Russian Sandworm group attacks energy company in Poland with DynoWiper, ESET Research discovers

Archived: 2026-04-29 07:13:15 UTC

- ESET researchers identified new data-wiping malware that ESET named DynoWiper, used against an energy company in Poland.
- The TTPs observed during the DynoWiper incident closely resemble those seen previously in an incident involving another data wiper, ZOV, in Ukraine.
- ESET Research attributes DynoWiper to the Russia-aligned threat group Sandworm with medium confidence.
- The incident is a rare and unreported case in which a Russia-aligned threat actor deployed destructive, data-wiping malware against an energy company in Poland.

BRATISLAVA — January 30, 2026 — ESET researchers identified new data-wiping malware that they named DynoWiper, used against an energy company in Poland. The tactics, techniques, and procedures (TTPs) observed during the DynoWiper incident closely resembles the previous one involving the ZOV wiper in Ukraine: Z, O, and V are Russian military symbols. ESET Research attributes DynoWiper to Russia-aligned threat group Sandworm with medium confidence.

This incident represents a rare and previously undocumented case in which a Russia-aligned threat actor deployed destructive, data-wiping malware against an energy company in Poland. In 2025, ESET investigated more than 10 incidents involving destructive malware attributed to Sandworm, almost all of them occurring in Ukraine.

The installed EDR/XDR product, ESET PROTECT, blocked execution of the wiper, significantly limiting its impact in the environment. CERT Polska did an excellent job investigating the incident and published a detailed analysis in a report available on its website.

On December 29th, 2025, DynoWiper samples were deployed to what probably is a shared directory in the victim's domain. It is possible that Sandworm operators first tested the operation on virtual machines before deploying the malware in the target organization. Three distinct samples were deployed and all attempts failed. The wiper overwrites files using a 16-byte buffer that contains random data generated at a single instance at the start of the wiper's execution. On an unprotected machine, files of size 16 bytes or fewer are fully overwritten. To speed up the destruction process, files larger than 16 bytes have only some parts of their contents overwritten. DynoWiper wipes files on all removable and fixed drives and finally forces the system to reboot, completing the destruction of the system.

Unlike other Sandworm malware including Industroyer and Industroyer2, the newly discovered DynoWiper samples focus solely on the IT environment, with no observed functionality targeting operational technology industrial components. However, this does not exclude the possibility that such capabilities were present elsewhere in the attack chain.

ESET Research identified several similarities to previously known destructive malware, specifically to the wiper ZOV, which ESET attributes to Sandworm with high confidence. DynoWiper operates in a broadly similar fashion to the ZOV wiper. Notably, the exclusion of certain directories and especially the clear separate logic present in the code for wiping smaller and larger files can also be found in the ZOV wiper. ZOV is destructive malware that we detected being deployed against a financial institution in Ukraine in November 2025. Once executed, the ZOV wiper iterates over files on all fixed drives and wipes them by overwriting their contents. There was another ZOV wiper case at an energy company in Ukraine, where the attackers deployed the wiper on January 25th, 2024.

Sandworm is a Russia-aligned threat group that performs destructive attacks, targeting a wide range of entities including government agencies, logistics companies, transportation firms, energy providers, media organizations, grain sector companies, and telecommunications companies. These attacks typically involve the deployment of wiper malware – malicious software designed to delete files, erase data, and render systems unbootable.

Besides Ukraine, the group has a decade-long history of targeting companies in Poland, including those in the energy sector. In October 2022, it carried out a destructive attack against logistics companies in both Ukraine and Poland, disguising the operation as a Prestige ransomware incident. Because the majority of Sandworm's cyberattacks currently target Ukraine, we collaborate closely with our Ukrainian partners, including the Computer Emergency Response Team of Ukraine (CERT-UA), to support both prevention and remediation efforts.

For a more detailed analysis of DynoWiper and Sandworm, check out the latest ESET Research blogpost "DynoWiper update: Technical analysis and attribution" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

Wallpaper dropped by the ZOV wiper

About ESET

ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit www.eset.com or follow our social media, podcasts, and blogs.

Source: https://www.eset.com/us/about/newsroom/research/eset-research-russian-sandwormapt-attacks-energy-company-poland-with-dynowiper/