Second data wiper attack hits Ukraine computer networks

therecord.media/second-data-wiper-attack-hits-ukraine-computer-networks/

February 23, 2022

Image: The Record

Two cybersecurity firms with a strong business presence in Ukraine—ESET and Broadcom's Symantec—have reported tonight that computer networks in the country have been hit with a new data-wiping attack.

The attack is taking place as Russian military troops have crossed the border and invaded Ukraine's territory in what Russian President Putin has described as a "peacekeeping" mission.

Details about the attack are still being collected, and the attack is still going on. It's scale and the number of impacted systems is still unknown.

> New #wiper malware being used in attacks on #Ukraine
> 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
>
> — Threat Intelligence (@threatintel) February 23, 2022

> 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

Today's event marks the second time this year that a data wiper was deployed on Ukrainian computer systems after a first attack took place in mid-January.

The deployment of that first malware (named **WhisperGate**) was hidden under the guise of a fake ransomware outbreak and during a series of coordinated defacements of Ukrainian government websites.

Similarly, today's data-wiping attacks were also accompanied by a series of distributed denial of service (DDoS) attacks against government websites, in a similar attempt to distract government IT workers and the public's attention.

"Targets have included finance and government contractors," Vikram Thakur, Technical Director at Symantec Threat Intelligence, a division of Broadcom Software, told *The Record* in an email. Infections were reported from Ukraine, but some systems were also hit across Latvia and Lithuania.

Malware corrupts data, rewrites the MBR

At the time of writing, Ukrainian government officials have not confirmed or released any details about the ongoing attack.

However, according to a technical analysis of the malware, which ESET said it was tracking as **HermeticWiper**, the wiper is sometimes deployed via Windows group policies, suggesting the attackers may have full control of some of their target's internal networks.

Once deployed, the wiper runs a version of the EaseUS Partition Master software, a disk partitioning utility, which it uses to corrupt local data and then reboot the computer.

According to Silas Cutler, a security researcher for Stairwell, HermeticWiper doesn't just destroy local data, but it also damages the master boot record (MBR) section of a hard drive, which prevents the computer from booting into the operating system after the forced reboot —behavior identical with the WhisperGate wiper attack from last month.

> I can confirm this damages a systems MBR. https://t.co/68B0V743lR
>
> — Silas (@silascutler) February 23, 2022

ESET said today's attack was first seen around 16:52, Ukraine time. According to security researcher MalwareHunterTeam, the malware appears to have been compiled just five hours before it was deployed in the wild, suggesting its code and operational infrastructure was most likely set up and ready to go well in advance.

Article updated at 4am ET with new name for the malware and to add that Russia has formally declared war on Ukraine hours after this piece of malware was deployed, confirming theories that HermeticWiper's primary role was to cripple local IT systems and prevent the Ukrainian government from reacting with its full capabilities. Almost 18 hours after it was deployed, it remains unclear if the malware succeeded.

Tags

- APT
- data wiper
- HermeticWiper
- malware
- MBR
- nation-state
- Russia
- Ukraine
- WhisperGate

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.