A destructive malware known as HermeticWiper (or, FoxBlade) was found by cybersecurity researchers. The malware is being used against organizations in Ukraine. The malware when executed on a Windows PC can wipe the partitions ending up destroying all data and the operating system.

- **Behavioral**: Detects the malware as trojan downloader and high risk, respectively.
- **FortiGuard**: Has Anti-Virus detection coverage on the malware as W32/KillDisk.NCV!tr. The ANN and Behavior Detection modules classify the malware as Behavior-HermeticWiper/ta-p/205842.
- **Outbreak Detection**: Detects any variants 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.
- **Pre-Execution**: Alert on the malware as a threat.

**Fortinet Products**

- **FortiSIEM**: Incident Response (Security Operations) and Cyber Kill Chain
- **FortiAnalyzer**: Incident Response (Security Operations) and Cyber Kill Chain
- **FortiADC**: Threat Hunting
- **FortiCWP**: Threat Hunting
- **FortiCASB**: Threat Hunting
- **FortiMail**: Threat Hunting
- **FortiAI**: Threat Hunting
- **FortiSandbox**: Threat Hunting
- **FortiSASE**: Threat Hunting
- **FortiClient**: Threat Hunting
- **FortiWeb**: Threat Hunting
- **FortiGate**: Threat Hunting
- **FortiEDR**: Threat Hunting
- **FortiClient**: Threat Hunting

**Summary**

Fortinet Products are being used against organizations in Ukraine. The malware is classified as high risk and can be detected by various Fortinet products such as FortiSIEM, FortiAnalyzer, FortiADC, FortiCWP, FortiCASB, FortiMail, FortiAI, FortiSandbox, FortiSASE, FortiClient, and FortiWeb. FortiGate also provides protection against the HermeticWiper malware. Fortinet provides updates on the malware, such as FortiSOAR updates to raise alerts and escalate to incident response.