France ties Russian APT28 hackers to 12 cyberattacks on French orgs

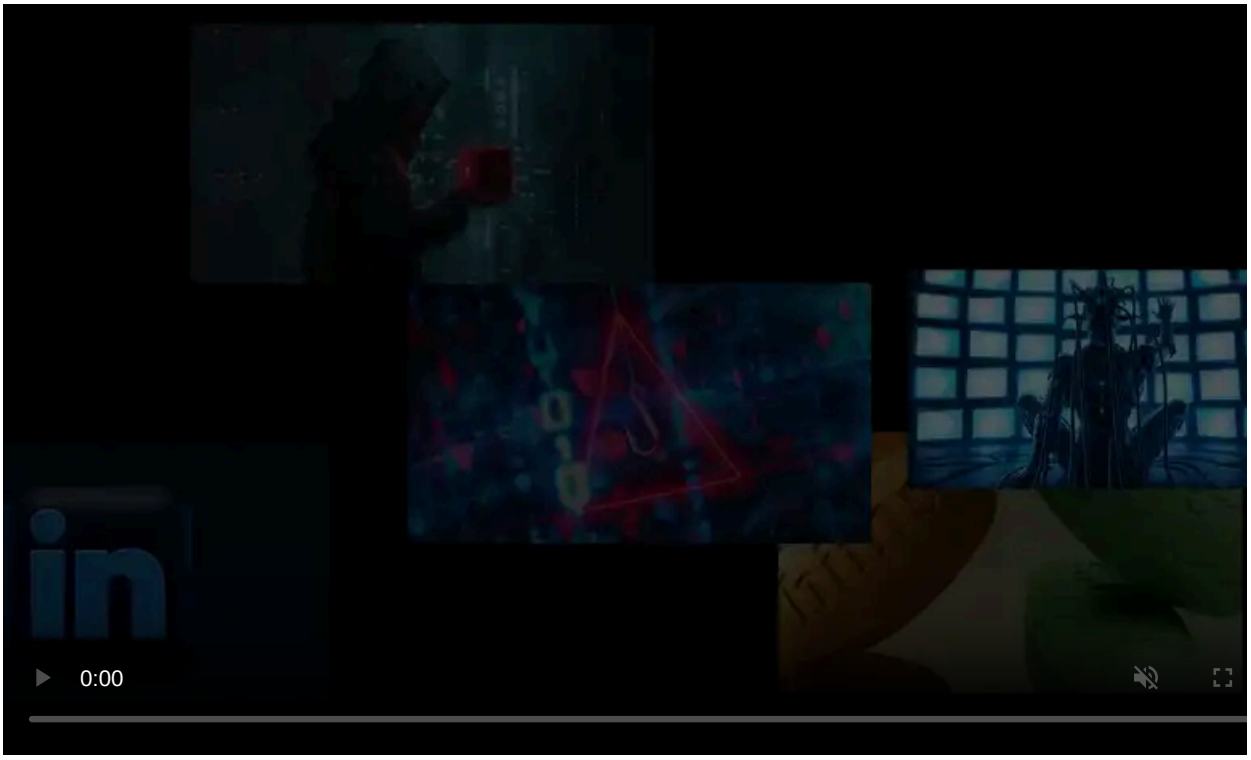
By Sergiu Gatlan

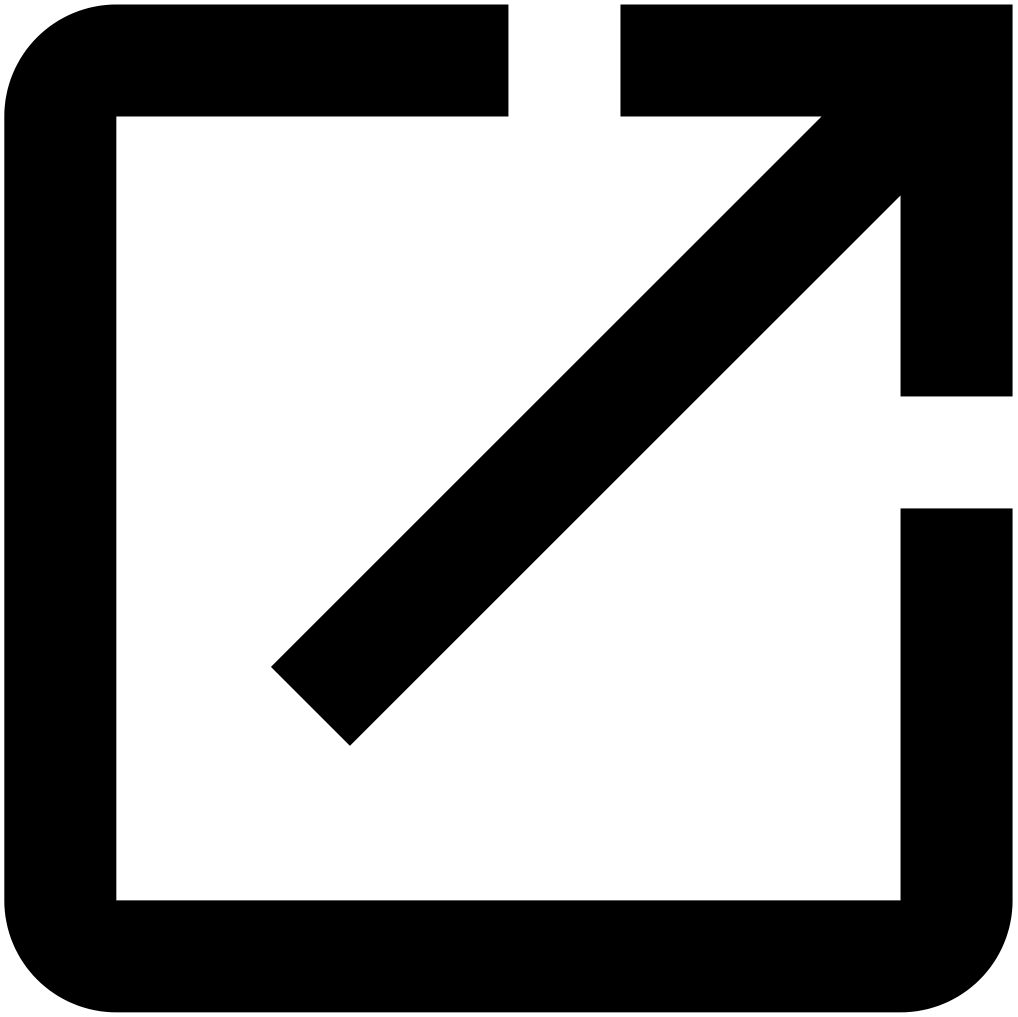
Published: 2025-04-29 · Archived: 2026-04-05 18:18:25 UTC

Today, the French foreign ministry blamed the APT28 hacking group linked to Russia's military intelligence service (GRU) for targeting or breaching a dozen French entities over the last four years.

"France condemns in the strongest terms the use by the Russian military intelligence service (GRU) of the APT28 attack procedure, which has led to several cyber attacks against French interests," a statement released on Tuesday says.

"These destabilizing activities are unacceptable and unworthy of a permanent member of the UN Security Council. They are also contrary to the United Nations standards on the responsible behaviour of states in cyberspace, to which Russia has subscribed."


0:00

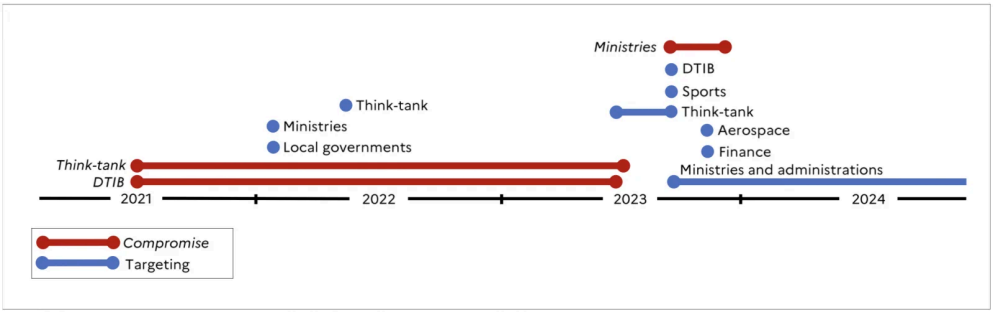


In a separate report published today, the French National Agency for the Security of Information Systems (ANSSI) says the list of French organizations attacked by APT28 military hackers includes ministerial entities, local governments, and administrations, organizations in the French Defence Technological and Industrial Base, aerospace entities, research organizations, think-tanks, and entities in the economic and financial sector.

ANSSI also highlighted several notable APT28 campaigns since 2021, including ones repeatedly targeting Roundcube e-mail servers and several others using free web services for phishing attacks.

It also mentioned the attackers' heavy use of "low-cost and ready-to-use outsourced infrastructure," including free hosting services, VPN services, rented servers, and temporary e-mail address creation services for increased flexibility and stealth.

Since the start of 2024, APT28's attacks have primarily focused on stealing "strategic intelligence" from governmental, diplomatic, research organizations, and think tanks from France, Europe, Ukraine, and North America.



Russian military intelligence attacks against French entities (ANSSI)

This isn't the first time ANSSI has linked the APT28 hackers to attacks. In an October 2023 report, the threat group was also accused of breaching many critical networks of government entities, universities, research institutes, businesses, and think tanks in France since the second half of 2021.

Since it was first spotted more than 20 years ago, the Russian state-backed hacking group (also tracked as Strontium and Fancy Bear) was linked to GRU's Military Unit 26165 and is believed to have coordinated many high-profile cyberattacks.

APT28's list of previous victims includes the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) before the 2016 U.S. Presidential Election and the breach of the German Federal Parliament (Deutscher Bundestag) in 2015.

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

Last year, Poland said that APT28's military hackers had targeted multiple Polish government institutions in a large-scale phishing campaign.

The same week, NATO, the European Union, and international partners also formally condemned a long-term APT28 espionage campaign against multiple European countries, including Germany and the Czech Republic. The North Atlantic Council also warned at the time about "recent Russian hybrid activities," describing them as a "threat to Allied security."

According to NATO, these recent incidents include "sabotage, acts of violence, cyber and electronic interference, disinformation campaigns, and other hybrid operations" that have impacted Czechia, Estonia, Germany, Latvia, Lithuania, Poland, as well as the United Kingdom.

"Together with its partners, France is determined to use all the means at its disposal to anticipate, deter and respond to Russia's malicious behaviour in cyberspace where appropriate," the French foreign ministry added on Tuesday.

Source: https://www.bleepingcomputer.com/news/security/france-ties-russian-apt28-hackers-to-12-cyberattacks-on-french-orgs/