Cybereason vs. HermeticWiper and IsaacWiper

By Cybereason Security Research Team

Archived: 2026-04-05 18:59:43 UTC

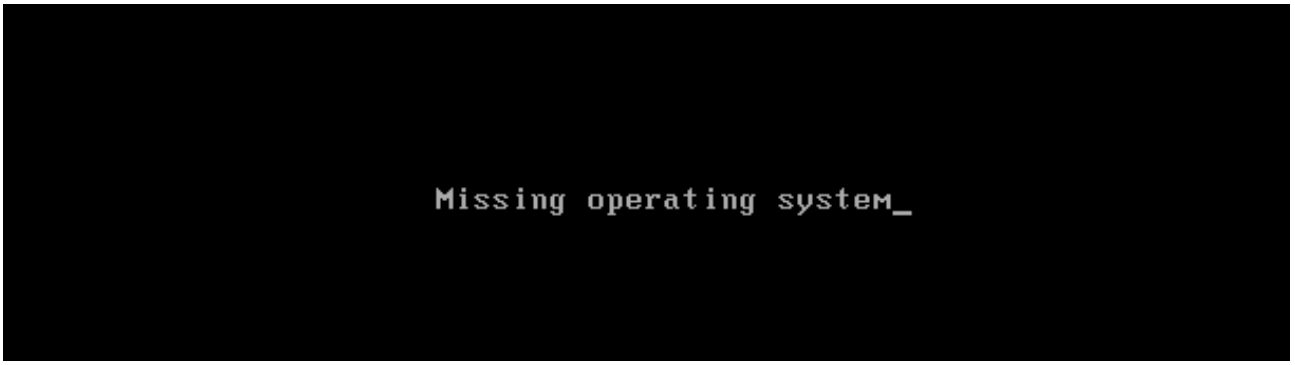
Ukraine has been attacked by several new data wipers as the cyberwar that started in 2013 enters a new round. For the last couple of months, there has been a wave of cyberattacks targeting Ukrainian interests involving website defacements and DDOS attacks.

The most recent discovery involves sophisticated multi-stage attacks that deliver a highly damaging wiper dubbed HermeticWiper. The Anti-Malware capability in the Cybereason XDR Platform detects and blocks the destructive *HermeticWiper* and also detects and blocks a recently discovered variant dubbed IsaacWider. Check out this brief demo that shows Cybereason ending the HermeticWiper threat:

Cybereason detects and blocks HermeticWiper Attacks

HERMETIC WIPER

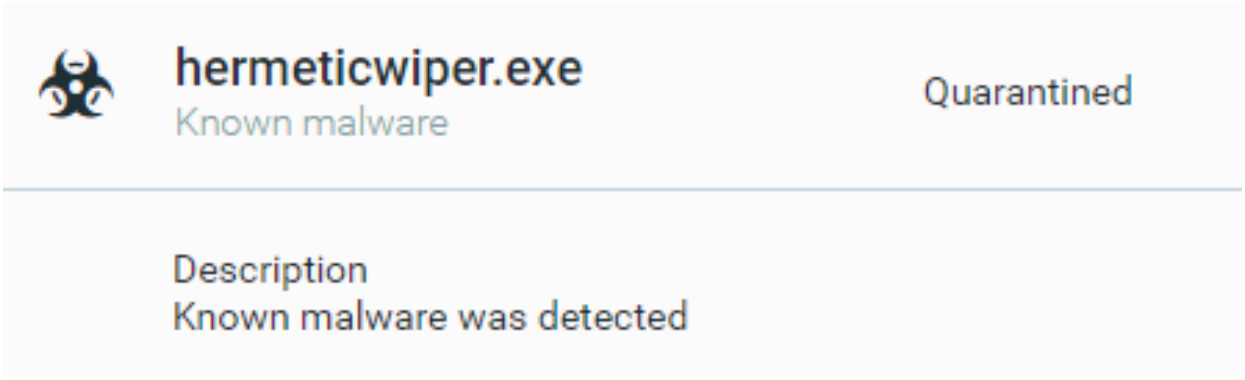
The HermeticWiper malware targets Windows devices, manipulating the master boot record and causing boot failure of the operating system:



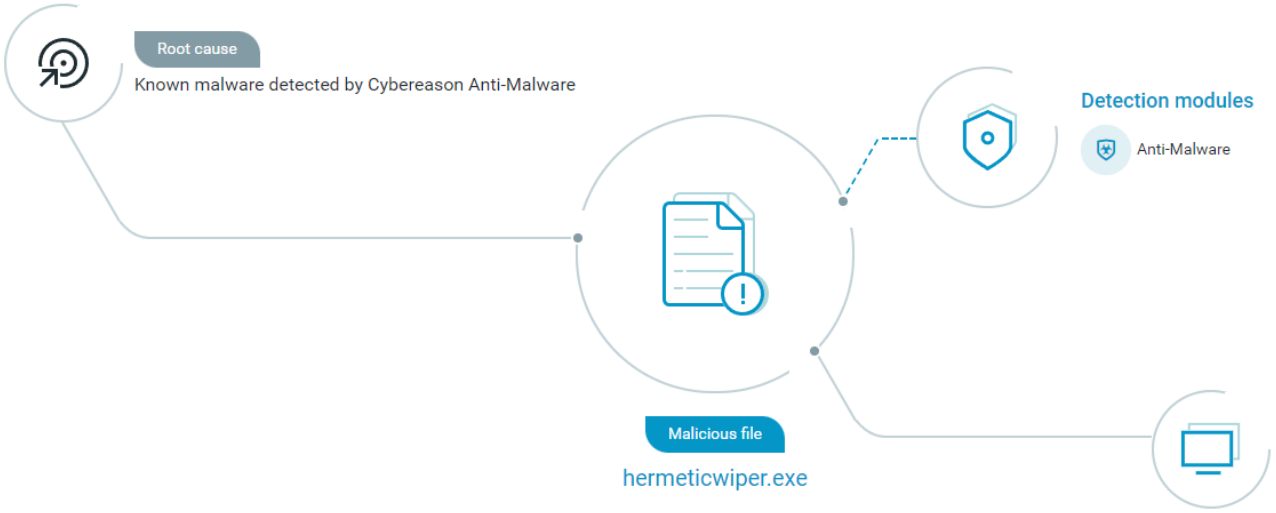
HermeticWiper attack outcome

The HermeticWiper wiper binary is signed by Hermetica Digital Ltd certificate. The wiper malware abuses legitimate driver software from EaseUS Partition Master Software in order to corrupt data.

While the wiper was not attributed to a specific Russian APT group, Ukrainian officials publicly attributed the attack to Russia, saying the attack is potentially an attempt to "prepare the ground" for an upcoming military operation:



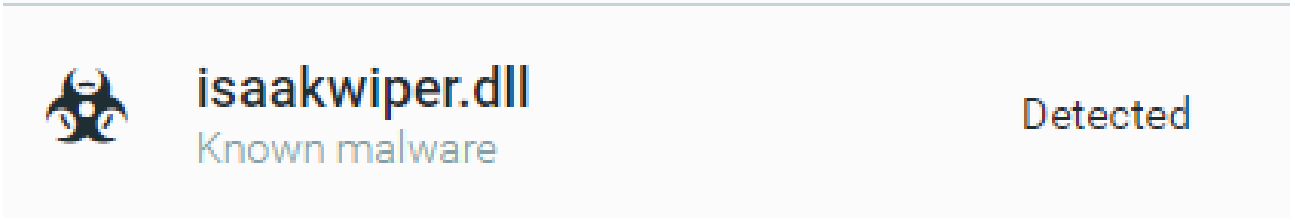
HermeticWiper conviction as seen in the Cybereason XDR Platform



HermeticWiper file path as seen in the Cybereason XDR Platform

HermeticWiper file conviction as seen in the Cybereason XDR Platform

In recent days an additional variant of wiper was discovered called *IsaacWiper*, the Cybereason platform detects and blocks it as well:



The Cybereason XDR Platform detects and blocks IsaacWiper variant

Security Recommendations:

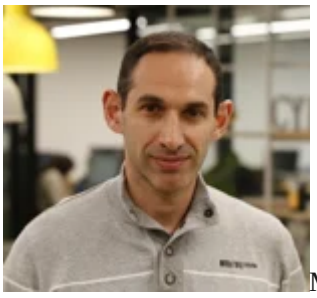
- **Enable Anti-Malware Feature on Cybereason NGAV:** Set Cybereason Anti-Malware mode to *Prevent* and set the detection mode to *Moderate* or above.
- **Keep Systems Fully Patched:** Make sure your systems are patched in order to mitigate vulnerabilities.
- **Regularly Backup Files to a Remote Server:** 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 takes place. More resources around emerging threats tied to the Russian aggression in Ukraine can be found here. Learn more about AI-driven Cybereason XDR here or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

About the Researchers

Alex Elbaum, Security Analyst at Cybereason

Alex Elbaum cyber security analyst at the Cybereason Security Research Team, in the past Alex worked as a threat hunter for a central bank. Alex is responsible for analyzing different types of malware in order to find methods to detect and prevent them.

 Mark Tsipershtein, Security Automation Analyst at Cybereason

Mark Tsipershtein, a cyber security analyst at the Cybereason Security Research Team, focuses on analysis automation and infrastructure. Mark has more than 20 years of experience in SQA, automation, and security testing.

About the Author

Cybereason Security Research Team

The Security Security Research Team creates and manages the core security content of Cybereason, including the detection and preventions logic of its products. The Team is leading the innovation of security defense features to detect and disrupt advanced cyberattacks. The Team is led by top-tier security researchers working with major enterprises, governments, and the military.
