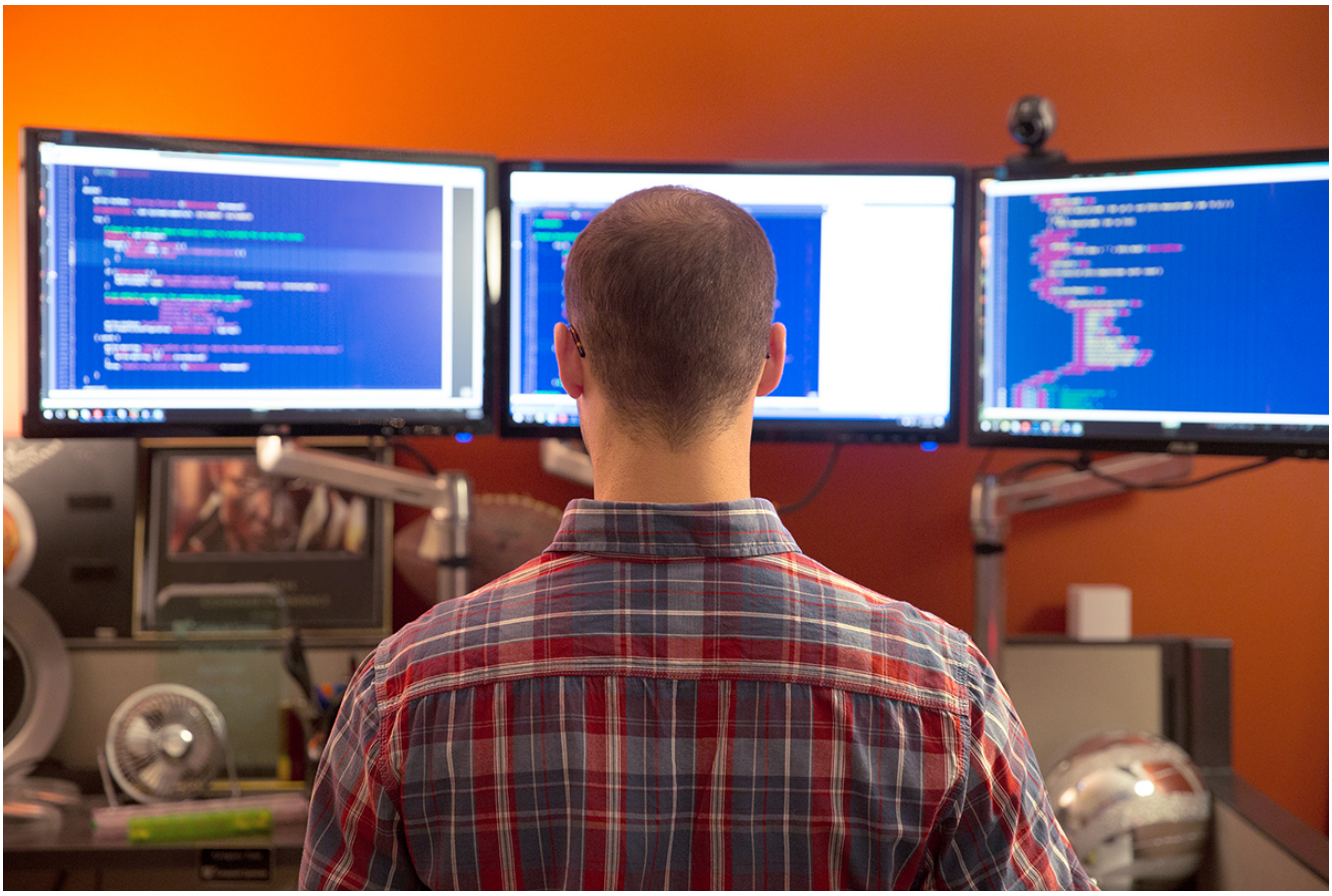
Destructive malware targeting Ukrainian organizations

microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

January 16, 2022



Microsoft Threat Intelligence Center (MSTIC) has identified evidence of a destructive malware operation targeting multiple organizations in Ukraine. This malware first appeared on victim systems in Ukraine on January 13, 2022. Microsoft is aware of the ongoing geopolitical events in Ukraine and surrounding region and encourages organizations to use the information in this post to proactively protect from any malicious activity.

While our investigation is continuing, MSTIC has not found any notable associations between this observed activity, tracked as DEV-0586, and other known activity groups. MSTIC assesses that the malware, which is designed to look like ransomware but lacking a ransom recovery mechanism, is intended to be destructive and designed to render targeted devices inoperable rather than to obtain a ransom.

At present and based on Microsoft visibility, our investigation teams have identified the malware on dozens of impacted systems and that number could grow as our investigation continues. These systems span multiple government, non-profit, and information technology organizations, all based in Ukraine. We do not know the current stage of this attacker's operational cycle or how many other victim organizations may exist in Ukraine or other geographic locations. However, it is unlikely these impacted systems represent the full scope of impact as other organizations are reporting.

Given the scale of the observed intrusions, MSTIC is not able to assess intent of the identified destructive actions but does believe these actions represent an elevated risk to any government agency, non-profit or enterprise located or with systems in Ukraine. We strongly encourage all organizations to immediately conduct a thorough investigation and to implement defenses using the information provided in this post. MSTIC will update this blog as we have additional information to share.

As with any observed nation-state actor activity, Microsoft directly and proactively notifies customers that have been targeted or compromised, providing them with the information they need to guide their investigations. MSTIC is also actively working with members of the global security community and other strategic partners to share information that can address this evolving threat through multiple channels. Microsoft uses DEV-#### designations as a temporary name given to an unknown, emerging, or a developing cluster of threat activity, allowing MSTIC to track it as a unique set of information until we reach a high confidence about the origin or identity of the actor behind the activity. Once it meets the criteria, a DEV is converted to a named actor or merged with existing actors.

Observed actor activity

On January 13, Microsoft identified intrusion activity originating from Ukraine that appeared to be possible Master Boot Records (MBR) Wiper activity. During our investigation, we found a unique malware capability being used in intrusion attacks against multiple victim organizations in Ukraine.

Stage 1: Overwrite Master Boot Record to display a faked ransom note

The malware resides in various working directories, including *C:\PerfLogs*, *C:\ProgramData*, *C:\,* and *C:\temp*, and is often named *stage1.exe*. In the observed intrusions, the malware executes via Impacket, a publicly available capability often used by threat actors for lateral movement and execution.

The two-stage malware overwrites the Master Boot Record (MBR) on victim systems with a ransom note (Stage 1). The MBR is the part of a hard drive that tells the computer how to load its operating system. The ransom note contains a Bitcoin wallet and Tox ID (a unique account identifier used in the Tox encrypted messaging protocol) that have not been previously observed by MSTIC:

```
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 8BEDC411012A33BA34F49130D0F186993C6A32DAD8976F6A5D82C1ED23054C057ECED5496F65
with your organization name.
We will contact you to give further instructions.
```

The malware executes when the associated device is powered down. Overwriting the MBR is atypical for cybercriminal ransomware. In reality, the ransomware note is a ruse and that the malware destructs MBR and the contents of the files it targets. There are several reasons why this activity is inconsistent with cybercriminal ransomware activity observed by MSTIC, including:

- Ransomware payloads are typically customized per victim. In this case, the same ransom payload was observed at multiple victims.
- Virtually all ransomware encrypts the contents of files on the filesystem. The malware in this case overwrites the MBR with no mechanism for recovery.

- Explicit payment amounts and cryptocurrency wallet addresses are rarely specified in modern criminal ransom notes, but were specified by DEV-0586. The same Bitcoin wallet address has been observed across all DEV-0586 intrusions and at the time of analysis, the only activity was a small transfer on January 14.
- It is rare for the communication method to be only a Tox ID, an identifier for use with the Tox encrypted messaging protocol. Typically, there are websites with support forums or multiple methods of contact (including email) to make it easy for the victim to successfully make contact.
- Most criminal ransom notes include a custom ID that a victim is instructed to send in their communications to the attackers. This is an important part of the process where the custom ID maps on the backend of the ransomware operation to a victim-specific decryption key. The ransom note in this case does not include a custom ID.

Microsoft will continue to monitor DEV-0586 activity and implement protections for our customers. The current detections, advanced detections, and IOCs in place across our security products are detailed below.

Stage 2: File corrupter malware

Stage2.exe is a downloader for a malicious file corrupter malware. Upon execution, *stage2.exe* downloads the next-stage malware hosted on a Discord channel, with the download link hardcoded in the downloader. The next-stage malware can best be described as a malicious file corrupter. Once executed in memory, the corrupter locates files in certain directories on the system with one of the following hardcoded file extensions:

```
.3DM .3DS .7Z .ACCDB .AI .ARC .ASC .ASM .ASP .ASPX .BACKUP .BAK .BAT .BMP .BRD .BZ .BZ2 .CGM
.CLASS .CMD .CONFIG .CPP .CRT .CS .CSR .CSV .DB .DBF .DCH .DER .DIF .DIP .DJVU.SH .DOC .DOCB
.DOCM .DOCX .DOT .DOTM .DOTX .DWG .EDB .EML .FRM .GIF .GO .GZ .HDD .HTM .HTML .HWP .IBD .INC
.INI .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 .TBK .TGZ .TIF .TIFF .TXT .UOP .UOT .VB .VBS .VCD .VDI .VHD
.VMDK .VMEM .VMSD .VMSN .VMSS .VMTM .VMTX .VMX .VMXF .VSD .VSDX .VSWP .WAR .WB2 .WK1 .WKS .XHTML
.XLC .XLM .XLS .XLSB .XLSM .XLSX .XLT .XLTM .XLTX .XLW .YML .ZIP
```

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). After overwriting the contents, the destructor renames each file with a seemingly random four-byte extension. Analysis of this malware is ongoing.

Recommended customer actions

MSTIC and the Microsoft security teams are working to create and implement detections for this activity. To date, Microsoft has implemented protections to detect this malware family as WhisperGate (e.g., DoS:Win32/WhisperGate.A!dha) via Microsoft Defender Antivirus and Microsoft Defender for Endpoint, wherever these are deployed on-premises and cloud environments. We are continuing the investigation and will share significant updates with affected customers, as well as public and private sector partners, as get more information. The techniques used by the actor and described in the this post can be mitigated by adopting the security considerations provided below:

- Use the included indicators of compromise to investigate whether they exist in your environment and assess for potential intrusion.

- Review all authentication activity for remote access infrastructure, with a particular focus on accounts configured with single factor authentication, to confirm authenticity and investigate any anomalous activity.
- Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity. *NOTE:* Microsoft strongly encourages all customers download and use password-less solutions like Microsoft Authenticator to secure accounts.
- Enable Controlled folder Access (CFA) in Microsoft Defender for Endpoint to prevent MBR/VBR modification.

Indicators of compromise (IOCs)

The following list provides IOCs observed during our investigation. We encourage customers to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems.

Indicator	Type	Description
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	SHA-256	Hash of destructive malware *stage1.exe*
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	SHA-256	Hash of *stage2.exe*
cmd.exe /Q /c start c:\stage1.exe 1> \\127.0.0.1\ADMIN$__[TIMESTAMP] 2>&1	Command line	Example Impacket command line showing the execution of the destructive malware. The working directory has varied in observed intrusions.

NOTE: These indicators should not be considered exhaustive for this observed activity.

Detections

Microsoft 365 Defender

Antivirus