# WHISPERGATE THREAT CONTEXT

Author:

Ángel Luis Rodríguez Martín-Palomino

# Table of Contents

**Terms and Acronyms** ..... **3**

**Threat Context** ..... **4**

Executive Summary ..... 4

Attack Chain ..... 5

*Initial Access* ..... *5*

*Delivery* ..... *6*

*Installation* ..... *6*

*Execution and Defense Evasion* ..... *7*

*Final Stages* ..... *8*

**Actions** ..... **9**

TTPs ..... 9

Mitigation ..... 11

Recommendations ..... 12

Conclusions ..... 12

IoCs ..... 13

**References** ..... **14**

**Tools** ..... **14**

# List of Images

**Image 1.** WhisperGate attack chain diagram ..... 5

**Image 2.** WhisperGate ransom message[3] ..... 6

**Image 3.** Windows Defender Virus & threat protection removed[3] ..... 9

# Terms and Acronyms

- **Beaconing Implant:** Type of malware that periodically sends signals to a remote server to check its status (connectivity) and receive instructions.
- **Cyber Kill-Chain:** Model developed by *Lockheed Martin* to highlight the stages of a cyberattack from its origin to its final objective. The main stages are: reconnaissance, weaponization, delivery, exploitation, installation, command and control, persistence.
- **Exploit:** Part of the malware that takes advantage of a vulnerability to cause unexpected behavior in the target, thereby being able to gain access to it. It is usually responsible for injecting the payload.
- **Malware:** Any type of software that performs unwanted actions with the aim of causing financial losses or other setbacks.
- **Payload:** It is the part of the malware that is executed after the vulnerability has been exploited and causes unwanted malicious actions.
- **Wiper:** Malicious program that seeks to cause irreparable damage by completely wiping the hard drive of the compromised machine.

- **CDN –** Content Delivery Network
- **CMS –** Content Management System
- **CVSS –** Common Vulnerability Scoring System
- **EDR –** Endpoint Detection and Response
- **GRU –** Central Intelligence Department of Russia.
- **MBR –** Master Boot Record
- **MFA –** Multifactor Authentication
- **PoC –** Proof of Concept
- **TTP –** Tactics, Techniques and Procedures

# Threat Context

## Executive Summary

| THREAT | WhisperGate |
|---|---|
| ACTOR | *Ember Bear* (APT28 – GRU) |
| SECTOR | Government |
| COUNTRY OF ORIGIN | Russia |
| TARGET COUNTRY | Ukraine |
| START DATE | 2022 |
| MOTIVATION | Cyberwarfare |
| ATTACK VECTOR | Software Vulnerability |
| TARGET SYSTEM | Windows |
| IMPACT | HIGH |

*WhisperGate*[1] is a malware variant first identified by Microsoft's threat intelligence team, MSTIC (*Microsoft Threat Intelligence Center*), on January 13, 2022, shortly before the outbreak of the armed conflict between Russia and Ukraine on February 24, 2022. After being investigated, this campaign has been attributed to a Russian state-sponsored cybercriminal group known as *Ember Bear*[2]; specifically, it is placed within APT28 (GRU) due to its modus operandi. Its targets are mainly government organizations of the Ukrainian state, as well as some non-profit organizations or companies in the IT sector. Through this attack, they mainly seek to cause irreparable damage to Ukraine's computer equipment, rendering it inoperable.

*WhisperGate* poses as ransomware by mimicking its traditional behavior, but without ever providing a decryption key or file recovery method, which indicates that its intention is not to obtain financial gain but to cause irreparable damage. Although a ransom note appears when the system starts, the malware is actually a *Wiper* that irreversibly deletes the information on the affected device. To achieve its goal, it employs techniques such as overwriting the MBR, corrupting files and directories, evading defenses and destroying the `C:\` volume.

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

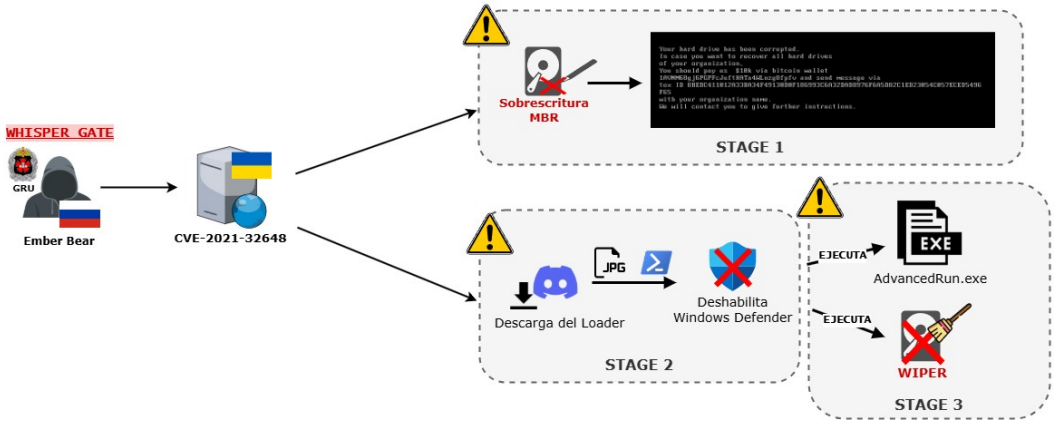
## Attack Chain

At a high level, this threat operates in three main stages. The first consists of overwriting the MBR to display the fake ransom note, while the second downloads content from a seemingly benign server such as Discord so that, later, in the third stage, it can perform actions on the device such as adding itself to a Windows Defender exclusion list to avoid detection, performing system discovery to identify physical disks and, finally, irreversibly wiping the device's data.

The attackers operate using *Living Off The Land Binaries* (LOLBINs), that is, programs already installed by default on the target machine (`powerhsell`, `reg`, `cmd`...) to carry out their privilege escalation, persistence and detection evasion actions. They also employ various anti-forensic techniques to prevent their modus operandi from being discovered.

Below is a small diagram of this threat's flow, after which the stages of the attack will be detailed in a simplified manner.

***Image 1.*** *WhisperGate attack chain diagram.*




## Initial Access

This threat actor generally obtains initial access to systems by exploiting vulnerabilities in its targets' web servers, CMS or Exchange servers, which are often located in the perimeter network or DMZ. Some of the vulnerabilities that have been exploited by this actor are:

- **CVE-2021-26084:** Affects *Confluence* servers and is rated as critical with a score of 9.8 in CVSS version 3 by NIST.
- **CVE-2022-4104:** Affects Exchange servers, causing infinite loops through a JPEG image.

- **CVE-2021-32648**: Affects a library of the CMS OctoberCMS version 1.0.471, causing a password change on a target account without properly validating the parameters. It has a critical rating of 9.1 in CVSS version 3 by NIST. This last CVE is believed to have been used to compromise Ukrainian government websites and request a password change for an administrator user without any interaction from the user themselves, according to some reports[3,4].

## Delivery

Once they have gained access to the system, the attackers execute the fake ransomware, known as `stage1.exe`, which overwrites the MBR to display the following ransom message.

***Image 2.*** *WhisperGate ransom message[3].*




Once the computer has been rendered unusable and with the distraction of the fake ransomware, stage 2 begins (`stage2.exe`), which consists of creating an HTTPS connection to download a JPG file stored on the Discord CDN (a legitimate platform where users can, among other things, create files to share through the CDN). The file in question is obtained from the following URL:

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

The image `Tbopbh.jpg` turns out to be an in-memory *payload* using MSIL (*Microsoft Intermidiate Language*) that delivers a *beaconing implant* which unleashes a series of malicious actions.

[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)

## Installation

After the *payload* is executed, a series of activities and patterns are triggered, which are discussed below.

1. A legitimate Windows binary (`InstallUtil.exe`) is copied to the `%TEMP%` directory of the affected machine. For example, the directory `C:\Users\[USERNAME]\AppData\Local\Temp`.
2. Two PowerShell instances are created with a base64-encoded command that puts the computer to sleep for 10 seconds to evade detection.
   - `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==`
3. A Visual Basic Script (VBS) file is created in `C:\Users\[USERNAME]\AppData\Local\Temp` named: `Nmddfrqqrbyjeygggda.vbs`

## Execution and Defense Evasion

Continuing with the actions triggered by the execution of the *payload* and once the Visual Basic file is in place.

4. The `wscript.exe` process (a LOLBIN)[5] is used to execute the Visual Basic script, which calls PowerShell to set a Windows Defender exclusion path, the root `C:\`. In effect, this PowerShell command disables Microsoft's antivirus protection in order to evade defenses and avoid detection.
   - `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Set-MpPreference -ExclusionPath 'C:\'`
5. Once the antivirus has been «disabled», the AdvancedRun.exe[6] process is created and written to `C:\Users\[USERNAME]\AppData\Local\Temp`.
6. `AdvancedRun.exe` creates another PowerShell process to stop and permanently remove Windows Defender using the following parameters.
   - `"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] The `AdvancedRun.exe` process is a NirSoft utility that allows a Windows program to be run with different users, privileges, settings or environment variables.

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

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

## Final Stages

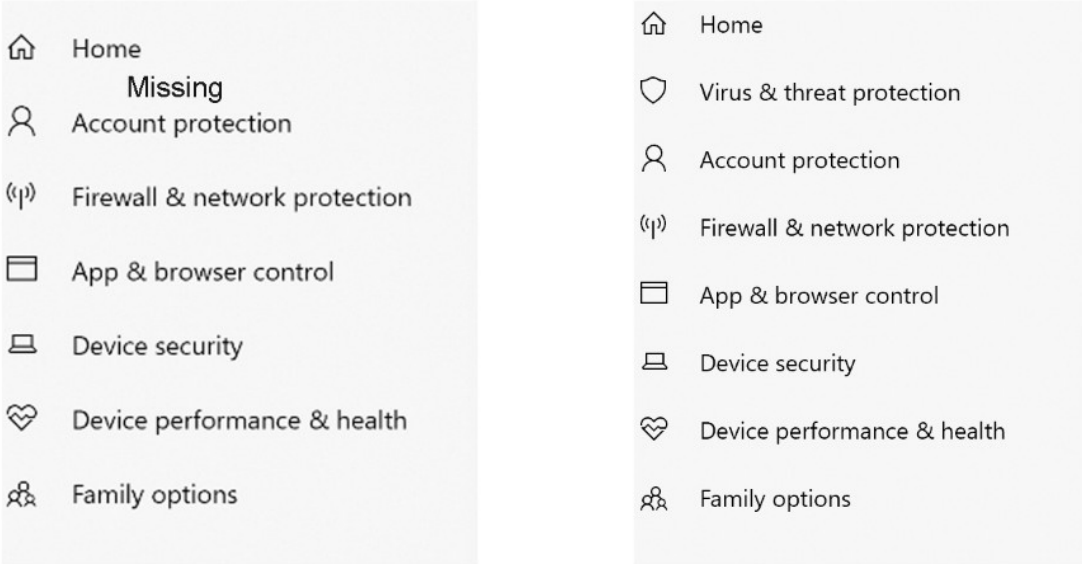
8. Several instances of `cmd.exe` call `Ping.exe` and `InstallUtil.exe` is deleted.
   - `cmd.exe /min /C ping 111.111.111[.]111 -n 5 -w 10 > Nul & Del /f /q %TEMP%\InstallUtil.exe`
9. `AdvancedRun.exe` is deleted from the user's temporary directory by `stage2.exe`.
10. ICMP traffic to the address `111.111.111[.]111`.
11. All directories and files, including those mounted via USB and network (excluding the `A:` volume) are overwritten with the byte `0xCC` up to the first megabyte (1MB) if they have any of the following extensions. Files

```
.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
```

    larger than 1MB are truncated before being overwritten.

12. Files are renamed with a seemingly random extension.
13. Finally, Windows Defender protection disappears.

***Image 3.*** *Windows Defender Virus & threat protection removed[3].*




# Actions

*WhisperGate* carries out a series of destructive actions on the systems it infects. First, it overwrites the master boot record (MBR) with a fake ransom note, which prevents the system from booting. Then, in a second stage, it corrupts files on the disk, overwriting them with «random» data and changing their extensions, making the files unrecoverable. Unlike traditional ransomware, it offers no way to recover the files, which shows that its goal is the permanent destruction of data, not profit.

This section will describe some of the TTPs it uses and will attempt to provide some mitigation measures and recommendations to address this threat from both a technical and an executive point of view.

## TTPs

After analyzing the threat and its samples, a total of **8 tactics** and **28 techniques** have been discovered. The following stand out among them.

- **Initial Access:** WhisperGate uses the operating system's native API (`ExitWindowsEx`) to flush the contents of the *buffer* to disk and stop running processes and other API calls, as well as to create services to download `AdvancedRun.exe` via `sc.exe` (`T1569.002`) .
- **Execution:** Execution of PowerShell commands to evade defenses, Visual Basic to exclude `C:\` from Windows Defender, executions via `cmd.exe`, etc.

- **Persistence:** Uses `T1542.003` (*Bootkit*) to overwrite the MBR and add a fake ransom note.
- **Privilege Escalation:** Use of `AdvancedRun.exe` to execute commands as the *Windows TrustedInstaller* group via `%TEMP%\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\sc.exe" /WindowState 0 /CommandLine "stop WinDefend" /StartDirectory "" /RunAs 8 /Run`
- **Defense Evasion:** Deletion of files on compromised machines (`T1070.004`), masquerading as a JPG file to avoid being detected as a malicious PE file (`T1036`), encoded/encrypted files (`T1027.013`), etc.
- **Discovery:** Locating files based on extension (`T1083`), detection of local and network-connected storage devices (`T1082` and `T1135`), checking for monitoring utilities (`T1497.001`).
- **Command and Control:** Use of application-layer communication protocols (HTTPS) to download files (`T1071.001`), downloading of campaign stages through the Discord CDN (`T1105` and `T1102`).
- **Impact:** Corruption of files by overwriting the first megabyte with `0xCC` (`T1485`), system shutdown/reboot (`T1529`) and wiping of disk contents and the MBR structure (`T1561.001` and `T1561.002`).

Below is the link to the MITRE matrix navigator, where all the tactics and techniques employed by *WhisperGate* can be viewed with additional information and with links to the official MITRE page that gathers detailed information on each tactic and technique.

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

Likewise, a link is provided to *Joe Sandbox*, a malware analyzer that allows us to learn about the behavior of stage 2 (download from Discord) and the tools used, as well as the TTPs in the MITRE matrix and YARA rules to detect the threat. Of particular interest is the behavior graph (*Behavior Graph*).

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

## Mitigation

Knowing the context of the threat and having analyzed the TTPs, a series of mitigation measures are proposed to address this threat, based on recommendations from official bodies and industry companies such as CISA or MIcrosoft. These measures cover several areas, applying the principle of defense in depth.

- Configure intrusion detection systems (IDS) and intrusion prevention systems (IPS), or any network defense mechanism, to alert on the domains used by *WhisperGate* and, after review, block connection attempts to and from those domains.
- Enforce mandatory MFA.
- Isolate machines infected by the threat from the network to prevent its spread.
- Consider applying network segmentation, whether through firewalls, VLANs or other techniques, to hinder the spread of malware.
- Monitor suspicious file creation or modification, particularly large-scale modifications, in user directories and critical system paths.
- Disable the execution of Microsoft Office macros and add-ins. If they are necessary, they must be signed.
- Detect calls to native Windows APIs and block them if they are identified with potentially malicious software.
- Use updated versions of PowerShell that include security improvements, such as version 5 onwards.
- Set the PowerShell *scripts* execution policy so that programs are required to be signed.
- Enable CFA (*Controlled Folder Access*) to prevent modification of the MBR.
- Implement a periodic backup system to recover from the deletion of disk information and file corruption.
- Add YARA rules for the detection of possible infections.

## Recommendations

- Continuous monitoring of accounts, access control lists, permissions and privileges on critical system resources.
- Review of network traffic for anomalous patterns, considering the implementation of an automated system based on Artificial Intelligence for anomaly detection.
- Review all authentication activity to the infrastructure via remote access, with a particular focus on accounts configured with single-factor authentication, to confirm authenticity and investigate any anomalous activity.
- Employ heuristic-based malware detection, not solely signature-based, and/or deploy EDR solutions.
- Apply controls on the download of unofficial or unsigned software.
- Harden the underlying operating system following official guides such as those from CIS and ensure that the latest security updates and patches are in place.
- Subject systems to Red Team exercises to assess the organization's resilience to stress testing and incident response.
- Ensure the correct recording (*logging*) of commands, audit logs and network devices, in order to be able to carry out a subsequent forensic analysis and understand how the threat works.

## Conclusions

*WhiperGate* poses a major threat to the affected organizations since it attacks the availability of the victims' data, rendering it unrecoverable. The impact of this threat on the targeted organizations can be devastating, which is why it is recommended to adapt the mitigation measures listed above to the context of each company in order to establish a plan that makes it possible to deal with this type of threat and that is aligned with the recommendations, also mentioned, to ensure a proper response to similar incidents and early detection of threats.

## IoCs

| Indicator | Type | Description |
|---|---|---|
| a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 | SHA 256 | Hash of the `stage1.exe` *wiper* malware. |
| dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78 | SHA 256 | Hash of `stage2.exe`. |
| 923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6 | SHA 256 | Hash of the *payload* `Tbopbh.jpg` |
| 29ae7b30ed8394c509c561f6117ea671ec412da50d435099756bbb257fafb10b | SHA 256 | Hash of the file `AdvancedRun.exe` |
| db5a204a34969f60fe4a653f51d64eee024dbf018edea334e8b3df780eda846f | SHA 256 | Hash of the Visual Basic script `Nmddfrqqrbyjeygggda.vbs`. |
| cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1 | Command Line | Example command for executing the *wiper*. |
| https[:]//cdn.discordapp[.]com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg | URL | Address of the payload on the Discord CDN. |
| 179.43.187[.]33 | IP | Address hosted on *JusticeUA* between March and April 2022 |
| 111.111.111[.]111 | IP | Address contacted via ICMP |

# References


- *Article by 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/
- *CISA Report*, 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/


# Tools

The tools used have mainly been MITRE's online navigation matrix (https://github.com/mitre-attack/attack-navigator) and the draw.io tool for creating the diagrams. The *online sandboxing* platform from Joe Sandbox was also used to analyze the behavior of the stage 2 malware.