LevelBlue - Open Threat Exchange

By PetrP.73

Archived: 2026-04-05 12:42:27 UTC

DynoWiper update: Technical analysis and attribution

CVE: 1 | **FileHash-MD5:** 6 | **FileHash-SHA1:** 7 | **FileHash-SHA256:** 6 | **URL:** 1 | **Domain:** 1

ESET researchers have identified a recent data destruction incident involving a new wiper malware named DynoWiper, attributed to the Russia-aligned threat group Sandworm. Sandworm is notorious for its destructive cyber operations targeting various sectors, including energy, transportation, and government, as exemplified by past attacks such as NotPetya and Olympic Destroyer. DynoWiper was deployed on December 29, 2025, in the shared directory C:\inetpub\pub\, using executable filenames like schtask.exe and schtask2.exe. Notably, the references to a Visual Studio project path suggest that the malware may have been developed in an environment utilizing the Vagrant tool for managing virtual machines. This indicates that Sandworm possibly tested DynoWiper on virtual machines before unleashing it within the target organization’s network.

- 161 Subscribers

- 258 Subscribers

Sandworm behind cyberattack on Poland's power grid in late 2025

FileHash-SHA1: 1

In late 2025, Poland's energy system was targeted by a major cyberattack, now attributed to the Russia-aligned APT group Sandworm by ESET Research. The attack involved data-wiping malware named DynoWiper, detected as Win32/KillFiles.NMO. While the full impact is still under investigation, researchers noted the attack's timing coincided with the 10th anniversary of Sandworm's 2015 attack on Ukraine's power grid. Sandworm continues to target critical infrastructure, particularly in Ukraine, with regular wiper attacks. The group's history of disruptive cyberattacks and the similarities in tactics, techniques, and procedures led to a medium-confidence attribution of this latest incident to Sandworm.

- 373,890 Subscribers

Weaponized Military Documents Deliver Advanced SSH-Tor Backdoor

FileHash-MD5: 7 | **FileHash-SHA1:** 7 | **FileHash-SHA256:** 8 | **URL:** 3 | **Domain:** 2 | **Hostname:** 2

Cyble is the world’s leading AI-driven security intelligence platform, providing a platform that can outsmart and prevent cyber attacks, incidents, and attacks on the dark web and other sites.

- 841 Subscribers

Weaponized Military Documents Deliver Advanced SSH-Tor Backdoor to Defense Sector.

FileHash-MD5: 12 | **FileHash-SHA1:** 11 | **FileHash-SHA256:** 13 | **URL:** 2 | **Domain:** 3

In October 2025, a sophisticated cyber attack was identified targeting the defense sector through a weaponized ZIP archive disguised as a PDF document related to military operations. The malware employs a multi-layered approach involving nested ZIP archives, LNK file disguises, and anti-sandbox checks to circumvent automated detection mechanisms. Upon interaction with the lure document, the attack is initiated through a LNK file that executes embedded PowerShell commands, facilitating the extraction and execution of further malicious payloads. The embedded PowerShell script first extracts a secondary ZIP file into a specific directory, then executes additional operations to establish persistence within the victim's system. Notably, the malware verifies system characteristics before proceeding, ensuring it bypasses environments designed for analysis by checking for a minimum number of LNK files and running processes, thus evading detection in sandbox setups.

- 161 Subscribers

Query Registry, Technique T1012 - Enterprise | MITRE ATT&CK®

CVE: 1 | **URL:** 6 | **Domain:** 2 | **Hostname:** 2

Adversaries can access the Windows Registry to gather information about the operating system, configuration, and installed software, as well as to make modifications to the system's registry, according to a report published in the Security Research Institute (CTI).

- 122 Subscribers

Google TI

CVE: 14 | **FileHash-MD5:** 31 | **FileHash-SHA1:** 20 | **FileHash-SHA256:** 30 | **URL:** 22 | **YARA:** 3 | **Domain:** 40 | **Hostname:** 19

- 1 Subscribers

- 841 Subscribers

- 258 Subscribers

- 103 Subscribers

Gozi strikes again, targeting banks, cryptocurrency and more

CVE: 1 | **FileHash-MD5:** 1 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 1 | **URL:** 6 | **Domain:** 6

Gozi, a strain of malware that has targeted banks, financial services and cryptocurrency companies, is now targeting Asia, according to security researcher X-Force, who has been working with the organisation for the past decade.

- 82 Subscribers

- 164 Subscribers

Threat Profile: RedLine Infostealer

FileHash-MD5: 308 | **FileHash-SHA1:** 308 | **FileHash-SHA256:** 307 | **URL:** 54 | **Domain:** 7 | **Email:** 1 | **Hostname:** 10

information stealer, named RedLine Stealer by the author, was identified being delivered through spam email campaigns, the malware is offered for sale on Russian dark web forums and as a tiered subscription allowing threat actors to use the information stealer, subscribe at different costs and purchase different access levels. In addition to being a password stealer, RedLine has the capabilities to steal login information, autocomplete data, passwords, and credit cards information from browsers.

- 240 Subscribers

Threat Profile: RedLine Infostealer

FileHash-MD5: 308 | **FileHash-SHA1:** 308 | **FileHash-SHA256:** 307 | **URL:** 54 | **Domain:** 7 | **Email:** 1 | **Hostname:** 10

information stealer, named RedLine Stealer by the author, was identified being delivered through spam email campaigns, the malware is offered for sale on Russian dark web forums and as a tiered subscription allowing threat actors to use the information stealer, subscribe at different costs and purchase different access levels. In addition to being a password stealer, RedLine has the capabilities to steal login information, autocomplete data, passwords, and credit cards information from browsers.

- 240 Subscribers

- 505 Subscribers

- 505 Subscribers

- 505 Subscribers

- 505 Subscribers

- 505 Subscribers

- 354 Subscribers
