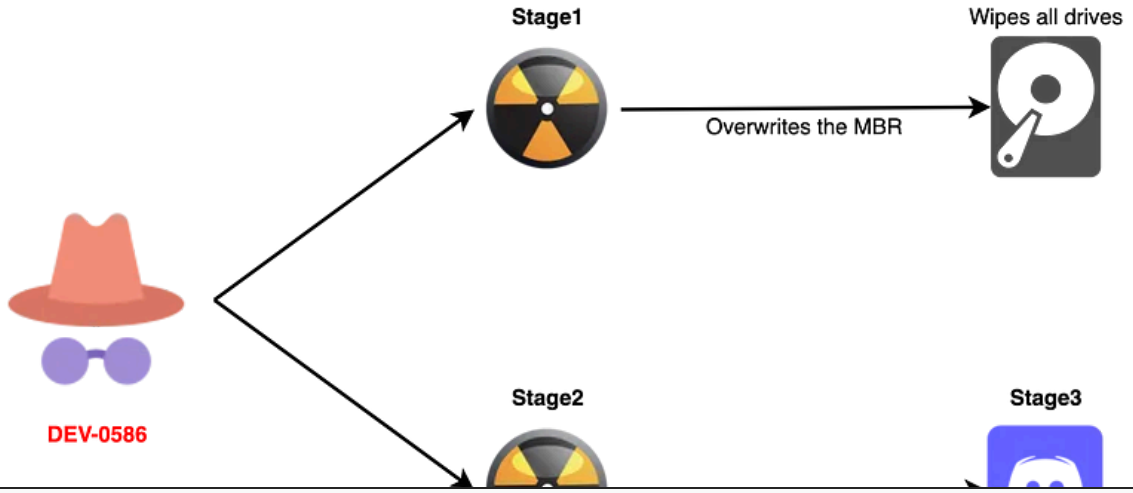
# Analysis of Destructive Malware (WhisperGate) targeting Ukraine

S2W · Follow

## Executive Summary

- 2022–01–15, MSTIC (Microsoft Threat Intelligence Center) identified and unveiled a cyberattack targeting Ukrainian organizations with "**WhisperGate**" overwrites Master Boot Record(MBR) and files.

```
An actor who conducted this attack tracked as DEV-0586 and has not
yet been attributed to existing groups
```



## Detailed Analysis

### Stage1

- SHA256: a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92
- Creation Time: 2022–01–10 10:37:18
- First Submission: 2022–01–16 20:30:19
- File Type: Win32 EXE

Write starts from LBA#1 of disk

- When disk access is successful, LBA is increased by 0xC7 (199) and written
- When disk access fails, increase the Drive Index and try to access the next disk

- Creation Time: 2022–01–10 14:39:54
- First Submission: 2022–01–16 20:31:26
- File Type: Win32 EXE

Stage2 does not perform malicious actions for 20 seconds to bypass the AV (Anti Virus). To do this, run the following command twice.

> *Command: powershell -enc*

### Stage3 (Tbopbh.jpg)

- **SHA256 :**
  923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6

### Tbopbh.jpg (Reversed)

- **SHA256 :**
  9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d

Stage3 loads “78c855a088924e92a7f60d661c3d1845” resource inside and performs decoding by XOR operation.

- AdvancedRun (GZIP Decompressed)
- Waqybg (Reversed and GZIP Decompressed)

> *"stop WinDefend" /StartDirectory "" /RunAs 8 /Run*
>
> *Command: "C:\Users\Administrator\AppData\Local\Temp\AdvancedRun.exe" /EXEFilename "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" /WindowState 0 /CommandLine "rmdir 'C:\ProgramData\Microsoft\Windows Defender' -Recurse" /StartDirectory "" /RunAs 8 /Run*

2. **Waqybg:** Overwrites target files

```
.JAR .SCH .VBS .BAT .CMD .ASM .PAS .CPP .SXM .STD .SXD .ODP .WB2
.SLK .DIF .STC .SXC .ODS .3DM .MAX .3DS .STW .SXW .ODT .PEM .P12
.CSR .CRT .KEY .PFX .DER .OGG .JAVA .INC .INI .PPK .LOG .VDI .VMDK
.VHD .MDF .MYI .MYD .FRM .SAV .ODB .DBF .MDB .ACCDB .SQL .SQLITEDB
.SQLITE3 .LDF .ARC .BAK .TAR .TGZ .RAR .ZIP .BACKUP .ISO .CONFIG
```

- Executes ping command and delete itself

> *cmd.exe /min /C ping 111.111.111.111 -n 5 -w 10 > Nul & Del /f /q \"[Filepath]\"*

## Appendix

- 923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6 (Stage3, Tbopbh.jpg)
- 9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d (Stage3, *Reversed* Tbopbh.jpg )
- 35FEEFE6BD2B982CB1A5D4C1D094E8665C51752D0A6F7E3CAE546D770C280F3A (Decoded Resource “78c855a088924e92a7f60d661c3d1845”)
- 29AE7B30ED8394C509C561F6117EA671EC412DA50D435099756BBB257FAFB10B(AdvancedRun.exe)

---


- Homepage: https://s2w.inc/
- Facebook: https://www.facebook.com/S2WLAB/
- Twitter: https://twitter.com/S2W_Official