparentemente aleatoria.
13. Finalmente, la protección de Windows Defender desaparece.

Imagen 3. *Protección contra virus y amenazas de Windows Defender eliminada[3].*



Acciones

WhisperGate lleva a cabo una serie de acciones destructivas en los sistemas que infecta. Primero, sobrescribe el registro de arranque maestro (MBR) con una nota falsa de rescate, lo que impide que el sistema se inicie. Luego, en una segunda etapa, corrompe archivos en el disco, sobrescribiéndolos con datos «aleatorios» y cambiando sus extensiones, haciendo que los archivos sean irrecuperables. A diferencia del ransomware tradicional, no ofrece una forma de recuperar los archivos, lo que demuestra que su objetivo es la destrucción permanente de datos, no el lucro.

En este apartado se describirán algunos TTPs que utiliza y se intentarán dar algunas medidas de mitigación y recomendaciones para afrontar esta amenaza desde un punto de vista tanto técnico como ejecutivo.

TTPs

Tras haberse analizado la amenaza y las muestras de la misma se han descubierto un total de **8 tácticas** y **28 técnicas**. Entre ellas destacan las siguientes.

- **Acceso inicial:** WhisperGate utiliza la API nativa del sistema operativo (`ExitWindowsEx`) para volcar los contenidos del *buffer* al disco y parar los procesos en ejecución y otras llamadas a la API, así como crear servicios para descargar `AdvancedRun.exe` mediante `sc.exe` (`T1569.002`).

- **Ejecución:** Ejecución de comandos de PowerShell para evadir defensas, Visual Basic para excluir `C:\` de Windows Defender, ejecuciones mediante `cmd.exe`, etc.
- **Persistencia:** Utiliza `T1542.003` (*Bootkit*) para sobrescribir el MBR y añadir una nota de rescate falsa.
- **Escalada de Privilegios:** Uso de `AdvancedRun.exe` para ejecución de comandos como el grupo de *Windows TrustedInstaller* via `%TEMP%\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop WinDefend" /StartDirectory "" /RunAs 8 /Run`
- **Evasión de Defensas:** Borrado de ficheros en máquinas comprometidas (`T1070.004`), enmascaramiento como archivo JPG para evitar ser detectado como fichero PE malicioso (`T1036`), ficheros codificados/encriptados (`T1027.013`), etc.
- **Descubrimiento:** Localización de ficheros basados en extensión (`T1083`), detección de dispositivos de almacenamiento locales y conectados en red (`T1082` y `T1135`), comprobación de utilidades de monitorización (`T1497.001`).
- **Comando y Control:** Uso de protocolos de comunicación a nivel de aplicación (HTTPS) para descarga de ficheros (`T1071.001`), descarga de fases de la campaña a través del CDN de Discord (`T1105` y `T1102`).
- **Impacto:** Corrupción de ficheros sobrescribiendo con `0xCC` el primer megabyte (`T1485`), apagado/reinicio del sistema (`T1529`) y borrado de contenidos del disco y estructura MBR (`T1561.001` y `T1561.002`).

A continuación, se adjunta el enlace al navegador de la matriz de MITRE donde se pueden ver todas las tácticas y técnicas empleadas por *WhisperGate* con información adicional y con enlaces a la página oficial de MITRE que recoge información detallada sobre cada táctica y técnica.

https://mitre-attack.github.io/attack-navigator//#layerURL=https%3A%2F%2Fattack.mitre.org%2Fsoftware%2FS0689%2FS0689-enterprise-layer.json

De la misma manera se adjunta un enlace a *Joe Sandbox* que es un analizador de malware que nos permite conocer el comportamiento de la fase 2 (descarga desde Discord) y las herramientas utilizadas, así como las TTPs en la matriz de MITRE y reglas YARA para detectar la amenaza. En concreto resulta de interés el gráfico de comportamiento (*Behavior Graph*).

https://www.joesandbox.com/analysis/553986/0/html

Mitigación

Conociendo el contexto de la amenaza y tras haber analizado los TTPs, se proponen una serie de medidas de mitigación para hacer frente a esta amenaza basadas en recomendaciones de entidades oficiales y empresas del sector como CISA o MIcrosoft. Estas medidas abarcan varios ámbitos aplicando el principio de defensa en profundidad.

- Configurar los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) o cualquier mecanismo de defensa de la red para alertar sobre los dominios utilizados por *WhisperGate* y, tras la revisión, bloquear los intentos de conexión hacia y desde dichos dominios.
- Aplicar MFA obligatorio.
- Aislar de la red las máquinas infectadas por la amenaza para prevenir su expansión.
- Considerar la aplicación de segmentación de red, ya sea a través de firewalls, VLAN u otras técnicas, para dificultar la expansión de un malware.
- Monitorizar la creación o modificación de archivos sospechosa, en particular grandes modificaciones, en los directorios de usuarios y rutas críticas del sistema.
- Desactivar la ejecución de macros y complementos de Microsoft Office. En el caso de ser necesarias, deben ir firmadas.
- Detectar llamadas a las APIs nativas de Windows y bloquearlas si se identifican con software potencialmente malicioso.
- Utilizar versiones actualizadas de PowerShell que incluyan mejoras de seguridad como a partir de la versión 5.
- Establecer la política de ejecución de *scripts* en PowerShell para que se requiera que los programas tengan que estar firmados.
- Habilitar CFA (*Controlled Folder Access*) para prevenir la modificación del MBR.
- Implementar un sistema de copias de seguridad periódico para sobreponerse a la eliminación de la información del disco y corrupción de archivos.
- Añadir reglas yara para la detección de posibles infecciones.

Recomendaciones

- Monitorización continúa de cuentas, listas de control de acceso, permisos y privilegios en recursos críticos del sistema.
- Revisión de tráfico de red en busca de patrones anómalos, considerando la implementación de un sistema automático basado en Inteligencia Artificial para detección de anomalías.
- Revisar toda la actividad de autenticación a la infraestructura mediante acceso remoto, con un particular enfoque en las cuentas configuradas con autenticación de factor único, para confirmar la autenticidad e investigar cualquier actividad anómala.
- Emplear detección de malware basado en heurísticas y no únicamente en firmas y/o implantar soluciones EDR.
- Aplicar controles para la descarga de software no oficial o no firmado.
- Fortificar el sistema operativo subyacente siguiendo guías oficiales como las del CIS y asegurar que se cuentan con las últimas actualizaciones y parches de seguridad.
- Someter a los sistemas a ejercicios de Red Team para evaluar la resiliencia de la organización a pruebas de estrés y respuesta ante incidentes.
- Asegurar el corrector registro (*logging*) de los comandos, logs de auditoría y dispositivos de red, para poder realizar un análisis forense posterior y entender el funcionamiento de la amenaza.

Conclusiones

WhiperGate supone una gran amenaza a las organizaciones afectadas ya que atenta contra la disponibilidad de los datos de las víctimas haciendo que estos sean irrecuperables. El impacto de esta amenaza para las organizaciones objetivo puede ser devastador, es por ello que se recomienda adaptar las medidas de mitigación listadas anteriormente al contexto de cada empresa para establecer un plan que permita hacer frente a este tipo de amenazas y que esté alineado con las recomendaciones, también mencionadas, para asegurar una correcta respuesta ante incidentes similares y una detección temprana de las amenazas.

IoCs

Indicador	Tipo	Descripción
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	SHA 256	Hash del `stage1.exe` *wiper* malware.
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	SHA 256	Hash del `stage2.exe`.
923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6	SHA 256	Hash de la *payload* `Tbopbh.jpg`
29ae7b30ed8394c509c561f6117ea671ec412da50d435099756bbb257fafb10b	SHA 256	Hash del fichero `AdvancedRun.exe`
db5a204a34969f60fe4a653f51d64eee024dbf018edea334e8b3df780eda846f	SHA 256	Hash del script de Visual Basic `Nmddfrqqrbyjeygggda.vbs`.
cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1	Línea de Comandos	Ejemplo de comando de ejecución del *wiper*.
https[:]//cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg	URL	Dirección del payload del CDN de Discord.
179.43.187[.]33	IP	Dirección alojada en *JusticeUA* entre marzo y abril de 2022
111.111.111[.]111	IP	Dirección contactada a través de ICMP

Referencias

- *Artículo Iván Portillo, Campus Ciberseguridad*, 2025 https://www.campusciberseguridad.com/blog/la-inteligencia-de-amenazas-o-cyber-threat-intelligence
- *AttackIQ*, https://www.attackiq.com/2024/11/12/emulating-whispergate-malware/
- *Cadet Blizzard*, *Microsoft Security Blog*, https://www.microsoft.com/en-us/security/blog/2023/06/14/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/
- *Informe CISA*, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a
- *Intel471*, https://intel471.com/blog/whispergate
- *Research Insikt Group*, https://www.recordedfuture.com/research/whispergate-malware-corrupts-computers-ukraine
- *Unit42, Palo Alto Networks*, https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/
- *WhisperGate Malware, Microsoft Security Blog*, https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
- *WhisperGate, MITRE ATT&CK*, https://attack.mitre.org/software/S0689/

Herramientas

Las herramientas utilizadas han sido principalmente la matriz de navegación online de MITRE (https://github.com/mitre-attack/attack-navigator) y la herramienta draw.io para la realización de los diagramas. También se ha utilizado la plataforma de *sandboxing online* de Joe Sandbox para analizar el comportamiento del malware de la fase 2.