HUNTER
EMERGING THREATS

WHISPERGATE MALWARE - UPDATE

Cyborg Security has published additional hunt packages, as well as updated a hunt package already available in the Hunter platform, as a result of additional analysis and research of the WhisperGate attack. These new packages work to identify techniques employed by WhisperGate specifically, as well as broader techniques employed by multiple malware variants. Each of the packages help to identify a portion of the attack chain observed by the stage 2 and stage 3 binaries utilized in the WhisperGate attack against the Ukrainian government in January 2022. Multiple packages were developed around general techniques, with the intent to identify future attacks by the same group or malware, even if revisions are made, as well as other malwares employing techniques in similar ways.

CYBORG SECURITY

Threat Summary

The WhisperGate malware variant was first identified by the MSTIC (Microsoft Threat Intelligence center) on January 13, 2022 and has attributed to the nation-state threat group given the name \"DEV-0586\" (temporary name given by MS until origin/identity is received).

This threat group has been observed conducting operations on Ukrainian government and organizations, during the geopolitical tensions between Ukraine and Russia. Specific Intent and targets was not identified in the MSTIC article but due to the political climate, systems within or associated to Ukraine should be prepared accordingly - as of today, there has been dozens of impacted systems identified and potentially growing that fall under that umbrella.

The variant has been observed as a Wiper, disguised as ransomware - similar to the NotPetya attack in 2017. Seen in both variants, a ransom demand is displayed upon boot but is deceptive, as the malware wipes data files rather than encrypting them like typical ransomware does. The intent is destruction rather than using the data as leverage. Although currently targeting Ukraine, the potentiality of this malware or a modified version of it or its techniques being utilized by another threat group is possible.

Synopsis

The WhisperGate malware variant was discovered targeting Ukraine government and organizations in early January by the MSTIC, and identified as a form of Wiper malware that is masquerading as ransomware. With that being said, although the variant is designed to be ransomware, there is no intention of allowing the recovery of the data that is affected. This reveals that the intent of the actor is seeking damage, rather than leverage with infections.

The malware has been observed to have two stages, the first is the overwriting of the Master Boot Records - this is where the fake ransom note is revealed as well to the victim. Due to the Master Boot Record being corrupted/overwritten, the recovery of the system if the user decides to potentially reboot or shutdown/startup. The MSTIC report mentions that the ransom note is unusual in the way it is crafted as well, with the irregularities including the same explicit payment amounts and wallet addresses being specified for each note and the absence of a custom ID that a victim is usually told to reference in communications.

The second stage that has been observed is the execution of a downloader (identified as Stage2.exe), that pulls the next stage malware and executes in memory. The malware then sprawls and corrupts files in specified directories on the system with specific file extensions (the specific extensions can be found in the MSTIC report). The corruption entails the overwriting of the contents of the file and renaming them with a random extension.

Further information regarding WhisperGate, as well as the extensions mentioned and IOCs identified can be found at the original MSTIC article at:
https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations

Hunt Packages

[Sign up for Free HUNTER Access]

AdvancedRun/InstallUtil Utilities Executed From Unusual Directory
As part of stage3 and stage4 of the WhisperGate malware attack, the WhisperGate malware dropped AdvancedRun.exe to the host's temp directory, and copied InstallUtil.exe from it's default location to AppData\Local\Temp. In the case of InstallUtil.exe, the malware utilized this for process hallowing to have a legitimate appearing binary running malicious code injected by WhisperGate. The AdvancedRun.exe utility was utilized by WhisperGate to further impair Windows Defender beyond the path exclusions added by a VBS file.
https://hunter.cyborgsecurity.io/details/use-case/74aab14a-4f32-498c-8e9d-d13cfd064744

Microsoft Defender Overly Broad Exclusion Change via PowerShell - Potential Malware Infection
Microsoft Windows Defender can be modified via PowerShell Set-MpPrefernce function. This allows setting exclusions for folders, processes, extensions, IPs as well as other configuration changes. Although a package already available in Hunter could identify when the Set-MpPreference was utilized (https://hunter.cyborgsecurity.io/details/use-case/aa6e2535-e1e3-4f0f-80e4-68cc47fc2684), this package focuses more on the specific folders being added as exclusions. The logic was developed based on research performed by Cyborg Security analysts, revealing several commands performed by PowerShell to inhibit Windows Defender's abilities to protect the compromised host. In the WhisperGate attack, the C:\ "folder" (root drive) was added as an excluded path. Cyborg Security analysts took this a step further and added other commonly abused folders by malware, which may be attempted in future attacks to exclude from monitoring or protection.
https://hunter.cyborgsecurity.io/details/use-case/32aa754b-f078-4d7f-aceb-ffc9b74d1191

VBS File Written to AppData\Local\Temp Directory - Potential Defense Evasion
Analysis and research revealed the stage3 binary associated with the WhisperGate malware attack on the Ukrainian government, the use of a VBS file dropped into the host's temp directory. This VBS file, located in AppData\Local\Temp, was utilized to run PowerShell commands to impair Windows Defender.
https://hunter.cyborgsecurity.io/details/use-case/b75bbec2-6ef3-4914-b640-3771c613f183

Windows Defender Bypass via Deleting the Directory - CommandLine Arguments
This packages identifies the activity surrounding command-line arguments that are executed to remove the Windows Defender directory (C:\ProgramData\Microsoft\Windows Defender) via PowerShell script block logging.
https://hunter.cyborgsecurity.io/details/use-case/d489b464-2127-4cd5-bf32-56fbd32ddef7

Execute Payload as Trusted Installer
This will identify the use of administrative tools to execute a payload as a Trusted Installer in order to elevate privileges and bypass security controls.
https://hunter.cyborgsecurity.io/details/use-case/d8160c37-219d-43c4-a975-90770d2e4437

Hunt Packages Continued

[Sign up for Free HUNTER Access]

Windows Defender Tampering - Possible Malware Activity
https://hunter.cyborgsecurity.io/details/use-case/aa6e2535-e1e3-4f0f-80e4-68cc47fc2684

DLL File Dropped in AppData Directory Matching WhisperGate Schema
https://hunter.cyborgsecurity.io/details/use-case/e37582e3-f7dc-4d40-907f-9b2a3063a1db

Potential Download from Discord - Known Malware Delivery Technique
https://hunter.cyborgsecurity.io/details/use-case/f03300e2-df9f-4b3b-8fae-2ff170e4aa38

Network Activity to Discord By Non-Discord App - Possible Malware Payload Delivery
https://hunter.cyborgsecurity.io/details/use-case/f5f4d9cc-b4cd-40eb-af06-a5dfa03b95fb

WScript Executing VBS From Temp Folder Locations - Potential Malware
https://hunter.cyborgsecurity.io/details/use-case/5b2420d4-68de-47a8-bce3-123e918ee2ff

Context

MITRE:

- Tactic Names:
  - Command and Control
  - Privilege Escalation
  - Defense Evasion
  - Execution
- Technique Names:
  - InstallUtil
  - Access Token Manipulation
  - Command and Scripting Interpreter
  - Visual Basic
  - Trusted Developer Utilities Proxy Execution
  - PowerShell
  - Disable or Modify Tools
  - Process Injection
  - Ingress Tool Transfer
  - Web Service
- Threat Names:
  - WhisperGate
  - Meteor

References

https://medium.com/s2wblog/analysis-of-destructive-malware-whispergate-targeting-ukraine-9d5d158f19f3

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

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

https://www.reliaquest.com/blog/threat-advisory-whispergate-malware-attacks-against-ukrainian-systems/

https://github.com/Neo23x0/signature-base/blob/master/yara/apt_ua_wiper_whispergate.yar

https://www.virustotal.com/gui/file/a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92

https://github.com/CyberSoldiers/IOCs/blob/main/WhisperGate

https://github.com/cado-security/DFIR_Resources_Whispergate/tree/58742dbebb54cf1d34a16d045515f1df6a7c405d

https://securityboulevard.com/2022/01/ttps-used-by-dev-0586-apt-group-in-whispergate-attack-targeting-ukraine/

https://thehackernews.com/2022/01/experts-find-strategic-similarities-bw.html

https://research.nccgroup.com/2020/06/23/wastedlocker-a-new-ransomware-variant-developed-by-the-evil-corp-group

https://www.winhelponline.com/blog/run-program-as-trustedinstaller-locked-registry-keys-files/

https://www.zdnet.com/article/researchers-break-down-whispergate-wiper-malware-used-in-ukraine-website-defacement/

https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wscript