CEO of Ukraine's largest telecom operator describes Russian cyberattack that wiped thousands of computers

By Daryna Antoniuk

Published: 2024-02-09 · Archived: 2026-04-05 20:42:25 UTC

In the two months since Russia-linked hackers attacked Ukraine’s largest telecom operator, many questions have emerged about how they gained access to the company's systems and lingered there, likely for months, undetected.

During a cybersecurity conference in Kyiv this week, Kyivstar CEO Oleksandr Komarov shed some light on what happened during the attack that left nearly 24 million customers in Ukraine without a mobile signal and internet for days.

Responding to a question from Recorded Future News about how the hackers gained initial access to Kyivstar systems, Komarov said that they likely compromised an employee account and then spent some time gaining access to other accounts, which eventually led them to those with administrative privileges. Then, they gained control over Active Directory — a centralized database that stores information about network resources and the directory's structure — "and could do whatever they wanted from there."

The head of the cybersecurity department at Ukraine’s security service (SBU), Illia Vitiuk, told Recorded Future News during the conference that it’s unlikely that the attack on Kyivstar originated from within the company — a possibility considered in the days following the attack.

"There isn't sufficient evidence to suggest that the network was compromised from the inside. We’ve seen how hackers navigated through the network, escalating their privileges. If they had an insider, it could have been done much more quickly," Vitiuk said.

According to him, the investigation into the incident is still ongoing and will "continue for a long time" because hackers “destroyed hundreds of Kyivstar servers and wiped thousands of computers, making it difficult to trace their movement through the network."

Kyivstar CEO Oleksandr Komarov. Image: Kyiv International Cyber Resilience Forum/Facebook

"Now what's more important for us is not just how they initially gained access to the network, but how they managed to navigate it, circumventing substantial security measures at Kyivstar," he added.

According to Vitiuk, the hackers attempted to penetrate Kyivstar in March 2023 or earlier, managed to get into the system at least as early as May, and likely gained full access to the network in November.

As for why they remained undetected for months, Komarov said that the group used a zero-day wiper malware, which Kyivstar's protection systems couldn't identify.

The hackers, previously attributed by the SBU to the Russian state-controlled threat group Sandworm, which overlaps with Seashell Blizzard and UAC-0082, planned to attack Kyivstar in two waves — targeting virtual and physical infrastructure, Komarov said.

While they succeeded in wiping out the virtual servers, their attempt to cause damage to physical equipment failed.

There are several reasons why the attack on physical infrastructure was thwarted, according to Komarov: the company swiftly responded to the incident and disconnected the equipment; a conflict arose between the two attacks, with one hindering the development of the other; and the group did not consider the diversity of vendors serving Kyivstar's physical infrastructure.

If the second wave of the attack succeeded, it could have damaged nearly 100,000 of Kyivstar’s base transceiver stations that linked mobile devices to the operator’s network. Given that they can only be fixed manually, Kyivstar would have needed months to restore communication, according to Komarov.

Lessons learned

Komarov called the attack on Kyivstar "a meticulously planned military operation that lasted several months." However, he dismissed the idea that the company was ill-prepared for Russian cyberattacks, stating that Ukrainian telecom operators have faced continuous cyber threats since the beginning of the war.

“Kyivstar worked according to the best international standards — we invested millions of dollars in cybersecurity, and we have 50 people working in our cyber protection team,” he said.

However, amid the ongoing cyber war, critical infrastructure companies are more susceptible to attacks, especially when dealing with sophisticated threat actors controlled by Russian intelligence.

Another factor exposing Kyivstar to cyberattacks is the architecture of the telecom operator’s systems. "And this isn't a mistake on Kyivstar's part; it's an industrial approach," Komarov said.

According to him, the company’s infrastructure is too centralized, making it easier for hackers to navigate. Komarov said that the company plans to restructure its systems and make them more segmented — when the network is divided into distinct zones, each with its own set of controls, access permissions, and security measures.

“We had segmentation in place before, but now we're looking to implement micro-segmentation. The aim is to ensure that, while securing the external perimeter, we establish multiple internal perimeters to prevent unrestricted movement between systems — similar to an airport, where entry is allowed only after passing through multiple security checks,” Komarov told Recorded Future News.

No previous article

No new articles

Daryna Antoniuk

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.
