Recent OT and Espionage Attacks Linked to Russia's Sandworm, Now Named APT44

By Eduard Kovacs

Published: 2024-04-17 · Archived: 2026-04-05 17:19:19 UTC

Google Cloud's Mandiant on Wednesday published a new report summarizing some of the latest activities of Russia's notorious Sandworm group, which it has started tracking as APT44.

Sandworm is one of Russia's most well-known threat groups, being involved in operations whose goal is espionage, disruption, or disinformation. It's known for the use of highly disruptive malware such as BlackEnergy and Industroyer.

Since the start of Russia's war against Ukraine, the group has focused on causing disruption within Ukraine, using wipers and other tactics to achieve its goals. Its cyber operations are often timed with conventional military activities.

Sandworm has often been believed to be the same as APT28 (Fancy Bear). While some of their activities overlap and they are both part of the GRU security service's Information Operations Troops (VIO), Mandiant says they are different groups and the company has decided to "graduate" Sandworm to a named advanced persistent threat, APT44.

Mandiant's new report reveals that APT44 has been using several hacktivist personas, including Cyber Army of Russia Reborn (CARR), XAKNET, and Solntsepek.

CARR is interesting because in the past months it has made some claims about being able to manipulate critical infrastructure operational technology (OT) assets in the United States and the European Union.

In January, the 'hacktivists' posted videos showing that they were able to manipulate human-machine interfaces (HMIs) at water utilities in Poland and the US. In March, the group posted a video allegedly showing that it disrupted energy generation at a hydroelectric facility in France by manipulating water levels.

While their claims could not be verified, publicly available information suggests that the hackers may have indeed caused some disruption.

"Approximately two weeks after the Telegram post taking credit for the U.S. targeting, a local official publicly confirmed a 'system malfunction' that led to a tank overflowing at one of the claimed victim facilities," Mandiant said in its report. "This activity was reportedly part of a series of cyber incidents impacting multiple local U.S. water infrastructure systems that stemmed from 'vendor software they use that keeps their water systems remotely accessible'."

Mandiant told *SecurityWeek* that its latest report for the first time links APT44 to several attacks and operations.

For instance, since at least April 2023, APT44 has provisioned infrastructure that may have been used by forward-deployed Russian military forces to exfiltrate encrypted Signal and Telegram messages from mobile devices captured on the battlefield.

APT44 has also conducted a supply chain attack involving wiper malware.

"In one recent case, access to a software developer resulted in the downstream compromise of critical infrastructure networks in Eastern Europe and Central Asia, followed by the deployment of wiper malware to a select victim organization," Mandiant said.

A recent attack that targeted the Netherlands-based investigative journalism group Bellingcat and other similar entities is now also being attributed to APT44 for the first time.

**APT44, according to Malpedia, is also tracked as Blue Echidna, Electrum, FrozenBarents, G0034, Iridium, Iron Viking, Quedagh, Seashell Blizzard, TEMP.Noble, TeleBots, UAC-0082, UAC-0113, and Voodoo Bear.*

Related: Destructive ICS Malware 'Fuxnet' Used by Ukraine Against Russian Infrastructure

Related: Russian Turla Cyberspies Target Polish NGOs With New Backdoor

---