A deeper look at the malware being used on Ukrainian targets

By Daryna Antoniuk

Published: 2023-01-12 · Archived: 2026-04-05 17:59:39 UTC

Over the last two months, the number of cyberattacks against Ukrainian government agencies, security and defense services, and commercial organizations has soared.

Before the war, Russia-linked hackers mostly attacked Ukraine to sow fear or panic and undermine trust in the government. But security experts warn that recent 'wiper' attacks could leave millions of Ukrainians without electricity and prevent them from receiving social assistance through government services or making payments with online banks.

Since February 24, Ukrainian security officials have identified at least eight new types of malware used by hackers to attack Ukraine: AcidRain, WhisperGate, WhisperKill, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero and Industroyer2.

Researchers have not yet identified all threat actors responsible for developing these variants of malware, but many attacks have been carried out by Kremlin-backed hacker groups, such as Sandworm, which are also attacking Europe and the U.S.

Knowing what these new types of malware can do and who is behind them help Ukrainian enterprises and state services detect vulnerabilities early, Ukrainian security official Victor Zhora told The Record.

According to him, the same hackers who are attacking Ukraine's information infrastructure are also attacking organizations in the EU that are helping Ukrainian refugees. "This means that hackers are not limited to attacks on Ukraine, but also to European cyberspace," Zhora said.

Here are some important things to know about the malware.

WhisperGate & WhisperKill

Attribution: Blamed on hackers tied to the Russian government.

Details of the attack: On the night of January 13 and into the following morning, unidentified hackers attempted to gain access to and deface the websites of more than 70 Ukrainian government agencies, according to Ukraine's security service. The attack successfully defaced 22 websites and severely damaged six.

The attackers used vulnerabilities in the October CMS website builder and employee accounts of a local IT firm named KitSoft to access servers hosting the sites and carry out the defacements.

Description: WhisperGate has some similarities to the NotPetya wiper that attacked Ukrainian businesses in 2017, according to CiscoTalos: it is designed to look like ransomware but lacks a ransom recovery mechanism.

It destroys the master boot record (MBR) instead of encrypting it. The malware's goal is to render targeted devices inoperable rather than to obtain a ransom, according to Microsoft.

How it works: WhisperGate downloads a payload that wipes the MBR, then downloads a malicious file hosted on a Discord server, which drops and executes another wiper payload that destroys files on the infected machines.

WhisperKill component, downloaded by WhisperGate, destroys files with specific extensions.

The attackers used stolen credentials to compromise their victims and they likely had access to the victim's network for months before the attack, according to Cisco

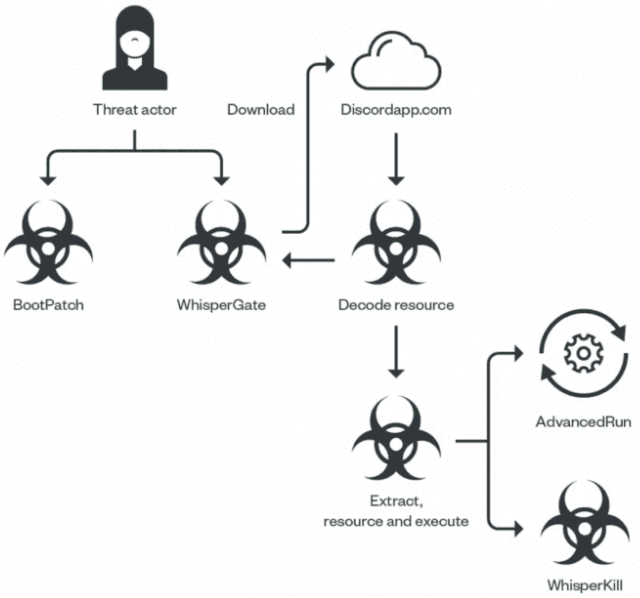

Image: TrendMicro

HermeticWiper

Attribution: A methodology and timing of the attack suggest the involvement of Russian government-associated hackers, according to Recorded Future.

Details of the attack: Several hours before the invasion, Ukrainian government agencies and banks were hit with distributed denial-of-service, or DDoS, attacks that took some websites offline. After these attacks, a data wiper malware called HermeticWiper was installed on hundreds of machines.

The attack might have been in preparation for almost two months, according to ESET. It had an impact outside Ukraine – in Latvia and Lithuania, according to cybersecurity firm Symantec.

Description: This malware was named "HermeticWiper" based on a digital certificate from a company called Hermetica Digital Ltd. It's possible that the attackers used a shell company to issue a certificate that allows bypassing detection capabilities, such as Microsoft Defender SmartScreen and built-in browser protections.

This wiper is remarkable for its ability to bypass Windows security features and gain access to many low-level data structures on the disk, according to Malwarebytes.

> Breaking. #ESETResearch discovered a new data wiper malware used in Ukraine today. ESET telemetry shows that it was installed on hundreds of machines in the country. This follows the DDoS attacks against several Ukrainian websites earlier today 1/n— ESET Research (@ESETresearch) February 23, 2022

How it works: The malware targets Windows devices, manipulating the master boot record, which results in subsequent boot failure, according to SentinelLabs.

A 32-bit Windows executable with an icon resembling a gift has to be run as administrator in order to work. As a result of the malware execution, the data on the disk gets more fragmented.

As the execution progresses, some applications stop working because the malware overwrites some files with random data. After reboot Windows OS will no longer work.

IsaacWiper

Attribution: Not yet determined

Details of the attack: IsaacWiper, hit at least one Ukrainian government organization on the day of Russia's invasion.

Its timestamp, October 19, 2021, suggests it was prepared months before the beginning of the full-scale war. IsaacWiper might have been used in previous operations, but not detected, ESET said.

On February 25, hackers dropped a new version of IsaacWiper with debug logs. It may indicate that earlier attacks weren't successful. Debug strings would allow IsaacWiper's developers to understand what was happening on infected hosts.

Description: IsaacWiper is a destructive malware that overwrites all physical disks and logical volumes on a computer, according to Recorded Future.

The attackers' goal is to destroy data on the victim's systems and make their computers unbootable, forcing victims to reinstall the OS.

There is no code overlap between IsaacWiper, HermeticWiper, or WhisperGate. IsaacWiper achieves a similar outcome by different means and is far less advanced than HermeticWiper, according to Malwarebytes.

How it works: This wiper iterates through the filesystem, enumerates files and overwrites them. This behavior is similar to ransomware activity, but in this case, there is no decryption key. Once the data has been overwritten, it is lost.

> #BREAKING #ESETresearch continues to investigate the #HermeticWiper incident. We uncovered a worm component #HermeticWizard, used to spread the wiper in local networks. We also discovered another wiper, called #IsaacWiper deployed in #Ukraine. https://t.co/hBA2NKy5Lf 1/4 pic.twitter.com/NzPIsYiwWW— ESET Research (@ESETresearch) March 1, 2022

AcidRain

Attribution: Researchers have not yet attributed the attack, but said that it has similarities with VPNFilter malware, which was attributed to the Russian-backed Fancy Bear hacking group by the FBI in 2018. More recently, the NSA and CISA tied it to Sandworm.

Details of the attack: The cyberattack on U.S. satellite communications provider Viasat disrupted its work across central and eastern Europe. A destructive wiper malware AcidRain rendered Viasat's KA-SAT network inoperable on February 24, the day of Russia's invasion of Ukraine.

This attack also disconnected remote access to about 5,800 Enercon wind turbines across Germany and disrupted the work of thousands of European organizations due to issues with satellite communications.

The attack took place in two phases, according to Viasat's statement: first, the DDoS attack temporarily knocked offline modems physically located within Ukraine. Then, modems gradually disappeared from the Viasat service.

Description: A new strain of wiper malware called AcidRain was discovered by SentinelLabs researchers on March 15 after it was uploaded to VirusTotal from a user in Italy with the name "ukrop," which the researchers say could be shorthand for "Ukraine operation."

AcidRain was designed to remotely erase vulnerable modems and routers, according to SentinelLabs. A wiper can overwrite key data in a modem's flash memory, rendering it inoperable and in need of reflashing or replacing.

How it works: The wiper performs an in-depth wipe of the filesystem and various known storage device files, before attempting to destroy the data. Once the wiping processes are complete, the device is rebooted and ultimately rendered inoperable.

CaddyWiper

Attribution: Not yet determined.

Details of the attack: This data-destroying malware affected a few dozen systems in a limited number of organizations on March 14, according to ESET.

Then it was used again during the attack on the Ukrainian energy company on April 12, according to CERT-UA.

In both cases it was deployed via Group Policy Object (GPO), indicating the attackers had control of the target's network beforehand.

> #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/gVzzlT6AzN— ESET Research (@ESETresearch) March 14, 2022

Description: This malware erases user data and splits information from any drives attached to a compromised machine. CaddyWiper does not share any significant code similarity with HermeticWiper or IsaacWiper. It was probably compiled the same day it was deployed to targeted networks. Its sample was written in C++.

How it works: CaddyWiper overwrites files on the computer with null byte characters, making them unrecoverable. This malware can be executed with or without administrator privilege. In both cases, it causes

lethal damage to the target machine. CaddyWiper execution without administrator privileges makes files worthless, according to Morphisec.

DoubleZero

Attribution: Not yet determined

Details of the attack: Hackers have launched spear-phishing attacks to disrupt the work of Ukrainian enterprises, according to CERT-UA. Ukrainian cybersecurity researchers traced several ZIP archives containing DoubleZero destructive malware.

Description: DoubleZero is a .NET-based malware that destroys files and registry keys on the infected system, according to the Cisco Talos threat intelligence group. The malware first destroys non-system files and then system-related files.

Before shutting down the system, DoubleZero destroys the following Windows registry branches: HKCU, HKU, HKLM, HKLM\BCD.

How it works: DoubleZero erases files in two ways: by overwriting them with zero blocks of 4096 bytes (FileStream.Write method) or using NtFileOpen, NtFsControlFile API calls (code: FSCTL_SET_ZERO_DATA).

It is still not clear how hackers compromised their victims, but according to eSentire Threat Intelligence, they could gain access to the infected machines and use the existing administrative privileges or bypass the user account control to manually execute the malware.

It is now impossible to determine when DoubleZero was compiled because hackers changed the timestamp to confuse the researchers.

Industroyer2

Attribution: Sandworm (UAC-0082)

Details of the attack: Russian hackers from the GRU military intelligence agency used Industroyer2 to attack electrical substations of the Ukrainian energy company in the west-central Vinnytsia region, according to ?.

In addition to Industroyer2, Sandworm hackers used wiper malware called CaddyWiper and regular disk wipers for Linux and Solaris operating systems—ORCSHRED, SOLOSHRED, and AWFULSHRED.

Sandworm tried to repeat its successful 2016 attack on Kyiv's power grid when the initial variant of Industroyer caused blackouts in parts of the city. This time Ukrainian officials say they thwarted the attack and no electrical outages were recorded.

Description: This malware is capable of interacting with industrial control systems (ICS) typically found in electric power systems, according to the cybersecurity firm ESET said that it does not yet know how attackers moved from the IT network to the ICS network.

Industroyer2 was compiled on March 23, but hackers penetrated the power grid networks at the end of February—before Russia invaded Ukraine—and uploaded Industroyer2 malware later, according to the Ukrainian state-

controlled cyberattacks response team CERT-UA.

How it works: Industroyer2 only implements the IEC 60870-5-104 protocol to communicate with industrial equipment. It can communicate with multiple devices at once. Before connecting to the targeted devices, Industroyer2 terminates its daily operation and renames its file to prevent the automatic restart of its work.

No previous article

No new articles

Daryna Antoniuk

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.
