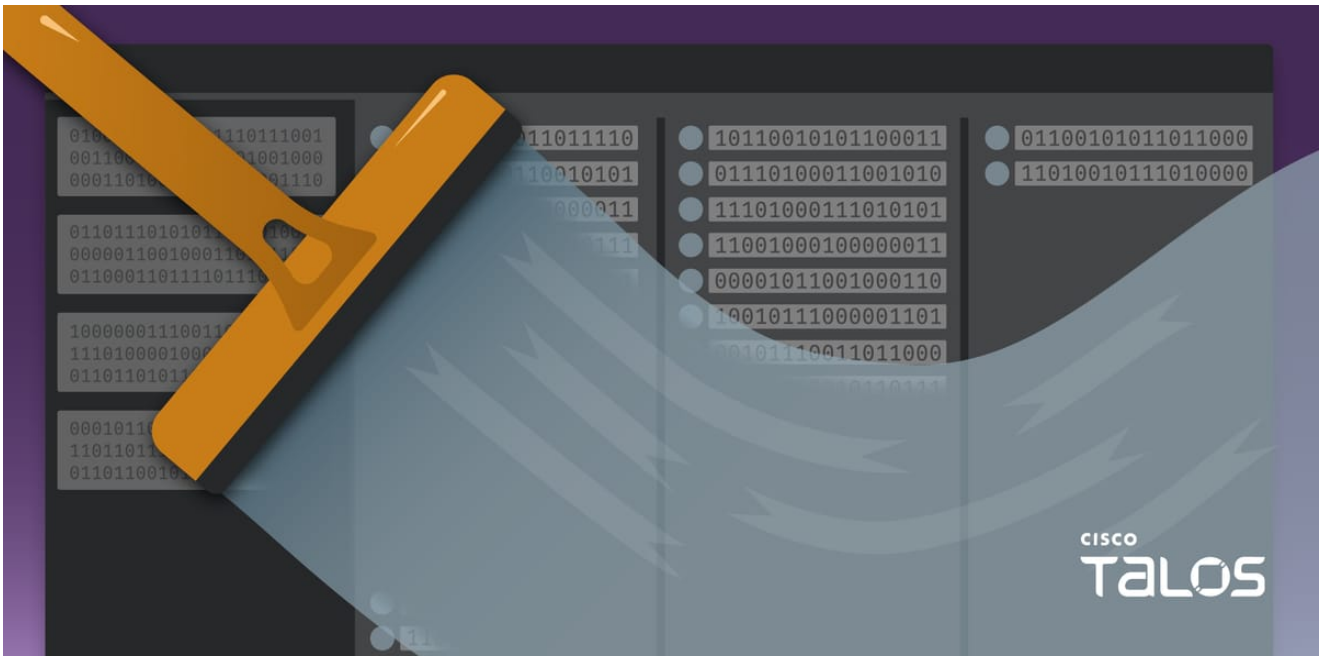
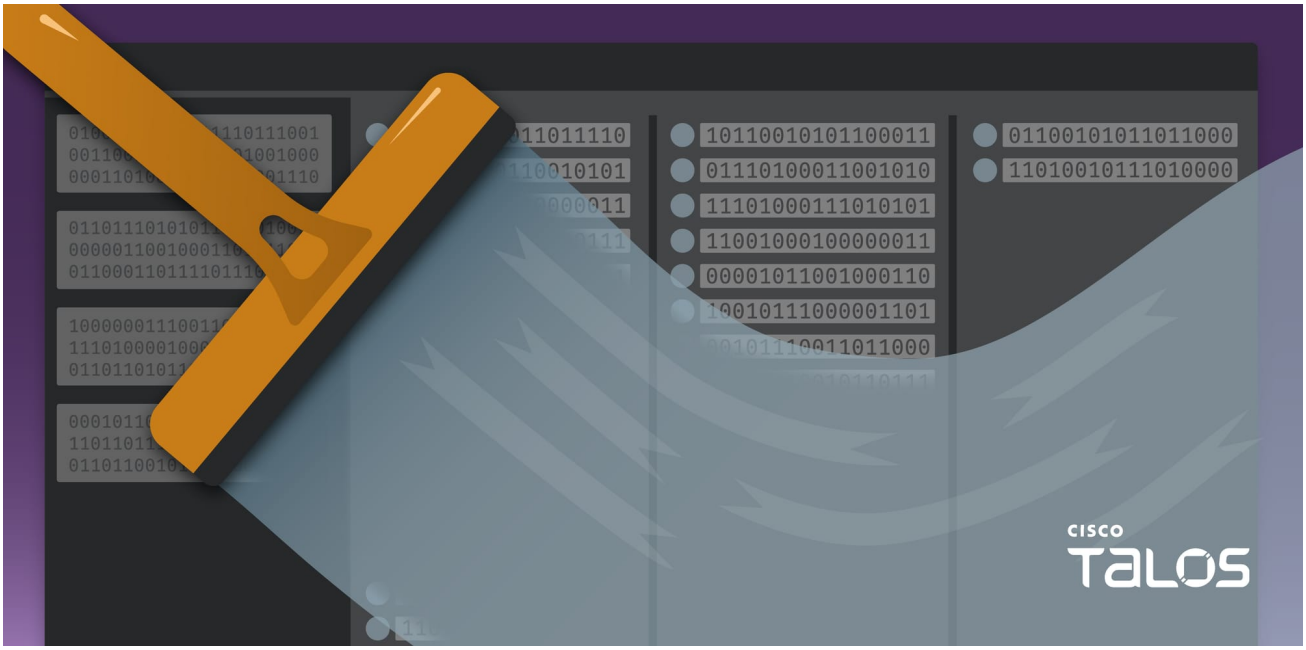
Newly identified wiper malware “PathWiper” targets critical infrastructure in Ukraine

blog.talosintelligence.com/pathwiper-targets-ukraine/

June 5, 2025





By Jacob Finn, Dmytro Korzhevin, Asheer Malhotra

Thursday, June 5, 2025 06:00

APT Ukraine wiper Threat Advisory

- Cisco Talos observed a destructive attack on a critical infrastructure entity within Ukraine, using a previously unknown wiper we are calling “PathWiper”.
- The attack was instrumented via a legitimate endpoint administration framework, indicating that the attackers likely had access to the administrative console, that was then used to issue malicious commands and deploy PathWiper across connected endpoints.
- Talos attributes this disruptive attack and the associated wiper to a Russia-nexus advanced persistent threat (APT) actor. Our assessment is made with high confidence based on tactics, techniques and procedures (TTPs) and wiper capabilities overlapping with destructive malware previously seen targeting Ukrainian entities.
- The continued evolution of wiper malware variants highlights the ongoing threat to Ukrainian critical infrastructure despite the longevity of the Russia-Ukraine war.

Proliferation of PathWiper

Any commands issued by the administrative tool’s console were received by its client running on the endpoints. The client then executed the command as a batch (BAT) file, with the command line partially resembling that of Impacket command executions, though such commands do not necessarily indicate the presence of Impacket in an environment.

The BAT file consisted of a command to execute a malicious VBScript file called ‘uacinstall.vbs’, also pushed to the endpoint by the administrative console:

```
C:\WINDOWS\System32\WScript.exe C:\WINDOWS\TEMP\uacinstall.vbs
```

Upon execution, the VBScript wrote the PathWiper executable, named ‘sha256sum.exe’, to disk and executed it:

```
C:\WINDOWS\TEMP\sha256sum.exe
```

Throughout the course of the attack, filenames and actions used were intended to mimic those deployed by the administrative utility’s console, indicating that the attackers had prior knowledge of the console and possibly its functionality within the victim enterprise’s environment.

PathWiper capabilities

On execution, PathWiper replaces the contents of artifacts related to the file system with random data generated on the fly. It first gathers a list of connected storage media on the endpoint, including:

- Physical drive names
- Volume names and paths
- Network shared and unshared (removed) drive paths

Although most storage devices and volumes are discovered programmatically (via APIs), the wiper also queries 'HKEY_USERS\Network\<drive_letter>| RemovePath' to obtain the path of shared network drives for destruction.

Once all the storage media information has been collected, PathWiper creates one thread per drive and volume for every path recorded and overwrites artifacts with randomly generated bytes. The wiper reads multiple file systems attributes, such as the following from New Technology File System (NTFS). PathWiper then overwrites the contents/data related to these artifacts directly on disk with random data:

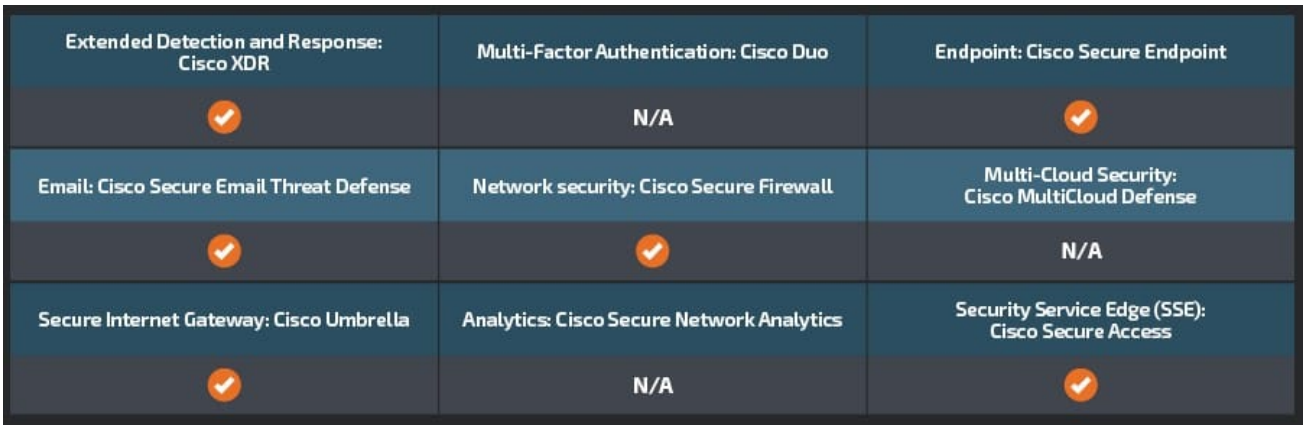
- MBR
- $MFT
- $MFTMirr
- $LogFile
- $Boot
- $Bitmap
- $TxfLog
- $Tops
- $AttrDef

Before overwriting the contents of the artifacts, the wiper also attempts to dismount volumes using the 'FSCTL_DISMOUNT_VOLUME IOCTL' to the MountPointManager device object. PathWiper also destroys files on disk by overwriting them with randomized bytes.

PathWiper's mechanisms are somewhat semantically similar to another wiper family, HermeticWiper, previously seen targeting Ukrainian entities in 2022. HermeticWiper, also known as FoxBlade or NEARMISS, is attributed to Russia's Sandworm group in third-party reporting with medium to high confidence. Both wipers attempt to corrupt the master boot record (MBR) and NTFS-related artifacts.

A significant difference between HermeticWiper and PathWiper is the corruption mechanisms used against recorded drives and volumes. PathWiper programmatically identifies all connected (including dismounted) drives and volumes on the system, identifies volume labels for verification and documents valid records. This differs from HermeticWiper's simple process of enumerating physical drives from 0 to 100 and attempting to corrupt them.

Coverage



Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Cisco Secure Access is a modern cloud-delivered Security Service Edge (SSE) built on Zero Trust principles. Secure Access provides seamless transparent and secure access to the internet, cloud services or private application no matter where your users work. Please contact your Cisco account representative or authorized partner if you are interested in a free trial of Cisco Secure Access.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

Snort 2 rules: 64742, 64743

Snort 3 rules: 301174

Indicators of compromise (IOCs)

```
7C792A2B005B240D30A6E22EF98B991744856F9AB55C74DF220F32FE0D00B6B3
```


© Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.