Ukraine says an energy facility disrupted a Fancy Bear intrusion

By Daryna Antoniuk

Published: 2023-09-05 · Archived: 2026-04-05 14:22:59 UTC

An infamous Russian cyberespionage group was caught attacking a critical energy facility in Ukraine, a government agency said on Tuesday.

A cybersecurity expert working for the targeted organization thwarted the attack, according to the report from Ukraine's computer emergency response team (CERT-UA). The agency attributed the incident to Kremlin-controlled hackers known as Fancy Bear or APT28.

CERT-UA said the group targeted an unspecified energy facility in Ukraine, using phishing emails to gain initial access to the targeted systems. Fancy Bear is believed to be associated with the Russian military intelligence agency GRU, and its history includes the attack on the U.S. Democratic National Committee during the 2016 elections.

The content of the malicious email was unusual. In past attacks, Russian hackers typically faked government documents or, in the case of Fancy Bear, distributed bogus software update advisories.

However, this time, the email shared by CERT-UA included three images and the following message: *"Hi! I talked to three girls, and they agreed. Their photos are in the archive; I suggest checking them out on the website."*

In addition to these images, the archive also contains a file in BAT format. BAT files are scripts used in Windows to automate various tasks.

When the victim runs this file, it opens a few fake web pages that are meant to look innocent, but it executes a harmful script on the targeted device.

The attackers also installed Tor on the victim's computer, researchers said. The software allows anonymous internet browsing by routing network traffic through a network of volunteer-operated servers, making it challenging to trace the data's source.

In the recent attack, an employee identified the cyberthreat and took steps to respond, CERT-UA said. They restricted access to certain web resources related to the Mockbin service, a tool used for testing and development, the report said. Fancy Bear has used Mockbin in the past to target Ukrainian government agencies.

Additionally, the energy facility blocked the use of Windows Script Host, a system for automating tasks in the Windows operating system, CERT-UA said.

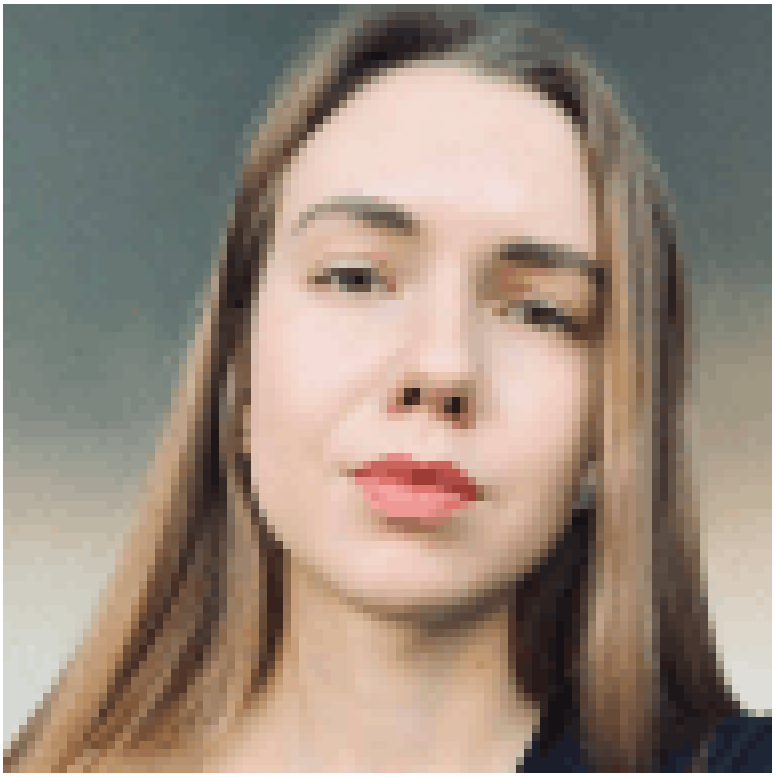
CERT-UA has not disclosed any information about the hackers' specific target. It has been some time since Ukrainian authorities publicly reported an attack on the country's energy infrastructure. Last fall, Ukraine experienced a combination of missile strikes and cyberattacks on its energy infrastructure, as Russia aimed to disrupt the country's power supply.

The onslaught resulted in the destruction of power plants, major transmission lines, and substations, leading to daily blackouts lasting for several hours.

The attacks stopped with the arrival of warmer weather, but there are concerns that new blackouts may occur this upcoming fall, as Russia is reportedly preparing its arsenal for such actions. The potential impact on cyberspace activity remains to be seen.

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.
