Destructive Data Wiper Malware Targeting high-profile Ukrainian Organizations

cybersecuritynews.com/destructive-data-wiper-malware/

Guru

March 16, 2022

A destructive data wiper was discovered recently by the ESET researchers that were used in attacks against Ukrainian organizations. It is the third strain of wiper malware that was discovered since the Russian invasion started to affect computers in Ukraine.

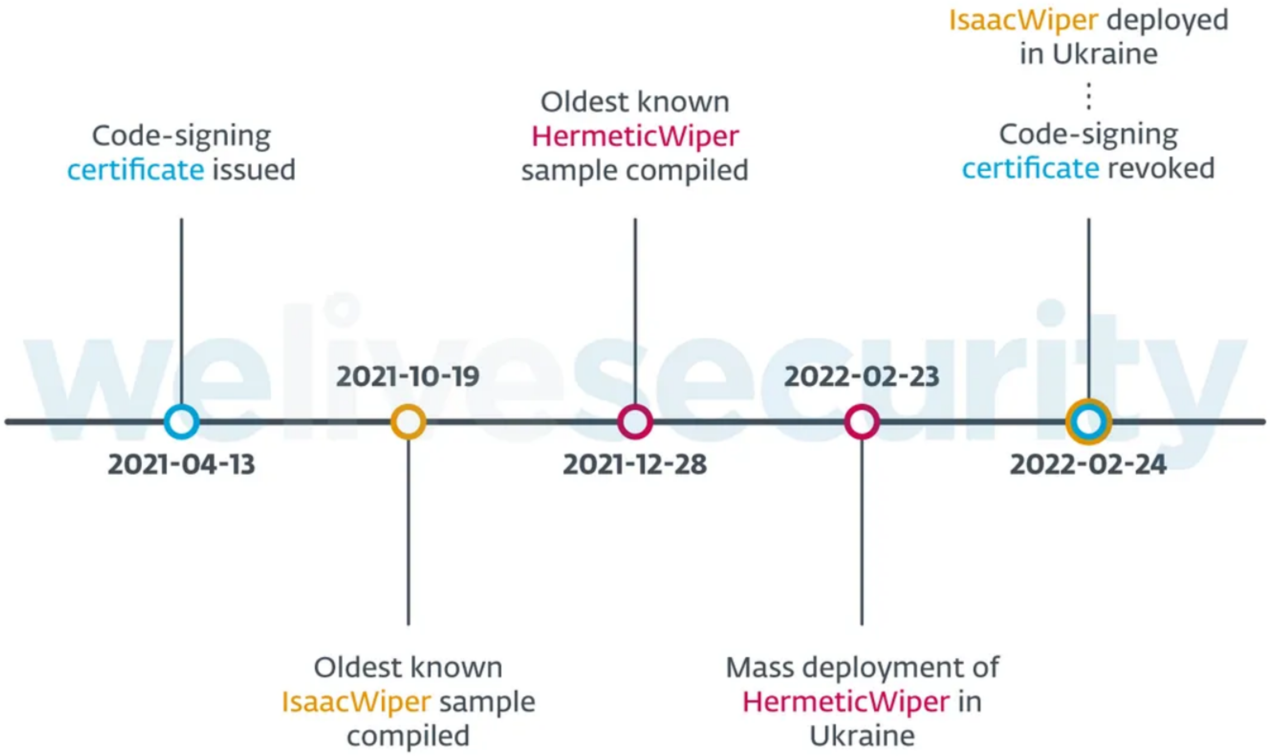
ESET researchers named this malware, CaddyWiper, and as soon as a compromised system is infected by this malware, it erases all the data and partition information.

ESET products detect this malware as *Win32/KillDisk[.]NCX* and there have been multiple reports of the wiper being installed on systems in a limited number of organizations.

While apart from this, neither HermeticWiper nor IsaacWiper (Two other strains of wiper malware targeting computers in Ukraine) shares any close code similarities with CaddyWiper. The CaddyWiper malware may have been launched after the threat actors hacked into the target network.

> #BREAKING #ESETresearch warns about the discovery of a 3rd destructive wiper deployed in Ukraine 🇺🇦. We first observed this new malware we call #CaddyWiper today around 9h38 UTC. 1/7 pic.twitter.com/gVzzIT6AzN
>
> — ESET research (@ESETresearch) March 14, 2022

However, till now it has been detected that only one organization has been targeted by the CaddyWiper, in short, the number of cases in the wild is small.


IsaacWiper deployed in Ukraine
Code-signing certificate revoked
Code-signing certificate issued
Oldest known HermeticWiper sample compiled
2021-10-19
2022-02-23
2021-04-13
2021-12-28
2022-02-24
Oldest known IsaacWiper sample compiled
Mass deployment of HermeticWiper in Ukraine
welivesecurity

In the days before Russia invaded Ukraine, ESET's telemetry discovered HermeticWiper on the networks of several high-profile organizations in Ukraine.

Furthermore, HermeticWiper was propagated inside local networks with HermeticWizard, as well as HermeticRansom, which served as decoy ransomware.

Here the malware is primarily designed with the sole intention of attacking the target rather than extracting any financial data, information, and reward from the victim.

In January of this year, a similar data wiper called WhisperGate struck multiple organizations in Ukraine. In the last eight years, high-profile targets in the country have been targeted in a series of malicious campaigns like this.

In this ongoing cyberwarfare, some of the hackers supporting Ukraine have used malware against pro-Russian cybercriminals, who use malware to degrade and destroy data on Ukrainian computer systems.

While on the other hand, other hackers have targeted Russian companies and government agencies to leak their confidential information. The Russia-Ukraine conflict has so far not resulted in a large-scale cyberattack, but larger attacks could still occur.