H

HermeticWiper Malware: Behavior, Detection, and Incident Response

HermeticWiper is destructive Windows malware used against Ukrainian organizations in 2022. Learn how it differs from HermeticWizard and HermeticRansom and how to respond safely.

PUBLISHER
Gridinsoft Support

UPDATED
Aug 19, 2026

READ TIME
5 min

CONTENTS

In this guide

HermeticWiper is destructive Windows malware used against organizations in Ukraine on February 23, 2022. Its purpose is to corrupt disk structures and files so affected computers cannot boot or reliably recover data. Microsoft also tracks the family as **FoxBlade**.

HermeticWiper is a historical malware family, not a general name for every disk wiper. A detection should be validated using the exact file hash, path, behavior, and security-vendor report.

01 HermeticWiper, HermeticWizard, and HermeticRansom

Name	Role in the observed campaign	Important distinction
HermeticWiper / FoxBlade	Corrupts disk structures and files, then leaves the system unable to boot.	The destructive payload.
HermeticWizard	Spreads the wiper inside an already compromised network using mechanisms including WMI and SMB.	A propagation component, not the wiper itself.
HermeticRansom / SonicVote	Encrypts files and displays a ransom message.	Observed alongside the wiper and may have served as a distraction; paying would not reverse disk destruction by HermeticWiper.

02 How HermeticWiper damages a system

Research by ESET found that HermeticWiper embedded legitimate, signed drivers from EaseUS Partition Master and selected one for the Windows version it encountered. The malware installed the driver as a service and used its low-level disk operations to corrupt data.

Observed activity included disabling the Volume Shadow Copy Service, corrupting the Master Boot Record and NTFS metadata such as the Master File Table, damaging registry and event-log files, overwriting data in important directories, deleting traces of the wiper itself, and restarting the computer. Once core disk structures and files are destroyed, the device may no longer boot and local recovery can be impossible.

A valid digital signature on an embedded driver did not make the overall program safe. The campaign is an example of a malicious program abusing a legitimate signed component for a harmful purpose.

03 How the 2022 campaign was deployed

Public reporting describes organizations that had been compromised before the destructive payload was launched. HermeticWiper was deployed through enterprise administration paths such as Group Policy in at least one case. HermeticWizard provided a way to spread inside a compromised network. This means defenders should investigate the earlier intrusion and lateral movement, not treat one wiped endpoint as the whole incident.

04 Indicators that deserve immediate escalation

- A specific antivirus or EDR detection for HermeticWiper, FoxBlade, or the associated campaign components.
- Unexpected creation of a service loading a randomly named driver under `C:\Windows\System32\drivers`, especially with related destructive activity.
- Unexplained VSS shutdown, widespread low-level disk writes, or simultaneous corruption across systems.
- Use of Group Policy, WMI, SMB, or remote execution to deploy unfamiliar binaries to many devices.
- Multiple hosts becoming unbootable in a short time, particularly after unusual administrator activity.
- HermeticRansom-style encryption appearing alongside signs of disk destruction.

Names and paths alone are not sufficient. Legitimate partition software can install related signed drivers, while attackers can rename their files. Correlate endpoint, identity, network, and domain-controller evidence.

05 Immediate response

1. **Isolate affected and at-risk network segments.** If destructive activity is active, prioritize stopping propagation over normal shutdown procedures.
2. **Protect identity and management systems.** Restrict compromised administrator accounts, review Group Policy changes, and secure remote-management infrastructure from known-clean systems.
3. **Preserve evidence where practical.** Capture EDR telemetry, process trees, service creation, authentication logs, GPO changes, network flows, and disk images from systems that have not yet been destroyed.
4. **Scope broadly.** Hunt for HermeticWizard, HermeticRansom, remote execution, credential theft, and the access that preceded the wiper deployment.
5. **Activate continuity plans.** Move essential operations to isolated, tested systems. Keep recovery networks separate from the compromised environment.

06 Recovery and data-restoration limits

Do not assume a repair utility can reconstruct a disk after destructive overwrites. For a confirmed infection, rebuild affected devices from trusted installation media and known-good firmware and configuration baselines. Restore data from offline or otherwise protected backups created before the intrusion.

Before reconnecting rebuilt systems, close the original entry path, rotate exposed credentials, validate domain and management infrastructure, and confirm that backup systems were not modified. Restoring too early can expose clean systems to the same compromised accounts or deployment mechanisms.

07 How organizations reduce wiper impact

- Maintain offline, immutable, or logically isolated backups and test full restoration.
- Separate user, server, management, backup, and operational networks.
- Use phishing-resistant MFA for privileged access and dedicated admin workstations.
- Limit who can modify Group Policy, deploy software, or use remote administration across the fleet.
- Monitor service creation, signed-driver abuse, VSS changes, destructive disk access, and unusual lateral movement.
- Keep Windows, endpoint controls, drivers, and internet-facing systems patched.
- Prepare a destructive-malware playbook that includes rapid isolation and business-continuity decisions.

08 Frequently asked questions

Is HermeticWiper ransomware?

No. It is a wiper designed to destroy data and system usability. Separate ransomware called HermeticRansom was observed during the same campaign.

Can paying a ransom recover a HermeticWiper system?

No reliable payment-based recovery exists for damage caused by the wiper. Recovery depends on rebuilding and restoring from protected backups.

Does this malware spread automatically?

The destructive payload and the propagation component should be distinguished. HermeticWizard was observed spreading HermeticWiper within compromised networks, while other deployments used administrative mechanisms.

09 References

- CISA and FBI: Destructive Malware Targeting Organizations in Ukraine
- ESET: HermeticWiper and HermeticWizard technical analysis
- Microsoft: Cyber threat activity in Ukraine