# CaddyWiper: New wiper malware discovered in Ukraine

welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

March 14, 2022

This is the third time in as many weeks that ESET researchers have spotted previously unknown data wiping malware taking aim at Ukrainian organizations

Editor
15 Mar 2022 - 12:00AM

This is the third time in as many weeks that ESET researchers have spotted previously unknown data wiping malware taking aim at Ukrainian organizations

ESET researchers have uncovered yet another destructive data wiper that was used in attacks against organizations in Ukraine.

Dubbed CaddyWiper by ESET analysts, the malware was first detected at 11.38 a.m. local time (9.38 a.m. UTC) on Monday. The wiper, which destroys user data and partition information from attached drives, was spotted on several dozen systems in a limited number of organizations. It is detected by ESET products as Win32/KillDisk.NCX.

*RELATED READING: Industroyer2: Industroyer reloaded*
CaddyWiper bears no major code similarities to either HermeticWiper or IsaacWiper, the other two new data wipers that have struck organizations in Ukraine since February 23rd.

Much like with HermeticWiper, however, there's evidence to suggest that the bad actors behind CaddyWiper infiltrated the target's network before unleashing the wiper.

> #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

## A wiper a week

This is the third time in as many weeks that ESET researchers have spotted a previously unknown strain of data-wiping malware in Ukraine.

On the eve of Russia's invasion of Ukraine, ESET's telemetry picked up HermeticWiper on the networks of a number of high-profile Ukrainian organizations. The campaigns also leveraged HermeticWizard, a custom worm used for propagating HermeticWiper inside local networks, and HermeticRansom, which acted as decoy ransomware.

The next day, a second destructive attack against a Ukrainian governmental network started, this time deploying IsaacWiper.

## Ukraine in the crosshairs

In January of this year, another data wiper, called WhisperGate, swept through the networks of multiple organizations in Ukraine.

All these campaigns are only the latest in a long string of attacks to have hit high-profile targets in the country over the past eight years. As explored by ESET researchers in a recent webinar and podcast, Ukraine has been on the receiving end of a number of highly disruptive cyberattacks since 2014, including the NotPetya attack that tore through the networks of a number of Ukrainian businesses in June 2017 before spreading beyond the country's borders.

*For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
*ESET Research now also offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page*

15 Mar 2022 - 12:00AM

***Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center***

## Newsletter

## Discussion