New destructive wiper malware deployed in Ukraine

cybernews.com/cyber-war/new-destructive-wiper-malware-deployed-in-ukraine/

March 14, 2022

Cybersecurity company ESET warned about the discovery of a 3rd destructive wiper malware deployed in Ukraine.

ESET first observed this new malware dubbed CaddyWiper on Monday, around 9h38 UTC.

CaddyWiper erases user data and partition information from attached drives. The malware was seen on a few dozen systems in a limited number of organizations.

"CaddyWiper does not share any significant code similarity with #HermeticWiper, #IsaacWiper, or any other malware known to us," ESET said in a tweet.

> twitter

ESET said the attackers had prior control of the target's network beforehand.

"Interestingly, CaddyWiper avoids destroying data on domain controllers. This is probably a way for the attackers to keep their access inside the organization while still disturbing operations," the company said.

Disk-wiping malware

Security researchers at Symantec and ESET first observed the wiper malware in February. According to a blog post by Symantec, attackers deployed a disk-wiping malware (Trojan.Killdisk) shortly before Russian forces crossed the Ukrainian border.

The wiper contains driver files that eventually damage the Master Boot Record (MBR) of the infected computer, rendering it inoperable.

According to Crowdstrike, the attackers misused legitimate EaseUS Partition Master drivers to gain raw disk access and manipulate the disk to make the system inoperable.

The wiper was dubbed HermeticWiper since the malware's certificate was issued to Hermetica Digital Ltd., a legitimate Cyprus-based company. Other researchers named the novel malware 'DriveSlayer.'

CISA released an advisory on the malware that targeted organizations in Ukraine, with recommendations and strategies to prepare for and respond to the threat.

More from Cybernews:

Open database leaves major Chinese ports exposed to shipping chaos

The Iron Curtain: which IT-related services got blocked or left the Russian market?

Underworld trends: criminals adopt DDoS attacks for extortion - report

89% of global cyberattacks are aimed at Russia or Ukraine

Subscribe to our newsletter
