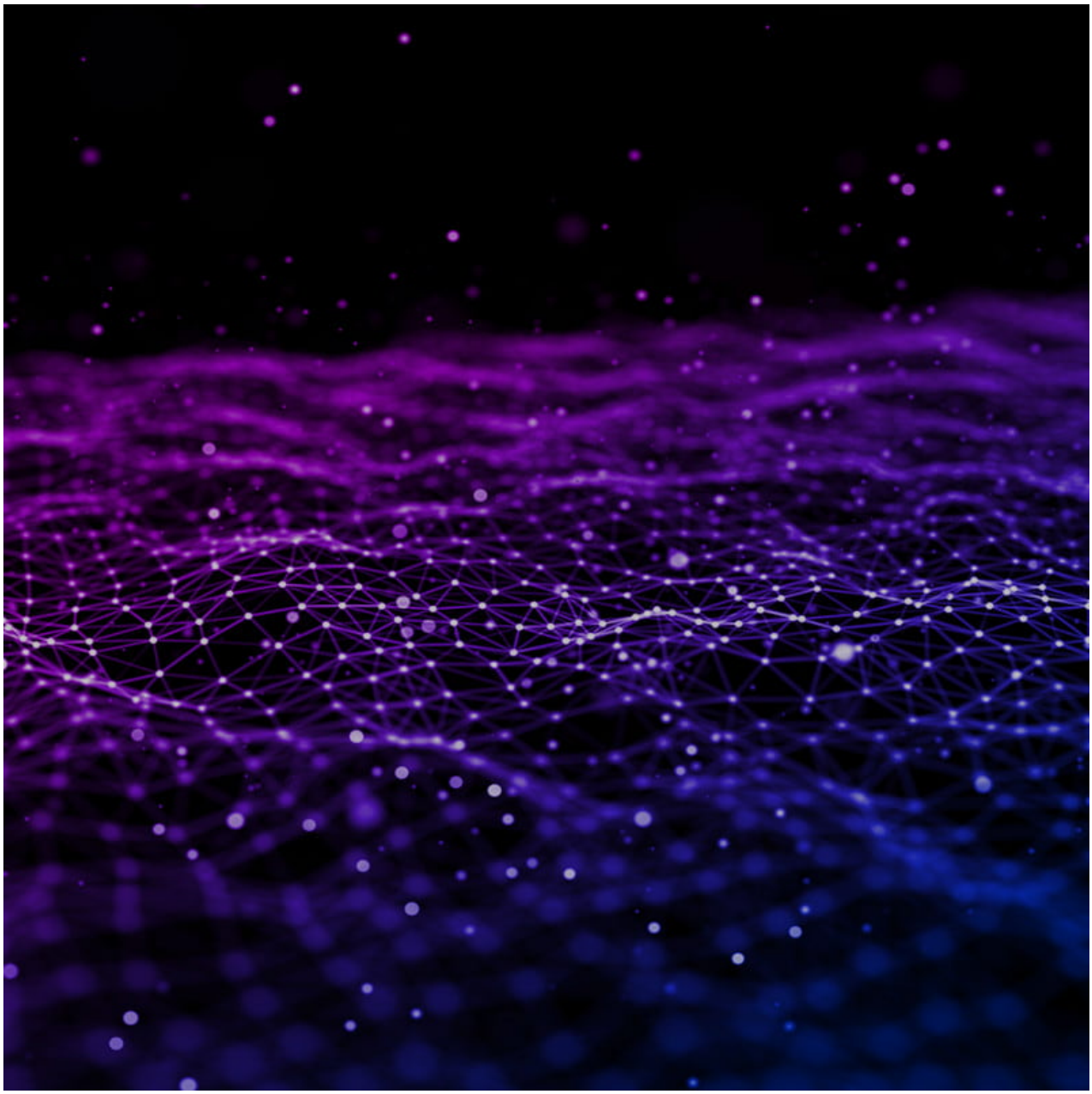
Disruptive Attacks in Ukraine Likely Linked to Escalating Tensions

secureworks.com/blog/disruptive-attacks-in-ukraine-likely-linked-to-escalating-tensions

Counter Threat Unit Research Team



Geopolitical tensions likely inspired a combination of website defacements, WhisperGate wiper malware attacks, and DDoS attacks targeting organizations in Ukraine. Friday, January 21, 2022 *By: Counter Threat Unit Research Team*
Secureworks® Counter Threat Unit™ (CTU) researchers are investigating reports of destructive malware attacks in Ukraine. On January 15, 2022, Microsoft reported a campaign that began on January 13 and leverages the WhisperGate malware. The timing coincides with defacement of Ukrainian government websites in which the content was replaced with a claim that Ukrainians' data had been breached (see Figure 1). Distributed denial of service (DDoS) attacks against some sites were also reported.

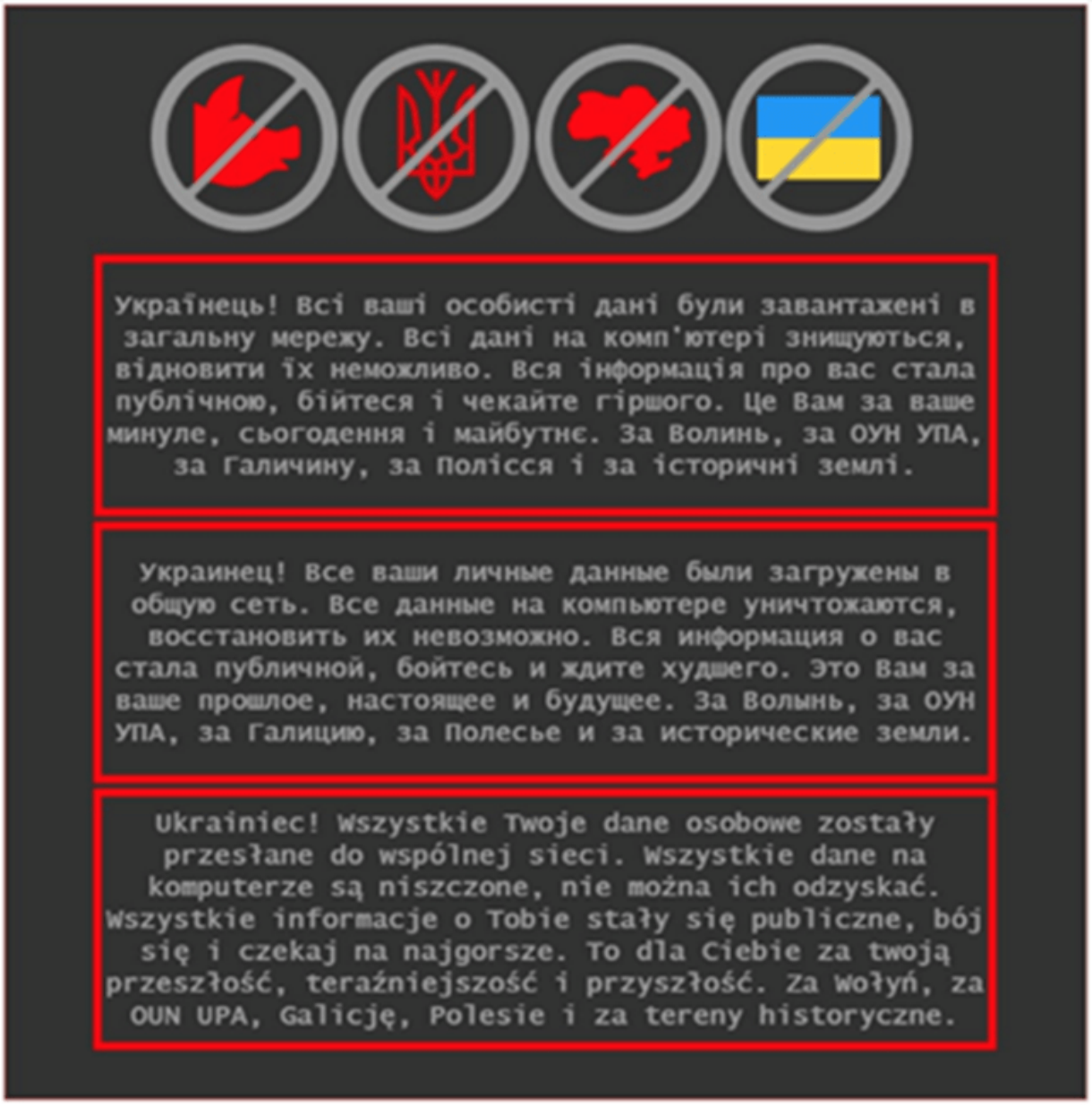


Figure 1. Defacement text on Ukrainian government websites. English translation: Ukrainian! All your personal data has been uploaded to the public network. All data on the computer is being destroyed, it is impossible to recover it. All information about you has become public, be afraid and expect the worst. This is for your past, present and future. For Volyn, for the OUN UPA, for Galicia, for Polissya and for historical lands. (Source: Secureworks)

Defacement activity

When the defacements were initially reported on January 14, it was unclear what data the threat actors meant. It may have referred to data destroyed by the WhisperGate destructive malware attacks, which had not been made public. As of this publication, no data leaks have been linked to these attacks. The threat actors could have been bluffing, or they could intend to leak the data in the future. In the defacement campaign, the threat actors made a crude attempt to suggest a Polish origin by referencing past conflicts between Poland and Ukraine and by injecting GPS coordinates into the EXIF data of the image (see Figure 2).

```
ResolutionUnit: 1
YCbCrPositioning: 1
GPSLatitudeRef: N
GPSLatitude: 52.20863049997415
GPSLongitudeRef: E
GPSLongitude: 21.009427100010672
```
Figure 2. GPS coordinates extracted from defacement image. (Source: Secureworks)

The image is not a photo and therefore would not typically contain GPS data. The coordinates map to a car park near Warsaw. The threat actors may have intended to point investigators to the adjacent General Staff of the Polish Army building (see Figure 3).

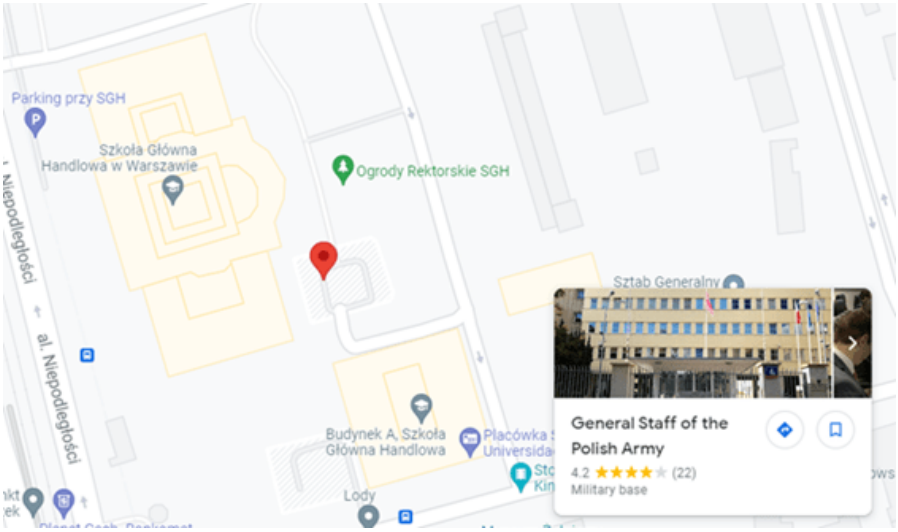


Figure 3. GPS coordinates map to a car park (red pin) near a Polish Army building. (Source: Google maps)

The Security Services of Ukraine (SSU) reported that over 70 government websites were attacked and that unauthorized access occurred on 10 of them. These numbers will likely change as investigations continue. The initial access vector for the defaced websites has not been confirmed, although several options are being investigated. The SSU indicated that a supply chain attack was used to obtain access to some of the websites, citing the compromise of a company that had administrative rights to the impacted websites. The company was not named, but as of this publication the website for Ukrainian digital technologies company Kitsoft redirects to a Facebook page that states its infrastructure was involved in the attacks. Other suggested attack vectors include exploitation of October CMS and Log4j vulnerabilities.

State Service of Special Communications and Information Protection of Ukraine reported that a subset of the organizations impacted by the defacement activity were also victims of the WhisperGate malware attacks. Details of the WhisperGate initial access vector and deployment mechanism are unclear as of this publication, although Microsoft stated that the threat actors used Impacket tools to execute the malware. WhisperGate is not a worm payload like the 2017 NotPetya ransomware, so the malware must be deployed and deliberately executed on every targeted host.

WhisperGate technical details

WhisperGate has two major components: a master boot record (MBR) wiper and a file wiper. The attackers appear to refer to these files as stage 1 (the MBR wiper) and stage 2 (the file wiper). However, these labels do not necessarily reflect the order they were executed, as the stages do not depend on each other.

The MBR wiper is written in the C programming language and compiled with the MinGW compiler. CTU™ analysis indicates that parts of the MBR wiper code are common to other MBR wiper examples found on the VirusTotal analysis service. These commonalities suggest that the WhisperGate MBR wiper developers borrowed code from publicly or privately shared source code repositories.

When executed, the MBR wiper overwrites the MBR with a small segment of code. The next time the computer is rebooted, the new MBR code displays a ransom message (see Figure 4) and attempts to overwrite the disk in the background using the BIOS Extended Write Sectors interrupt call. Testing on Windows 10 revealed the malware operates as designed. However, the malware caused a Windows 11 system to crash, likely due to the GUID Partition Table (GPT) scheme replacing the older MBR partition scheme in Windows 11.

Figure 4. Ransom message presented by WhisperGate MBR wiper. (Source: Secureworks)

Despite the use of a ransom note, there is no prospect of data recovery. This malware is a destructive wiper, not ransomware.

The file wiper involves a loader (Tbopbh.exe) and a packed payload (Tbopbh.jpg) that the loader downloads and executes. The loader is written in .NET. When executed, it uses a PowerShell command to sleep for 20 seconds, likely as an antivirus or sandbox evasion tactic. It then downloads the packed payload from a Discord channel (see Figure 5).

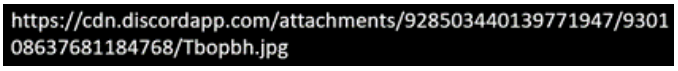


Figure 5. Discord channel hosting WhisperGate payload. (Source: Secureworks)

Although the payload's filename suggests that it is a JPG image file, it is a DLL file. The file byte order is reversed, likely to evade detection by host-based controls. The loader restores the byte order and then performs multiple rounds of extraction and decoding of nested resources to get to the final malicious code. Figure 6 shows the processes created during unpacking. The final malicious files are dropped into C:\Users\<*username*>\AppData\Local\Temp\. The loader attempts to disable Microsoft Defender Antivirus.

Figure 6. Process tree showing execution of the WhisperGate file wiper. (Source: Secureworks)

The loader drops Nmddfrqqrbyjeygggda.vbs, which contains a one-line script to exclude the C:\ drive from locations monitored by Microsoft Defender Antivirus (see Figure 7). The loader drops the AdvancedRun.exe NirSoft tool to stop the antivirus service and recursively remove its starting directory.

```
CreateObject("WScript.Shell").Run "powershell Set-MpPreference -ExclusionPath 'C:\'", 0, False
```
Figure 7. Contents of Nmddfrqqrbyjeygggda.vbs. (Source: Secureworks)

InstallUtil.exe is copied from C:\Windows\Microsoft.NET\Framework\v4.0.30319\ and written to C:\Users\<*username*>\AppData\Local\Temp\. This file is used to create the host process where the final wiper payload is injected, using a technique known as process hollowing. The code also included a function that runs a command (cmd.exe /min /C ping 111.111.111.111 -n 5 -w 10 > Nul & Del /f /q "%s") that uses ping to inject a brief time delay before deleting a file. However, CTU researchers did not observe this command being run the sandbox execution of the malware.

Like the MBR wiper, the file wiper code is written in C and compiled using MinGW. The file wiper targets a hard-coded list of file extensions (see Figure 8). It destroys data in identified files by writing 0xCC to the first 0x100000 bytes, which translates to approximately 1MB of data. The list includes file types that are not typically targeted by ransomware, such as the .602 extension used by a Czech word processor. The WCry (also known as WannaCry) ransomware targeted this extension, but there is no known connection between the two malware families.

```
.HTML .HTM .SHTML .XHTML .PHTML .PHP .JSP .ASP .PHPS .PHP5 .ASPX .PHP4 .PHP6
.PHP7 .PHP3 .DOC .DOCX .XLS .XLSX .PPT .PPTX .PST .OST .MSG .EML .VSD .VSDX
.TXT .CSV .RTF .WKS .WK1 .PDF .DWG .ONETOC2 .SNT .JPEG .JPG .DOCB .DOCM .DOT
.DOTM .DOTX .XLSM .XLSB .XLW .XLT .XLM .XLC .XLTX .XLTM .PPTM .POT .PPS .PPSM
.PPSX .PPAM .POTX .POTM .EDB .HWP .602 .SXI .STI .SLDX .SLDM .BMP .PNG .GIF
.RAW .CGM .SLN .TIF .TIFF .NEF .PSD .AI .SVG .DJVU .SH .CLASS .JAR .BRD .SCH
.DCH .DIP .PL .VB .VBS .PS1 .BAT .CMD .JS .ASM .H .PAS .CPP .C .CS .SUO .ASC
.LAY6 .LAY .MML .SXM .OTG .ODG .UOP .STD .SXD .OTP .ODP .WB2 .SLK .DIF .STC
.SXC .OTS .ODS .3DM .MAX .3DS .UOT .STW .SXW .OTT .ODT .PEM .P12 .CSR .CRT
.KEY .PFX .DER .OGG .RB .GO .JAVA .INC .WAR .PY .KDBX .INI .YML .PPK .LOG
.VDI .VMDK .VHD .HDD .NVRAM .VMSD .VMSN .VMSS .VMTM .VMX .VMXF .VSWP .VMTX
.VMEM .MDF .IBD .MYI .MYD .FRM .SAV .ODB .DBF .DB .MDB .ACCDB .SQL .SQLITEDB
.SQLITE3 .LDF .SQ3 .ARC .PAQ .BZ2 .TBK .BAK .TAR .TGZ .GZ .7Z .RAR .ZIP
.BACKUP .ISO .VCD .BZ .CONFIG
```

Figure 8. Extensions targeted by the WhisperGate file wiper. (Source: Secureworks)

Figure 9 shows an example of the autoexec.bat file being overwritten.

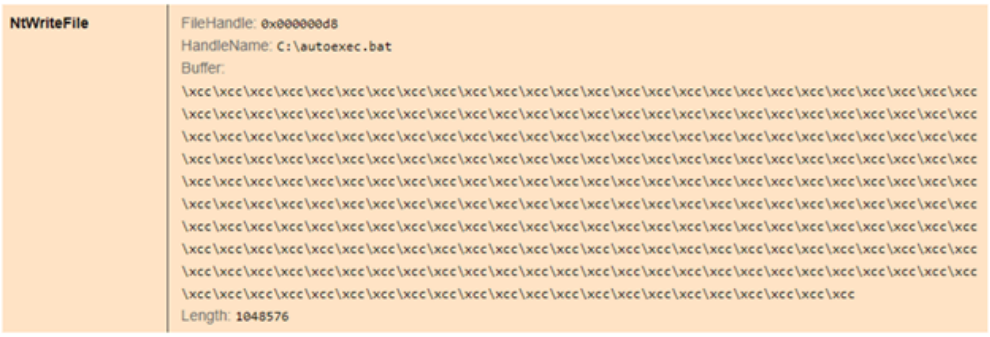


Figure 9. Overwrite of autoexec.bat. (Source: Secureworks)

Based on analysis of additional samples that appeared to use the same loading and packing mechanism but were unrelated to WhisperGate, it is likely that the WhisperGate developers used PureCrypter or a similar crimeware crypter to generate the .NET code in both the loader (Tbopbh.exe) and the initial payload (Tbopbh.jpg) of the file wiper. Detection rules based on these components will likely match other crimeware components unrelated to WhisperGate. A YouTube video posted by user Pure Coder demonstrates PureCrypter features such as the Advanced Runtime (AdvancedRun.exe), Windows Defender Exclusion, and Disable functionality. The tool allows the operator to select the process where the payload is injected. Options include InstallUtil, as used by WhisperGate (see Figure 10).

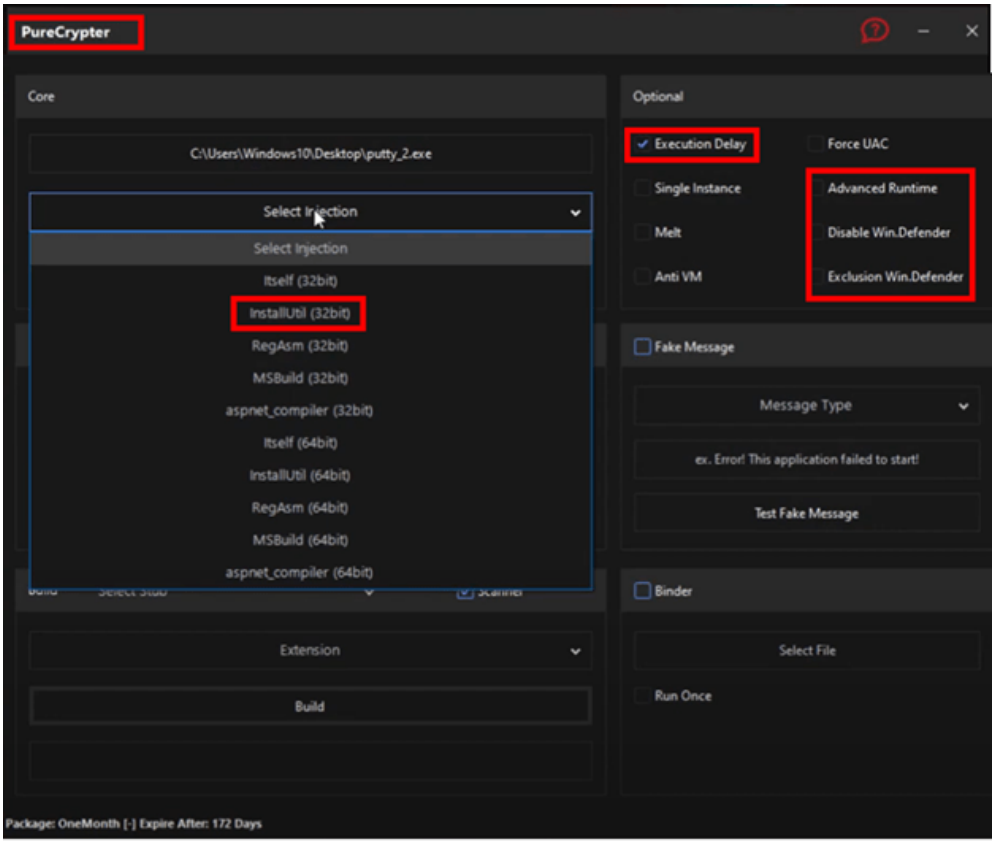


Figure 10. PureCrypter panel. (Source: Secureworks)

Attribution

As of this publication, there is insufficient evidence to determine attribution for the Ukrainian defacement, DDoS, and wiper attacks. However, it is highly likely that they are linked to the current geopolitical tensions centered on the border between Ukraine and Russia. If tensions are not deescalated, additional cyberattacks are likely. These attacks do not have the sophistication or destructive power of previous attacks on Ukraine, such as NotPetya. The threat actors attempted to misdirect attribution using inauthentic metadata and used publicly available crimeware services and code to minimize the amount of custom code involved in the attack.

Recommendations

Organizations with operations in Ukraine should be extra vigilant and review business continuity and resilience plans. Organizations should maintain current backups of business-critical systems and data, exercise restoration processes before they are needed, and ensure that backups cannot be impacted by ransomware-style or wiper malware attacks. Organizations should also prepare for continuity of operations in the case of power disruptions or loss of other business-critical services.

It is unlikely that organizations outside of Ukraine or unrelated to the political situation will be directly targeted. However, organizations should consider their exposure to collateral damage from attacks launched in Ukraine that could spread to global operations. Impacted organizations could include business partners and service providers in Ukraine that have logical access to customer networks. Applying robust network segmentation between higher risk and lower risk areas can mitigate risk. Additionally, all organizations should maintain basic security practices such as patching internet-facing systems against known vulnerabilities, implementing and maintaining antivirus solutions, and monitoring endpoint detection and response solutions.

For more information about WhisperGate versus NotPetya, read the accompanying blog post.

Threat indicators

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1.

Indicator	Type	Context
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	SHA256 hash	WhisperGate MBR wiper
189166d382c73c242ba45889d57980548d4ba37e	SHA1 hash	WhisperGate MBR wiper
5d5c99a08a7d927346ca2dafa7973fc1	MD5 hash	WhisperGate MBR wiper
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	SHA256 hash	WhisperGate file wiper loader (Tbopbh.exe)
16525cb2fd86dce842107eb1ba6174b23f188537	SHA1 hash	WhisperGate file wiper loader (Tbopbh.exe)
14c8482f302b5e81e3fa1b18a509289d	MD5 hash	WhisperGate file wiper loader (Tbopbh.exe)
923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6	SHA256 hash	WhisperGate file wiper packed payload (Tbopbh.jpg)
b2d863fc444b99c479859ad7f012b840f896172e	SHA1 hash	WhisperGate file wiper packed payload (Tbopbh.jpg)
b3370eb3c5ef6c536195b3bea0120929	MD5 hash	WhisperGate file wiper packed payload (Tbopbh.jpg)
9ef7dbd3da51332a78eff19146d21c82957821e464e8133e9594a07d716d892d	SHA256 hash	WhisperGate file wiper packed DLL (Frkmlkdkdubkznbkmcf.dll)
82d29b52e35e7938e7ee610c04ea9daaf5e08e90	SHA1 hash	WhisperGate file wiper packed DLL (Frkmlkdkdubkznbkmcf.dll)
e61518ae9454a563b8f842286bbdb87b	MD5 hash	WhisperGate file wiper packed DLL (Frkmlkdkdubkznbkmcf.dll)
Nmddfrqqrbyjeygggda.vbs	Filename	WhisperGate malware script
Tbopbh.exe	Filename	WhisperGate file wiper loader
Tbopbh.jpg	Filename	WhisperGate file wiper packed payload
Frkmlkdkdubkznbkmcf.dll	Filename	WhisperGate file wiper packed DLL

Table 1. Indicators for this threat.

If you need urgent assistance with an incident, contact the Secureworks Incident Response team. For other questions on how we can help, use our general contact form.