

New CaddyWiper data wiping malware hits Ukrainian networks

By Sergiu Gatlan

Published: 2022-03-14 · Archived: 2026-04-05 13:58:41 UTC



Newly discovered data-destroying malware was observed earlier today in attacks targeting Ukrainian organizations and deleting data across systems on compromised networks.

"This new malware erases user data and partition information from attached drives," ESET Research Labs [explained](#).

"ESET telemetry shows that it was seen on a few dozen systems in a limited number of organizations."



Visit Advertiser website [GO TO PAGE](#)

While designed to wipe data across Windows domains it's deployed on, CaddyWiper will use the `DsRoleGetPrimaryDomainInformation()` function to check if a device is a domain controller. If so, the data on the domain controller will not be deleted.

This is likely a tactic used by the attackers to maintain access inside the compromised networks of organizations they hit while still heavily disturbing operations by wiping other critical devices.

While analyzing the PE header of a malware sample discovered on the network of an undisclosed Ukrainian organization, it was also discovered that the malware was deployed in attacks the same day it was compiled.

"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," ESET added.

"Similarly to HermeticWiper deployments, we observed CaddyWiper being deployed via GPO, indicating the attackers had prior control of the target's network beforehand."

```
[ IMAGE_FILE_HEADER ]
0xCC      0x0      Machine:                0x14C
0xCE      0x2      NumberOfSections:      0x3
0xD0      0x4      TimeDateStamp:         0x622EEC88 [Mon Mar 14 07:19:36 2022 UTC]
0xD4      0x8      PointerToSymbolTable:  0x0
0xD8      0xC      NumberOfSymbols:       0x0
0xDC      0x10     SizeOfOptionalHeader:  0xE0
0xDE      0x12     Characteristics:        0x102
Flags: IMAGE_FILE_32BIT_MACHINE, IMAGE_FILE_EXECUTABLE_IMAGE
```

CaddyWiper compilation date ([ESET](#))

Fourth data wiper deployed in Ukraine this year

CaddyWiper is the fourth data wiper malware deployed in attacks in Ukraine since the start of 2022, with ESET Research Labs analysts previously discovering two others and Microsoft a third.

One day before the Russian invasion of Ukraine started, on February 23rd, ESET researchers spotted a data-wiping malware [now known as HermeticWiper](#), used to target Ukraine together with [ransomware decoys](#).

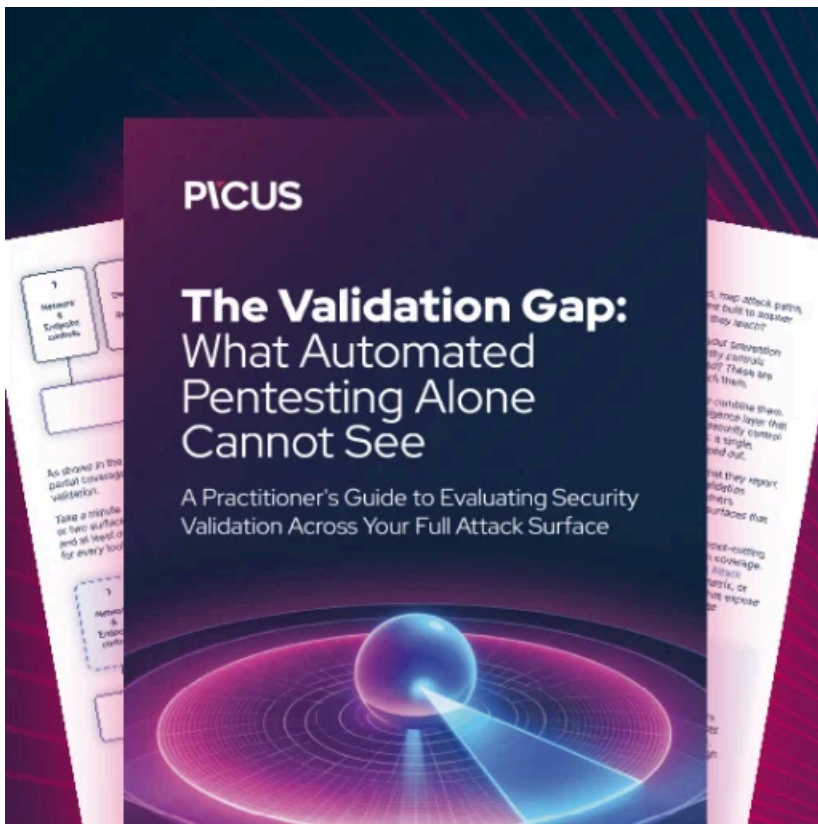
They also discovered a [data wiper they dubbed IsaacWiper](#) and a new worm named HermeticWizard the attackers used to drop HermeticWiper wiper payloads, deployed the day Russia invaded Ukraine.

Microsoft also [found a wiper now tracked as WhisperGate](#), used in data-wiping attacks against Ukraine in mid-January, disguised as ransomware.

As Microsoft President and Vice-Chair Brad Smith said, these ongoing attacks with destructive malware against Ukrainian organizations "have been precisely targeted."

This contrasts with the indiscriminate NotPetya worldwide malware assault that hit Ukraine and other countries in 2017, an attack later [linked to Sandworm](#), a Russian GRU Main Intelligence Directorate hacking group.

Such destructive attacks are part of a "[massive wave of hybrid warfare](#)," as the Ukrainian Security Service (SSU) described them right before the war started.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/new-caddywiper-data-wiping-malware-hits-ukrainian-networks/>