Cybereason vs. WhisperGate and HermeticWiper

By Cybereason Nocturnus

Archived: 2026-04-05 18:31:55 UTC

As geopolitical tensions are escalating between Russia and Ukraine, the cyberwar that has been going on since 2013 recently had another round of escalation. For the last couple of months, there have been a wave of cyberattacks targeting Ukrainian interests involving website defacements and DDOS attacks.

The most recent discovery of sophisticated multi-stage attacks that delivered a highly destructive wipers dubbed WhisperGate and HermeticWiper. Cybereason detects and blocks both of these destructive malware strains. See below for a demo that shows Cybereason blocking the WhisperGate variant.

WhisperGate Wiper

WhisperGate is masquerading as ransomware and has paralyzed numerous Ukrainian organizations. This is not the first time a destructive malware makes its way to Ukrainian organizations by the Russians. A similar attack was conducted in 2017 when thousands of Ukrainian businesses were targeted with the NotPetya ransomware, which was attributed to the elite Russian APT group known as *Sandworm*.

Even though the NotPetya attacks started as attacks targeting only Ukraine, it later "spilled" worldwide, causing massive collateral damage across Europe, Asia and the US. Based on history, it is not an unlikely scenario that the spillage will happen again, where WhisperGate or similar wipers will eventually cause damage in other countries, potentially causing mass disruption.

Cybereason Detects and Blocks the WhisperGate Wiper

WhisperGate is delivered through of a multi-stage infection chain with two main malware components:

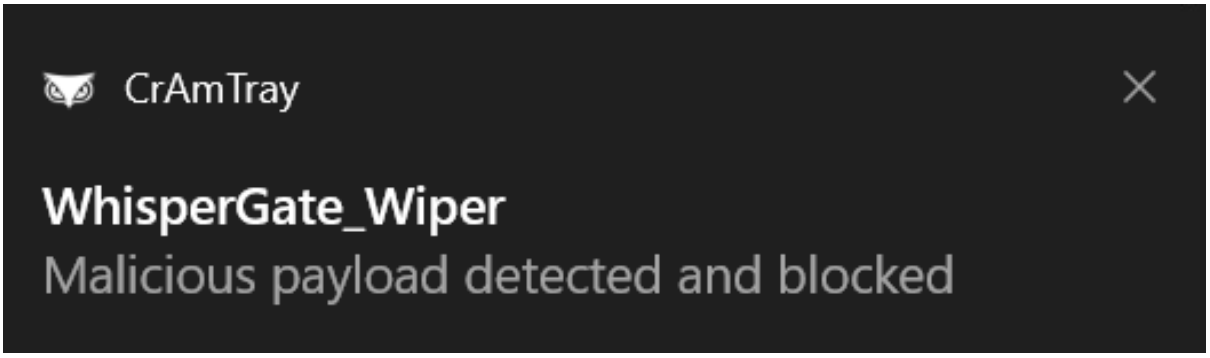
- **Stage 1**: A Master Boot Record (MBR) locker used to overwrite the operating system's MBR, which effectively prevents the operating system from loading successfully
- **Stage 2:** A disk-wiper used to wipe and destroy files on the target machine.

While the wiper was not attributed to a specific Russian APT group, Ukrainian officials publicly attributed the attack to Russia, potentially a step of "preparing the ground" for an upcoming military operation.

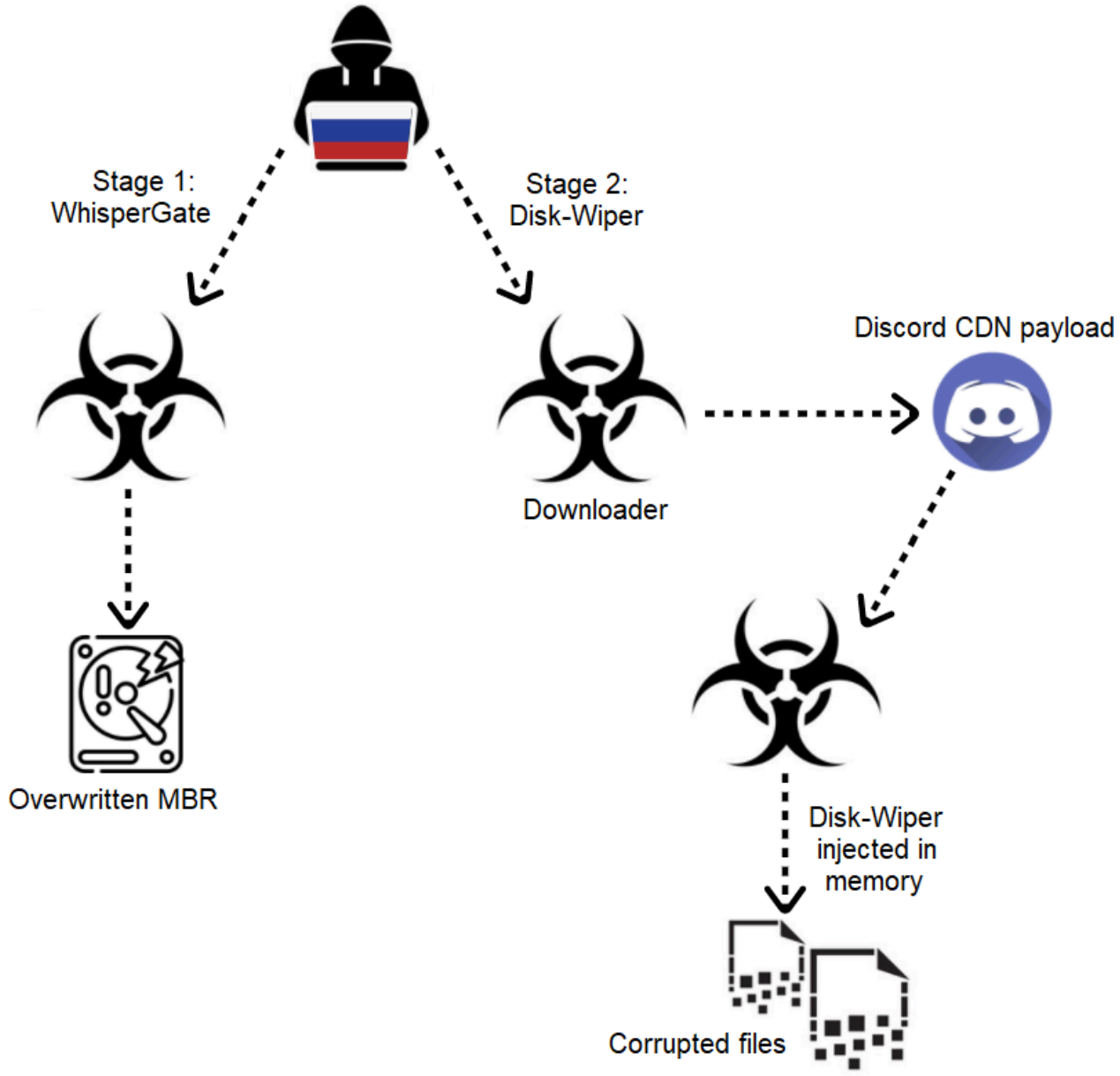
The Cybereason Anti-Ransomware and Anti-MBR corruption technology in the Cybereason XDR Platform detects and prevents the WhisperGate wiper, as well as every other ransomware and wiper strain:

Cybereason protects against WhisperGate

Cybereason detects WhisperGate - UI notification



Cybereason blocks WhisperGate - user notification



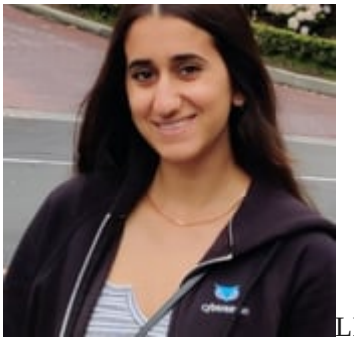
WhisperGate Attack flow graph

Security Recommendations:

- **Enable the Anti-Ransomware Feature on Cybereason NGAV:** Set Cybereason Anti-Ransomware protection mode to *Prevent* with MBR protection set to O*n* - more information for Cybereason customers can be found here
- **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* and above - more information for Cybereason customers can be found here
- **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities
- **Regularly Backup Files to a Remote Server:** Restoring your files from a backup is the fastest way to regain access to your data
- **Use Security Solutions:** Protect your environment using organizational firewalls, proxies, web filtering and mail filtering.

Cybereason is dedicated to teaming with defenders to end attacks on the endpoint, across enterprise, to everywhere the battle is taking place. More resources around emerging threats tied to the Russian aggression in Ukraine can be found here. Learn more about Cybereason AI-driven XDR here or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

About the Researcher:



LIOR ROCHBERGER, SENIOR THREAT RESEARCHER AND THREAT HUNTER, CYBEREASON

As part of the Nocturnus team at Cybereason, Lior has created procedures to lead threat hunting, reverse engineering and malware analysis teams.

Lior has also been a contributing researcher to multiple threat and malware blogs including Bitbucket, Valak, Ramnit, and Racoon stealer. Prior to Cybereason, Lior led SOC operations within the Israeli Air Force.

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world's brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing

new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus
