HermeticWiper: New data-wiping malware hits Ukraine

welivesecurity.com/2022/02/24/hermeticwiper-new-data-wiping-malware-hits-ukraine/

February 24, 2022

Hundreds of computers in Ukraine compromised just hours after a wave of DDoS attacks brings down a number of Ukrainian websites

Editor
24 Feb 2022 - 10:32AM

Hundreds of computers in Ukraine compromised just hours after a wave of DDoS attacks brings down a number of Ukrainian websites

A number of organizations in Ukraine have been hit by a cyberattack that involved new data-wiping malware dubbed HermeticWiper and impacted hundreds of computers on their networks, ESET Research has found. The attack came just hours after a series of distributed denial-of-service (DDoS) onslaughts knocked several important websites in the country offline.

> Breaking. #ESETResearch discovered a new data wiper malware used in Ukraine today. ESET telemetry shows that it was installed on hundreds of machines in the country. This follows the DDoS attacks against several Ukrainian websites earlier today 1/n
>
> — ESET research (@ESETresearch) February 23, 2022

Detected by ESET products as Win32/KillDisk.NCV, the data wiper was first spotted just before 5 p.m. local time (3 p.m. UTC) on Wednesday. The wiper's timestamp, meanwhile, shows that it was compiled on December 28th, 2021, suggesting that the attack may have been in the works for some time.

HermeticWiper misused legitimate drivers of popular disk management software. "The wiper abuses legitimate drivers from the EaseUS Partition Master software in order to corrupt data," according to ESET researchers.

Additionally, the attackers used a genuine code-signing certificate issued to a Cyprus-based company called Hermetica Digital Ltd., hence the wiper's name.

It also appears that at least in one case, the threat actors had access to a victim's network before unleashing the malware.

READ ALSO: IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine
Earlier on Wednesday, a number of Ukrainian websites were knocked offline in a fresh wave of DDoS attacks that have been targeting the country for weeks now.

In the middle of January, another data wiper swept through Ukraine. Called WhisperGate, the wiper masqueraded as ransomware and brought some echoes of the NotPetya attack that hit Ukraine in June 2017 before causing havoc around the world.

For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.
ESET Research now also offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page

24 Feb 2022 - 10:32AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion