Russian hackers wiped thousands of systems in KyivStar attack

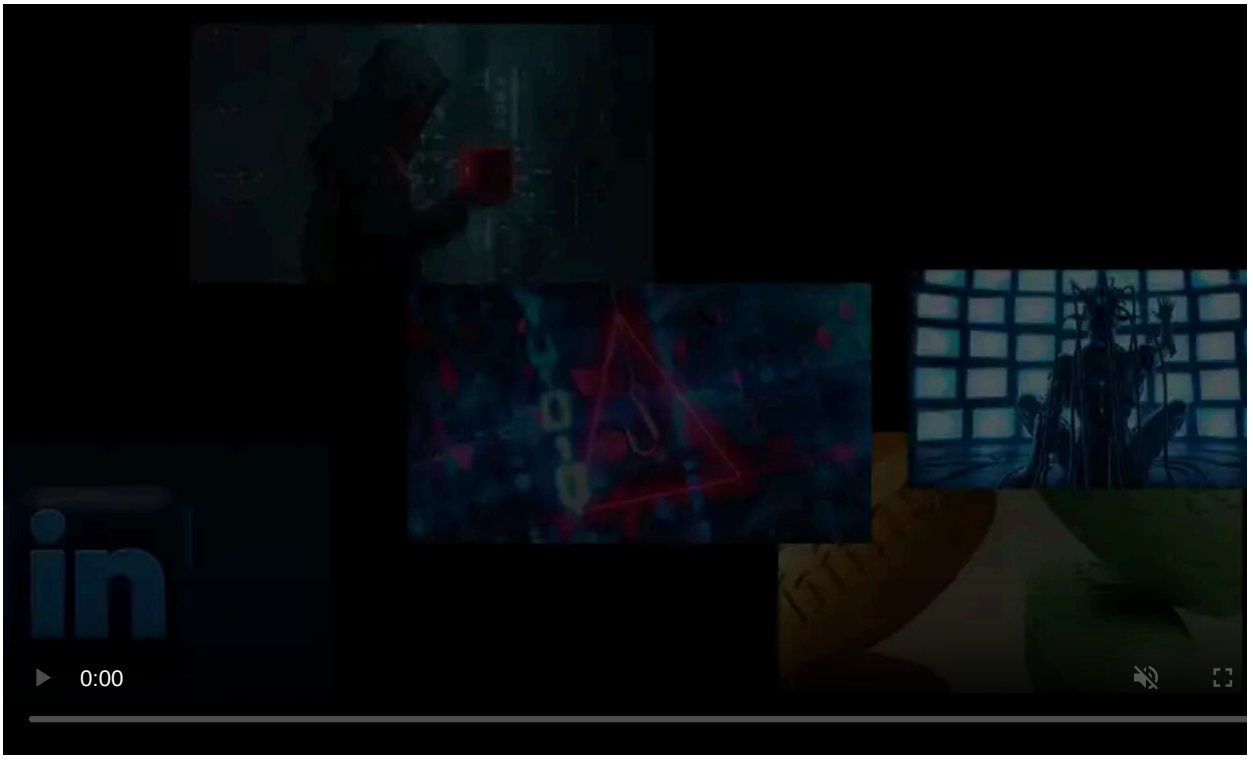
By Sergiu Gatlan

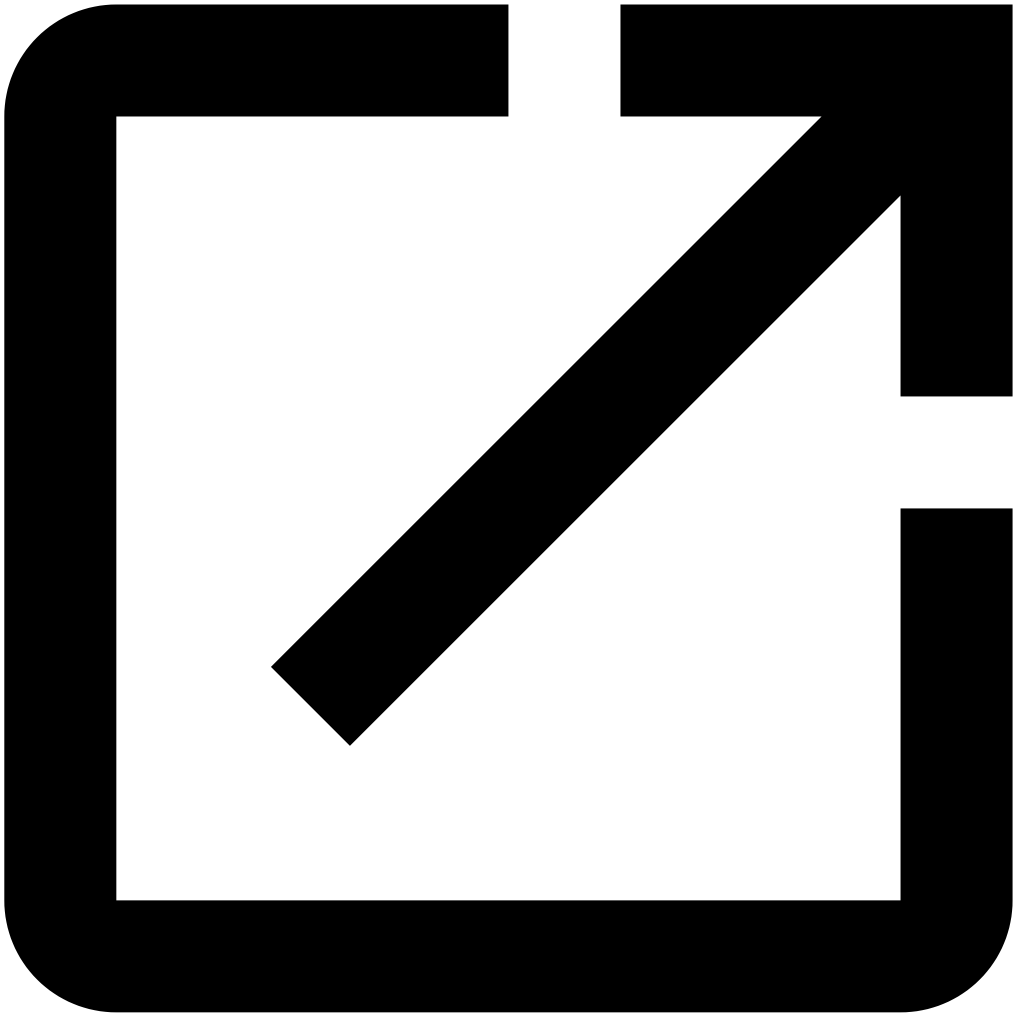
Published: 2024-01-04 · Archived: 2026-04-05 16:44:46 UTC

The Russian hackers behind a December breach of Kyivstar, Ukraine's largest telecommunications service provider, have wiped all systems on the telecom operator's core network.

Following the incident, Kyivstar's mobile and data services went down, leaving most of its 25 million mobile and home internet subscribers without an internet connection.

Illia Vitiuk, the head of the Security Service of Ukraine's (SSU) cybersecurity department, told Reuters in an interview that the threat actors breached Kyivstar's network in May 2023.


0:00



They launched the attack months later, wiping thousands of virtual servers and computers and "completely" destroying "the core" of the telecoms operator.

"For now, we can say securely, that they were in the system at least since May 2023. I cannot say right now, since what time they had ... full access: probably at least since November," he said.

"After a large-scale break, we prevented a number of attempts to cause even more damage to the operator," Vitiuk added in a statement published on Thursday SSU's website.

"Currently, the cyber specialists of the Security Service are already researching individual samples of malware used by the enemy. The attack was carefully prepared for many months."

The cyberattack had a considerable impact on the country's civilian population, yet it notably did not significantly disrupt military communications. Vitiuk said that this is because of Ukraine's Defense Forces employing different algorithms and communication protocols.

Breached by Sandworm military hackers

Following the incident, Kyivstar's CEO and the SSU suggested that Russian hackers may have been involved, given the ongoing conflict between Ukraine and Russia.

One day later, the attack was claimed by Russian hackers from the Solntsepek group (believed to be linked to the Sandworm Russian military hacking group). They said they wiped 10,000 computers and thousands of servers on Kyivstar's network.

"We, the Solntsepek hackers, take full responsibility for the cyber attack on Kyivstar. We destroyed 10 thousand computers, more than 4 thousand servers, all cloud storage and backup systems," the group said in a Telegram post.

"We attacked Kyivstar because the company provides communications to the Armed Forces of Ukraine, as well as government agencies and law enforcement agencies of Ukraine."

Today, Vityuk confirmed that Sandworm was behind the December attack on Kyivstar, saying that this Russian military intelligence unit carried out other cyberattacks targeting Ukrainian targets, "in particular [..] telecom operators and ISPs."

An October report from Ukraine's Computer Emergency Response Team (CERT-UA) revealed that Russian Sandworm hackers breached the networks of 11 Ukrainian telecom service providers since May 2023.

This has led to service interruptions after the hackers deployed scripts during the final stages of the attacks to wipe Mikrotik equipment and backups to make recovery more challenging.

Source: https://www.bleepingcomputer.com/news/security/russian-hackers-wiped-thousands-of-systems-in-kyivstar-attack/