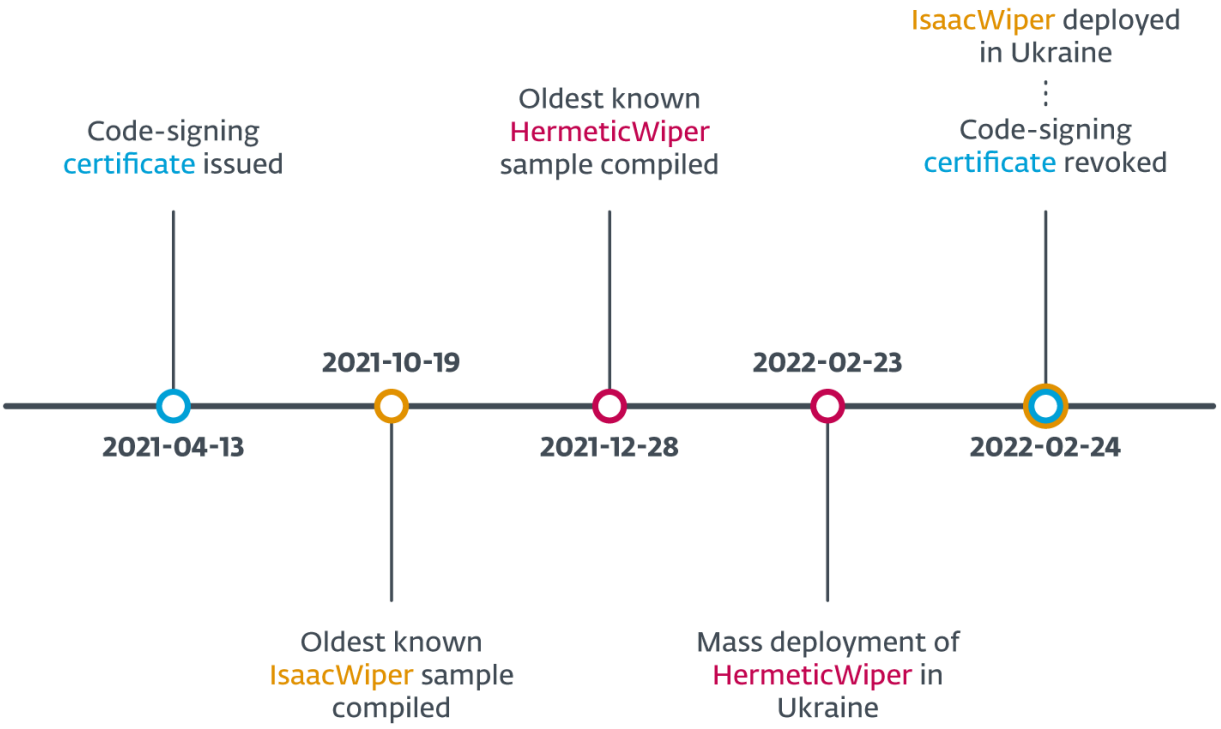
CaddyWiper, a new data wiper hits Ukraine

By Pierluigi Paganini

Published: 2022-03-15 · Archived: 2026-04-06 00:10:49 UTC



Experts discovered a new wiper, tracked as CaddyWiper, that was employed in attacks targeting Ukrainian organizations.

Experts at ESET Research Labs discovered a new data wiper, dubbed CaddyWiper, that was employed in attacks targeting Ukrainian organizations.

The security firm has announced the discovery of the malware with a series of tweets:

“This new malware erases user data and partition information from attached drives,” ESET Research Labs reported. “ESET telemetry shows that it was seen on a few dozen systems in a limited number of organizations.”

CaddyWiper is the third wiper observed by ESET in attacks against Ukraine after HermeticWiper and IsaacWiper, experts pointed out that it does not share any significant code similarity with them.

Similar to HermeticWiper deployments, CaddyWiper being deployed via GPO, a circumstance that suggests the attackers had initially compromised the target’s Active Directory server.

In order to maintain access to the target organization while still disturbing operations, the CaddyWiper avoids destroying data on domain controllers. CaddyWiper uses the DsRoleGetPrimaryDomainInformation() function to determine if a device is a domain controller.

The CaddyWiper sample analyzed by ESET was not digitally signed, the malware was compiled.

Microsoft researchers also observed another wiper that was employed in attacks against Ukraine, it was tracked as WhisperGate.

In Mid-February, the Security Service of Ukraine (SSU) today revealed the country was the target of an ongoing "wave of hybrid warfare" conducted by Russia-linked malicious actors. Threat actors aim at destabilizing the social contest in the country and instilling fear and untrust in the country's government. Data wiper usage was part of this hybrid warfare strategy.

Follow me on Twitter: **@securityaffairs** and **Facebook**

[adrotate banner="9″]	[adrotate banner="12″]

Pierluigi Paganini

(SecurityAffairs – hacking, CaddyWiper)

[adrotate banner="5″]

[adrotate banner="13″]
