Microsoft: Fake ransomware targets Ukraine in data-wiping attacks

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)** January 16, 2022 01:32 PM **0**

Microsoft is warning of destructive data-wiping malware disguised as ransomware being used in attacks against multiple organizations in Ukraine.

Starting January 13th, Microsoft detected the new attacks that combined a destructive MBRLocker with a data-corrupting malware used to destroy the victim's data intentionally.

A two-stage attack destroys data

Microsoft calls this new malware family 'WhisperGate' and explains in a report that it is conducted through two different destructive malware components.

The first component, named **stage1.exe**, is launched from the *C:\PerfLogs*, *C:\ProgramData*, *C:*, or *C:\temp* folders that overwrites the Master Boot Record to display a ransom note.

An MBR locker is a program that replaces the 'master boot record,' a location on a computer's hard drive that contains information on disk partitions and a small executable that is used to load the operating system.

MBR lockers replace the loader in the master boot record with a program that commonly encrypts the partition table and displays a ransom note. This prevents the operating system from loading and data from being accessible until a ransom is paid and a decryption key is obtained.

The WhisperGate ransom note, shown below, tells the victim to send $10,000 in bitcoin to the 1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv (https://www.blockchain.com/btc/address/1AVNM68gj6PGPFcJuftKATa4WLnzg8fpfv) address and then contact the threat actors via an included Tox chat ID.

```
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 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5
D82C1ED23054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

While Microsoft points to the use of Tox as a reason for the ransomware being fake, BleepingComputer knows of numerous ransomware operations that use Tox as a communication method, so this is not unusual.

However, the MBRLocker's ransom note uses the same bitcoin address for all victims and does not provide a method to input a decryption key. When combined, this typically indicates fake ransomware designed for destructive purposes.

The second component, named **stage2.exe**, is executed simultaneously to download a data-destroying malware named **Tbopbh.jpg** hosted on Discord that overwrites targeted files with static data.

"If a file carries one of the extensions above, the corrupter overwrites the contents of the file with a fixed number of 0xCC bytes (total file size of 1MB)," explains Microsoft's report (https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/).

"After overwriting the contents, the destructor renames each file with a seemingly random four-byte extension."

The file extensions targeted by the stage2 component for corruption are:

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

As neither of the two malware components offer means to enter decryption keys to restore the original Master Boot Record and as the files are overwritten with static undecryptable data, Microsoft classifies this as a destructive attack rather than one used to generate a ransom payment.

Indicators of compromise and download links for the malware samples can be found in the IOC section later in the article.

Microsoft is unable to attribute the attacks to any particular threat actor and is tracking the hacker's activities as DEV-0586.

With the geopolitical tensions escalating in the region between Russia and Ukraine, it is believed that these attacks are designed to sow chaos in Ukraine.

A similar attack was conducted in 2017 when thousands of Ukrainian businesses were targeted with the NotPetya ransomware (https://www.bleepingcomputer.com/news/security/surprise-notpetya-is-a-cyber-weapon-its-not-ransomware/).

While NotPetya was based on real ransomware known as Petya (https://www.bleepingcomputer.com/news/security/petya-ransomware-skips-the-files-and-encrypts-your-hard-drive-instead/), the NotPetya attacks were conducted as a cyberweapon against Ukraine rather than to generate payments.

In 2020, the USA formally indicted Russian GRU hackers (https://www.bleepingcomputer.com/news/security/us-indicts-russian-gru-sandworm-hackers-for-notpetya-worldwide-attacks/) believed to be

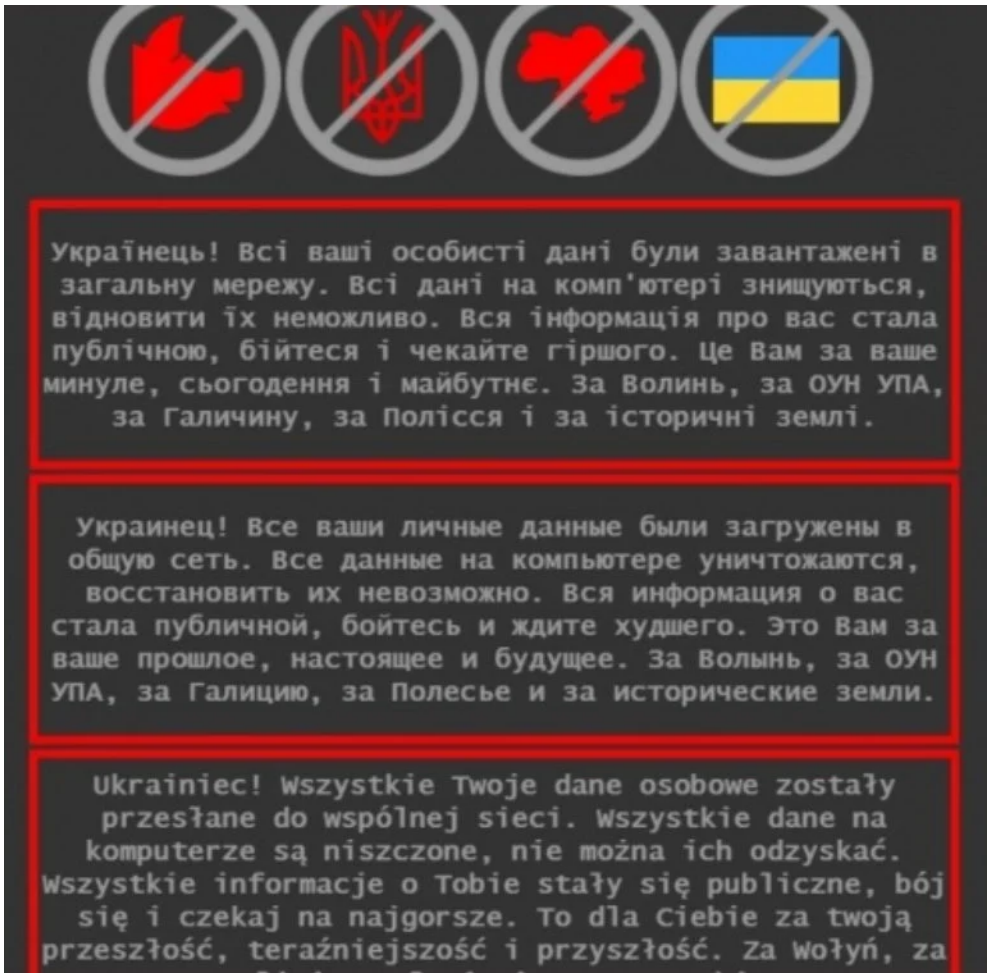
part of the elite Russian hacking group known as "Sandworm" for the NotPetya attacks.

Ukraine under siege by cyberattacks

This week, at least fifteen websites of Ukrainian public institutions and government agencies were hacked, defaced, and subsequently taken offline.

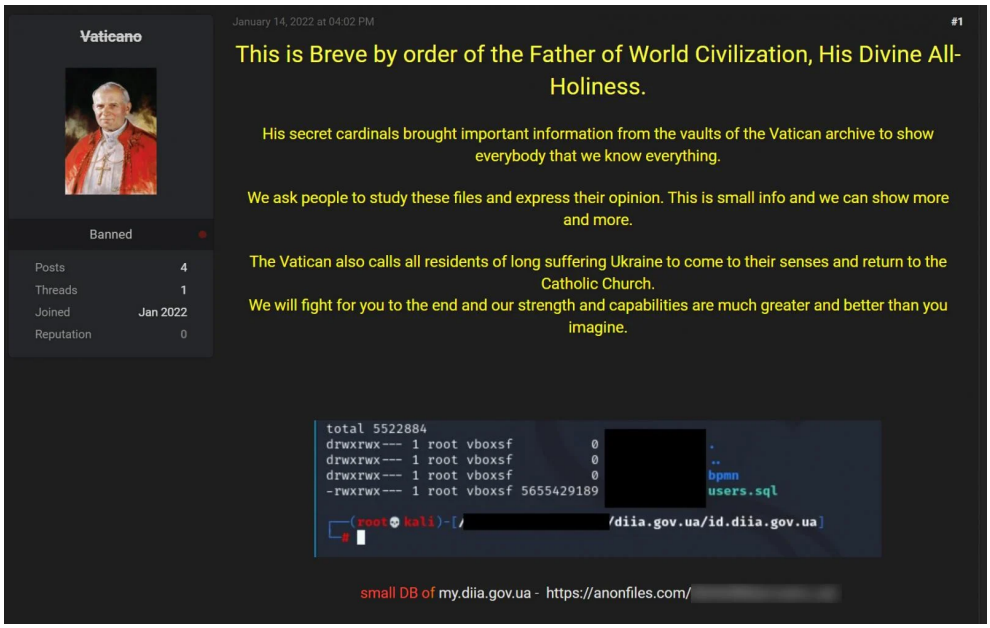
Hackers defaced these websites (https://www.bleepingcomputer.com/news/security/multiple-ukrainian-government-websites-hacked-and-defaced/) to show a message warning visitors that their data was stolen and publicly shared online.

"Ukrainian! All your personal data has been uploaded to the public network. All data on the computer is destroyed, it is impossible to recover them. 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," reads the translated website defacement.



Ukrainian website defacement

As part of this intimidation campaign, the threat actors created new accounts on the popular RaidForums hacking forum to release the allegedly stolen data.



Allegedly stolen data from Ukrainian government agency

However, threat actors who have reviewed the published data say it is unrelated to Ukraine government agencies and contains data from an old leak.

Ukraine has attributed the attacks to Russia, with the goal of undermining the confidence in the Ukrainian government.

"Russia's cyber-troops are often working against the United States and Ukraine, trying to use technology to shake up the political situation. The latest cyber attack is one of the manifestations of Russia's hybrid war against Ukraine, which has been going on since 2014," the Ukraine government announced (https://thedigital.gov.ua/news/rosiya-mae-namir-zniziti-doviru-do-vladi-feykami-pro-vrazlivist-kritichnoi-informatsiynoi-infrastrukturi-ta-zliv-danikh-ukraintsiv) today.

"Its goal is not only to intimidate society. And to destabilize the situation in Ukraine by stopping the work of the public sector and undermining the confidence in the government on the part of Ukrainians. They can

achieve this by throwing fakes into the infospace about the vulnerability of critical information infrastructure and the "drain" of personal data of Ukrainians."

Related Articles:

Ukranian police arrests ransomware gang that hit over 50 firms (https://www.bleepingcomputer.com/news/security/ukranian-police-arrests-ransomware-gang-that-hit-over-50-firms/)

Russia charges 8 suspected REvil ransomware gang members (https://www.bleepingcomputer.com/news/security/russia-charges-8-suspected-revil-ransomware-gang-members/)

Qlocker ransomware returns to target QNAP NAS devices worldwide (https://www.bleepingcomputer.com/news/security/qlocker-ransomware-returns-to-target-qnap-nas-devices-worldwide/)

The Week in Ransomware - January 14th 2022 - Russia finally takes action (https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-january-14th-2022-russia-finally-takes-action/)

Russia arrests REvil ransomware gang members, seize $6.6 million (https://www.bleepingcomputer.com/news/security/russia-arrests-revil-ransomware-gang-members-seize-66-million/)

IOCs

Stage1.exe:
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92 [VirusTotal (https://www.virustotal.com/gui/file/a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92)] [MalShare (https://malshare.com/sample.php?action=detail&hash=5d5c99a08a7d927346ca2dafa7973fc1)]

Stage2.exe:
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78 [VirusTotal (https://www.virustotal.com/gui/file/dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78)] [MalShare (https://malshare.com/sample.php?action=detail&hash=14c8482f302b5e81e3fa1b18a509289d)]

Tbopbh.jpg (third stage):
923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6 [VirusTotal (https://www.virustotal.com/gui/file/923eb77b3c9e11d6c56052318c119c1a22d11ab71675e6b95d05eeb73d1accd6)] [MalShare