Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 12:55:43 UTC

Tool: WhisperGate

Names	WhisperGate WhisperKill PAYWIPE
Category	Malware
Type	Ransomware, Wiper
Description	(Microsoft) 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.
Information	<https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/> <https://elastic.github.io/security-research/malware/2022/01/01.operation-bleeding-bear/article/> <https://unit42.paloaltonetworks.com/ukraine-cyber-conflict-cve-2021-32648-whispergate/> <https://blog.talosintelligence.com/2022/01/ukraine-campaign-delivers-defacement.html> <https://www.deepinstinct.com/blog/the-ukrainian-government-cyberattack-what-you-need-to-know> <https://therecord.media/ukrainian-government-calls-out-false-flag-operation-in-recent-data-wiping-attack/> <https://www.cybereason.com/blog/cybereason-vs.-whispergate-wiper> <https://therecord.media/a-deeper-look-at-the-malware-being-used-on-ukrainian-targets/>

	<https://cybersecurity.att.com/blogs/labs-research/analysis-on-recent-wiper-attacks-examples-and-how-they-wiper-malware-works>
MITRE ATT&CK	<https://attack.mitre.org/software/S0689/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.whispergate>

Last change to this tool card: 30 December 2022

Download this tool card in JSON format

All groups using tool WhisperGate

Changed	Name	Country	Observed	
APT groups				
	Cadet Blizzard		2020-Jun 2024	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=fb9145d6-3e77-48f0-80ae-a2897eaf49d3