

# WhisperGate Malware Corrupts Computers in Ukraine

 [recordedfuture.com/whispergate-malware-corrupts-computers-ukraine/](https://recordedfuture.com/whispergate-malware-corrupts-computers-ukraine/)



 Insikt Group

*This report is a technical overview of the WhisperGate malware reported by Microsoft Threat Intelligence on January 15, 2022. It is intended for those looking for a high-level overview of the malware's TTPs and mitigations.*

## Executive Summary

WhisperGate is a new malware family being used in an ongoing operation targeting multiple industries in Ukraine, including government, non-profit, and information technology organizations. The malware is a 3-stage master boot record (MBR) wiper designed to destroy a victim's MBR and corrupt files on attached storage devices. Each stage of the malware has a discrete task: stage 1 overwrites the MBR with a ransom note and code to overwrite sections on each drive found, stage 2 downloads and executes stage 3, which is hosted on Discord's CDN as a JPG attachment, and stage 3 corrupts any file that matches a list of 191 file extensions. The developers of the malware use obfuscation, particularly in stage 3, to evade detection and analysis.

WhisperGate wipes and corrupts a Windows system to the point where files and drives are no longer recoverable or usable. Details around the motive for WhisperGate and the threat actor behind the attacks are still emerging. These attacks take place in the context of an escalating risk of a Russian invasion of Ukraine and the Ukrainian government website defacements that occurred on January 14, 2022.

## Key Judgments

- As of this writing, the threat actor group deploying WhisperGate has not been attributed to any known threat groups, but other researchers suspect the group is state sponsored.

- The same precautions taken against ransomware with respect to data backups should be applied to mitigate the effects of WhisperGate’s data destruction capabilities.
- WhisperGate malware has not been observed in use as part of any other attacks outside of Ukraine, indicating it may have been developed specifically for this operation.


## Background

---

On January 15, 2022, Microsoft reported a destructive malware operation targeting multiple organizations in Ukraine. This activity has not been attributed to any existing threat actor group and is therefore being tracked using Microsoft's DEV-##### naming convention, which is used to track unknown emerging clusters of threat activity. This group has been given the designation DEV-0586 until it is eventually converted to a named actor or merged with an existing actor. Microsoft started seeing this malicious activity on January 13, 2022, which led to the investigation that uncovered a new malware family that is being tracked as WhisperGate.

## WhisperGate Technical Analysis


---

The WhisperGate malware has 3 stages, detailed below in Figure 1. All 3 stages must be executed prior to the machine rebooting for maximum effect. Stage 1 corrupts the MBR of the victim’s boot disk and upon reboot will corrupt other drives on the system. Stage 2 downloads stage 3, which is used to corrupt files on attached file systems and network drives. File damage will occur if even just one of either stage 1 or stage 2 executes successfully. In testing, we found that GUID Partition Table (GPT) disks are not irreparably destroyed by WhisperGate’s stage 1 malware and therefore are partially immune to that stage of the malware. We speculate that the inclusion of stage 2 and 3 may be a way to ensure that victims using GPT-style boot disks are affected by the malware too. However, stage 3 also targets remote network drives, which would cause further damage regardless of the partitioning scheme used by the victim’s boot disk.  **Figure 1: Stages of WhisperGate malware** (Source: Recorded Future)

### Stage 1: Overwrite Master Boot Record (MBR)

---


Stage 1 is compiled using the Minimalist GNU for Windows (MinGW) development environment, which supports GNU Compiler Collection (GCC) 6.3.0 on Windows. The binary’s primary objective is to overwrite the MBR of “\\.\PhysicalDrive0” with a custom MBR whose effect won’t be seen until the machine reboots. At startup, the computer’s BIOS determines the disk order to

use when looking for the MBR. Overwriting the MBR on PhysicalDrive0 is making an assumption that that disk is the first one in line to be checked by the BIOS, which is normally a reasonable assumption. Once the machine reboots and the custom MBR code executes, the user is presented with the ransom note displayed in Figure 2.  **Figure 2: Ransom note displayed after stage 1 of WhisperGate is executed (Source: Recorded Future)**

After displaying the ransom note, the MBR code overwrites sections of each drive, on 199-byte intervals, with the contents shown in Figure 3. The content written to each drive differs at the sixth byte, incrementing sequentially from 0x00.

 **Figure 3: Hex view of the contents that are written to disk (Source: Recorded Future)**

The MBR code writes the content multiple times to each drive by making extended write function calls via interrupt 0x13, as shown in Figure 4.

 **Figure 4: MBR instructions that enumerate the drives and overwrite sections on each disk found (Source: Recorded Future)**

In the event that a victim is using GPT-style partition tables on their boot disk, then stage 1 will not be effective. Upon reboot, Windows will not be able to boot; however, WhisperGate's MBR code, which corrupts the disk drives, will not run. Since GPT disks maintain a backup copy of the GPT table at the end of a disk, victims can restore the GPT table by running a live Linux distribution and using the gdisk utility's recovery command like shown in Figure 5.

 **Figure 5: Restoring the corrupted GPT table with the gdisk recovery command (Source: Recorded Future)**


## Stage 2: Downloader

---



Stage 2 is written in .NET, and its primary functionality is to download the third stage of the malware and execute it. It begins execution after 20 seconds, using the PowerShell command "`powershell -enc UwB0AGEAcgB0AC0AUwBsAGUAZQBwACAALQBzACAAMQAwAA==`", which decodes to "`Start-Sleep -s 10`". The 10-second delay is executed twice and is likely used to help the malware evade detection by AV engines. The malware retrieves the third stage from a Discord attachment hosted on `https://cdn[.]discordapp[.]com`, named `Tbopbh.jpg`. Stage 2 reverses the JPG file's bytes, reflectively loads the JPG file as a .NET assembly, and then calls the exported function "`YlfwdwgmPilzyaph`".

## Stage 3: File Corrupter

---

Stage 3 of the malware is written in .NET and obfuscated with eazfuscator. Upon execution, 2 embedded PE executable resources (AdvancedRun and Wagybg) are unpacked, decoded, and GZIP decompressed. Next, a .vbs script is written to “%AppData%\local\Temp\Nmddfrqqrbyjeygggda.vbs” and executed with Wscript.exe. The script, shown in Figure 6, is used to exclude the entire C drive from being scanned by Windows Defender.  **Figure 6:** Contents of “%AppData%\local\Temp\Nmddfrqqrbyjeygggda.vbs” (Source: Recorded Future)

AdvancedRun is then executed to stop the Windows Defender service and delete its program data folder. AdvancedRun is benign software developed by NirSoft and used to run programs under different settings. The author used AdvancedRun due to its ability to run programs with TrustedInstaller privileges, which are needed to execute the command that disables Windows Defender. Figures 7 and 8 show the command line arguments used to run AdvancedRun.exe. The use of the “/RunAs 8” argument instructs AdvancedRun to use the TrustedInstaller privileges.


 **Figure 7:** “AdvancedRun.exe” stopping the Windows Defender service (Source: Recorded Future)  **Figure 8:** “AdvancedRun.exe” recursively deleting Windows Defender’s program data (Source: Recorded Future)

Finally, Wagybg is run via process hollowing in an InstallUtil.exe process. A similar technique was used to load the Netwire trojan in 2019 as part of a phishing campaign. InstallUtil is a benign program produced by Microsoft and distributed as part of the .NET framework.

This stage of the malware is used to perform file corruption. It first gets a list of logical drives on the system by calling GetLogicalDrives(), then identifies those that are fixed media or network drives. The malware searches these drives for files ending in 1 of the 191 file extensions shown in Figure 9 below. It then corrupts matching files by overwriting the first 1 MiB of each file with 0xCC bytes.

 **Figure 9:** Targeted file extensions (Source: Recorded Future)

After it finishes corrupting files, the corrupter sends 5 ping requests to 111.111.111[.]111 and then deletes itself as shown in Figure 10. While it is unclear exactly why the malware makes the ping requests, we speculate that it could be to add a time delay before deleting itself or to keep a record of infected hosts.

 **Figure 10:** Self-deletion function used by the file corrupter (Source: Recorded Future)

## Mitigations

---

We recommend that organizations consider an offsite backup strategy to protect their data from the destruction capabilities of the WhisperGate malware.

- Network segmentation can prevent attackers and malware from gaining access to other parts of an organization's network. This solution involves splitting the larger network into smaller network segments and can be accomplished through firewalls, virtual local area networks, and other separation techniques.
- Consider keeping sensitive client information on systems that are disconnected from the internet or segmented from the rest of the corporate network. Since WhisperGate malware will tamper with files on a victim system, moving highly sensitive customer data to a system with no internet access or access to the rest of the network will minimize the access WhisperGate malware would have to those files.
- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and, upon review, consider blocking connection attempts to and from — the external IP address mentioned.
- If remote access solutions are crucial to daily operations, all such remote access services and protocols, such as Citrix and RDP, should be implemented with two-factor or multi-factor authentication.
- Monitor for the creation of suspicious file modification activity, particularly large quantities of file modifications in user directories.
- Set the Execution Policy for PowerShell to require that scripts be signed in order to be executed. This will only be effective for scripts being run traditionally (for example by double-clicking) and will not protect against base64-encoded scripts executed on the command line as an argument to the PowerShell program (such as powershell.exe <command>).
- Use newer versions of PowerShell, such as version 5, which added some security-related improvements.

AntiMalware Scan Interface (AMSI): This feature was introduced in Windows 10 and Windows Server 2016 and provides “file and memory or stream scanning, content source URL/IP reputation checks, and other techniques” and can integrate with PowerShell, UAC, Windows Script Host, JavaScript, VBScript, and Office VBA Macros. Research into how AMSI can be bypassed indicates that the use of obfuscation (such as XOR or base64-encoding “banned” commands) or a simple execution bypass, among other more sophisticated methods such as memory patching, can be used to get around AMSI.

- Ensure logging of scripts and commands is enabled. These include: Module Logging (records pipeline execution of PowerShell scripts, including some portions of the script, some deobfuscated code and some data formatted for output), Script Block Logging (records execution, including full contents of scripts and commands that are executed), and Transcription (creates a unique record of each PowerShell session, including input and output). While logging will not necessarily prevent malicious PowerShell from executing, it could help with understanding what kind of malicious behavior or indicators were involved.

## Outlook

---

As of this writing, it appears that DEV-0586 has only been using WhisperGate to target organizations in Ukraine. We expect more information about this threat actor, including attribution, will be published over the next few days or weeks. Now that WhisperGate has been publicly reported and security professionals have been alerted to the malware, it is possible that the developers of WhisperGate will alter the wiper to better evade detections.