FORTINET

OUTBREAK ALERTS

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 — 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.

Announced — 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.

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

PROTECT

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

- Reconnaissance
- Weaponization
- Delivery

AV

Detects the HermeticWiper Malware

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 89.09902	*DB 89.09902*	*DB 89.09902*	*DB 89.09902*	*DB 89.09902*	*DB 89.09902*	*DB 89.09902*

FortiADC	FortiProxy
DB 89.09902	*DB 89.09902*

AV (Pre-filter)

Detects the HermeticWiper Malware

FortiEDR	FortiSandbox	FortiNDR
DB 89.09902	*DB 89.09902*	*DB 89.09902*

Behavior Detection

Detects any variants of HermeticWiper Malware as High Risk

FortiSandbox
v3.2+

ANN

Detects the malware as a Wiper

FortiNDR
DB 1.094

- Exploitation
- Installation
- C2
- Action

DETECT

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

Threat Hunting

FortiEDR	FortiAnalyzer	FortiSIEM
v5.0+	*v6.4+*	*v6.0+*

Outbreak Detection

FortiAnalyzer
DB 1.00051

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

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

Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

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

Response Readiness

IDENTIFY

Identify processes and assets that need protection:

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