

HermeticWiper Malware

Destructive malware targeting organizations in Ukraine

Malware known as Hermetic (or, FoxBlade) was found by cybersecurity researchers being used against organizations in Ukraine.

Background

Announced

Malware actors have deployed destructive malware targetting organizations in Ukraine during the advent of the unprovoked Russian attack against Ukraine. The malware when executed on a Windows PC can wipe the partitions ending up destroying all data and the operating system.

Latest Developments

FortiGuard has Anti-VIrus detection coverage on the malware as W32/KillDisk.NCV!tr. The ANN and behavioural detects the malware as trojan downloader and high risk, respectively.



PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

February 26, CISA announced a destructive malware targetting Ukraine known as HermeticWiper..

Reconnaissance

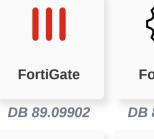
Weaponization

Delivery

AV











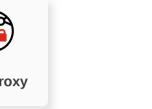


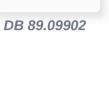


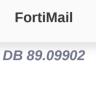






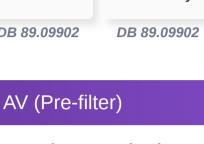


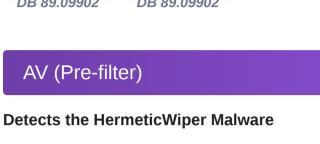












FortiNDR

DB 89.09902

FortiSandbox FortiEDR DB 89.09902 DB 89.09902

Behavior Detection

Detects any variants of HermeticWiper Malware as High Risk



Detects the malware as a Wiper

ANN



Exploitation



C2





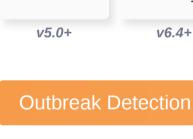
Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

v6.4+

DETECT

Threat Hunting





FortiAnalyzer DB 1.00051



Automated Response

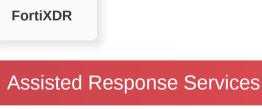
RESPOND

Services that can automaticlly respond to this outbreak.

Develop containment techniques to mitigate impacts of security events:

FortiSIEM

v6.0+



Response

(and recovery from) security incidents:

Experts to assist you with analysis, containment and response activities.



InfoSec Services

Response Readiness

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Improve security posture and processes by implementing security awareness and training, in preparation for





Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

Security Rating



Additional Resources

FortiGuard Threat Signal https://www.fortiguard.com/threat-signal-report/4425

Learn more about FortiGuard Outbreak Alerts