Poland says Russian military hackers target its govt networks

By Sergiu Gatlan

Published: 2024-05-09 · Archived: 2026-04-05 14:34:11 UTC

Poland says a state-backed threat group linked to Russia's military intelligence service (GRU) has been targeting Polish government institutions throughout the week.

According to evidence found by CSIRT MON, the country's Computer Security Incident Response Team (led by the Polish Minister of National Defense) and CERT Polska (the Polish computer emergency response team), Russian APT28 state hackers attacked multiple government institutions in a large-scale phishing campaign.

The phishing emails tried tricking the recipients into clicking an embedded link that would provide them with access to more information regarding a "mysterious Ukrainian woman" selling "used underwear" to "senior authorities in Poland and Ukraine."

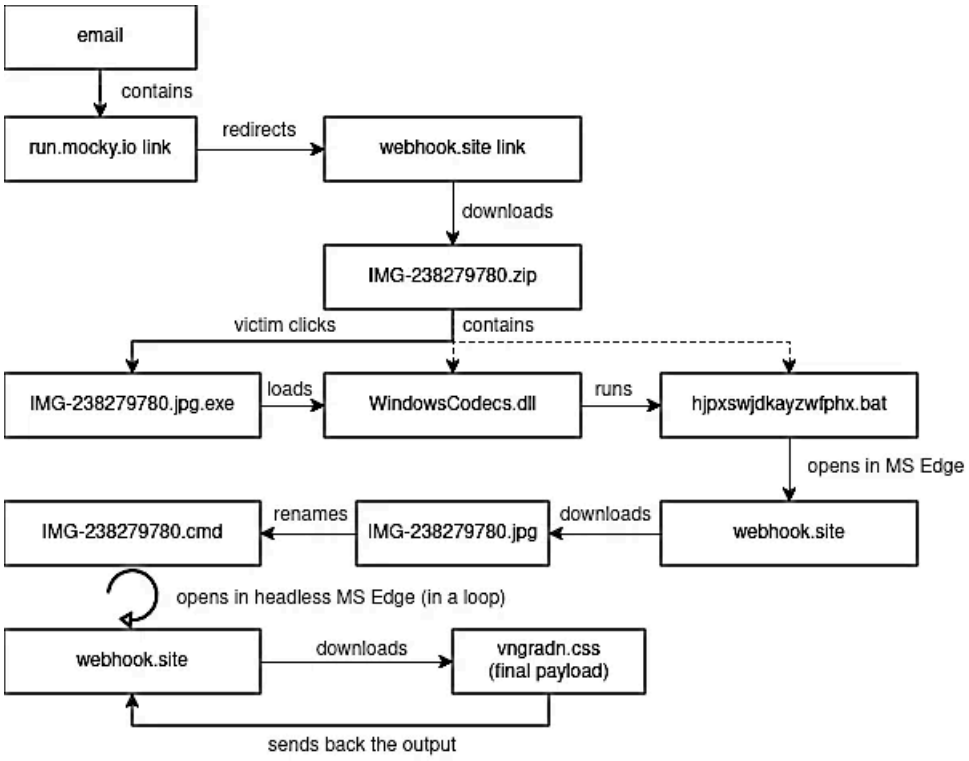

DIE LINKE.
0:00

Once clicked, the link redirected them through multiple websites before landing on a page that downloaded a ZIP archive. The archive contained a malicious executable disguised as a JPG image file and two hidden files: a DLL and a .BAT script.

If the target opens the camouflaged executable file, it loads the DLL via DLL side loading, which runs the hidden script. The script displays a photo of a woman in a swimsuit in the Microsoft Edge browser as a distraction while simultaneously downloading a CMD file and changing its extension to JPG.

"The script we finally received collects only information about the computer (IP address and list of files in selected folders) on which they were launched, and then send them to the C2 server. Probably computers of the victims selected by the attackers receive a different set of the endpoint scripts," CERT Polska said.

The tactics and infrastructure used in these attacks are identical to those used in another highly targeted campaign in which APT28 operatives used Israel-Hamas war lures to backdoor devices of officials from 13 nations, including United Nations Human Rights Council members, with Headlace malware.



APT28 attack flow (CERT Polska)

Since it surfaced in the mid-2000s, the Russian state-backed hacking group has coordinated many high-profile cyber-attacks and was linked to GRU's Military Unit 26165 in 2018.

APT28 hackers were behind hacks of the Democratic National Committee (DNC) and the Democratic Congressional Campaign Committee (DCCC) before the 2016 U.S. Presidential Election and the breach of the German Federal Parliament (Deutscher Bundestag) in 2015.

The United States charged multiple APT28 members for their involvement in the DNC and DCCC attacks in July 2018, while the Council of the European Union sanctioned APT28 in October 2020 for the Bundestag hack.

One week ago, NATO and the European Union, with international partners, also formally condemned a long-term APT28 cyber espionage campaign against multiple European countries, including Germany and Czechia.

Germany said the Russian threat group compromised many email accounts belonging to members of the Social Democratic Party's executive committee. The Czech Ministry of Foreign Affairs also revealed that APT28 targeted some Czech institutions in the same Outlook campaign in 2023.

The attackers exploited the CVE-2023-23397 Microsoft Outlook vulnerability in the attack, a security flaw used as a zero-day to target NATO members in Europe, Ukrainian government agencies, and NATO fast reaction corps starting in April 2022.

"We call on Russia to stop this malicious activity and abide by its international commitments and obligations. With the EU and our NATO Allies, we will continue to take action to disrupt Russia's cyber activities, protect our citizens and foreign partners, and hold malicious actors accountable," the U.S. State Department said in a statement.

Source: https://www.bleepingcomputer.com/news/security/poland-says-russian-military-hackers-target-its-govt-networks/