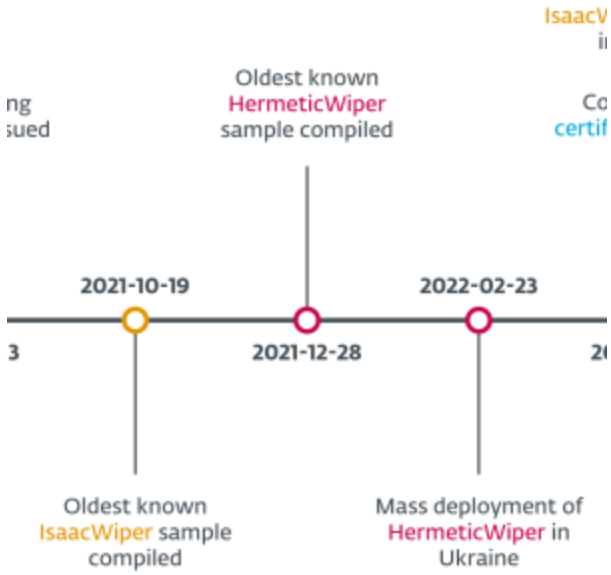
CaddyWiper, a new data wiper hits Ukraine

securityaffairs.co/wordpress/129069/cyber-warfare-2/caddywiper-wiper-hits-ukraine.html

March 15, 2022



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:

> #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

> CaddyWiper does not share any significant code similarity with #HermeticWiper, #IsaacWiper or any other malware known to us. The sample we analyzed was not digitally signed. 3/7https://t.co/EGp9NnctD9
>
> — ESET research (@ESETresearch) March 14, 2022

"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.

> Information from the PE header of CaddyWiper suggests it was compiled the same day it was deployed to targeted networks. 6/7 pic.twitter.com/Ay363IRGzX
>
> — ESET research (@ESETresearch) March 14, 2022

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.

Pierluigi Paganini

(SecurityAffairs – hacking, CaddyWiper)

You might also like

Experts believe that Russian Gamaredon APT could fuel a new round of DDoS attacks

May 28, 2022 By Pierluigi Paganini

There you can buy or download for free private and compromising data of your competitors. We public schemes, drawings, technologies, political and military secrets, accounting reports and clients databases. All this things were gathered from the largest worldwide companies, conglomerates and concerns with every activity. We gather data using vunlerability in their IT infrastructure. in their IT infrastructure.

Industrial spy team processes huge massives every day to devide you results. You can fid it in their portal:

http://[redacted]

(Tor browser required)

We can save your time gaining your own goals or goals of your company.With our information you could refuse partnership with unscrupulous partner, reveal dirty secrets of your competitors and enemies and earn millions dollars using insider information.

"He who owns the information, owns the world"

Nathan Mayer Rothschild

The strange link between Industrial Spy and the Cuba ransomware operation

May 28, 2022 By Pierluigi Paganini

Back to top

- Home
- Cyber Crime

- Cyber warfare
- APT
- Data Breach
- Deep Web
- Digital ID
- Hacking
- Hacktivism
- Intelligence
- Internet of Things
- Laws and regulations
- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism
- ICS-SCADA
- EXTENDED COOKIE POLICY
- Contact me