H

HermeticWiper Malware: Behavior and Response

HermeticWiper is destructive Windows malware associated with attacks on Ukrainian organizations in 2022. Its purpose is disruption, not ransom recovery.

PUBLISHER
Gridinsoft Support

UPDATED
Jul 17, 2026

READ TIME
2 min

What it is

HermeticWiper is destructive Windows malware used in attacks against organizations in Ukraine beginning in February 2022. Its purpose is disruption, not financial recovery. The name comes from a digital certificate issued to Hermetica Digital Ltd. that was used to sign a component of the malware.

How it works

The wiper abuses a legitimate partition-management driver to access disk structures and corrupt data needed for the operating system to start. Attackers may deploy it through compromised administrative infrastructure after gaining privileged access. Some incidents also included a decoy ransomware component, but paying would not reverse destructive disk damage.

Key points

- A wiper may resemble ransomware on screen while having no workable decryption path.
- Centralized deployment across many hosts usually indicates earlier compromise of privileged systems.
- Recovery depends on protected backups and clean rebuilding, not simply deleting the executable.

What to do

- Separate affected networks while preserving essential safety and operational communications.
- Protect offline backups and revoke compromised administrative credentials before restoration.
- Rebuild damaged systems from trusted media and validate firmware and boot integrity.
- Investigate the initial intrusion and deployment mechanism across identity and management systems.

Why this historical case still matters

HermeticWiper is the name of a 2022 campaign, so the date identifies the incident rather than the age of the guidance. The durable lesson is to treat destructive activity as an identity and infrastructure compromise. Maintain offline, tested backups; limit administrative deployment rights; monitor mass remote execution; and prepare a clean rebuild process. See ransomware for the difference between recoverable encryption and destructive behavior, and malware for general containment steps.