France warns of APT31 cyberspies targeting French organizations

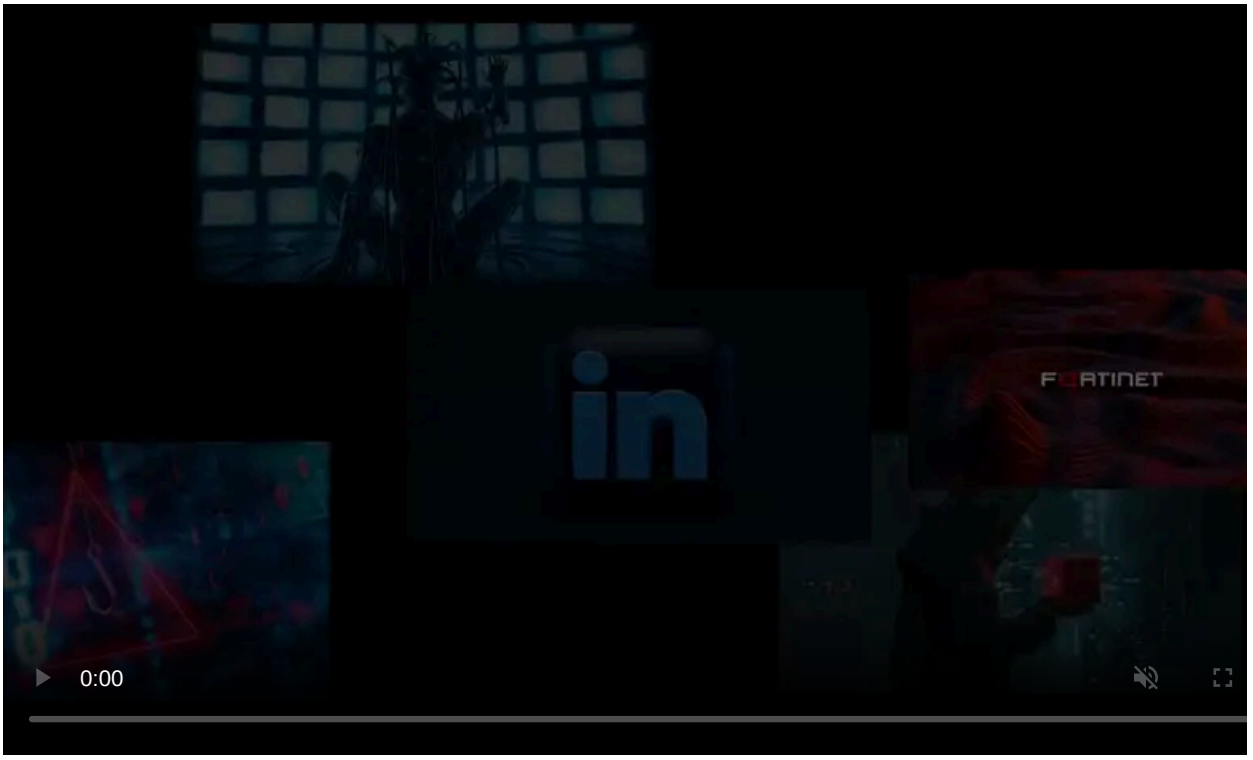
By Sergiu Gatlan

Published: 2021-07-21 · Archived: 2026-04-05 19:11:43 UTC

Today, the French national cyber-security agency warned of an ongoing series of attacks against a large number of French organizations coordinated by the Chinese-backed APT31 hacking group.

"It appears from our investigations that the threat actor uses a network of compromised home routers as operational relay boxes in order to perform stealth reconnaissance as well as attacks," ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) says in an alert bulletin issued today.

"As such, indicators of compromises (IOCs) are shared to help assess possible compromises (searches should start at the beginning of 2021) and used in detection services."


0:00

Organizations that detect any of the shared IOCs in their logs pointing at an attack potentially connected to this ongoing APT31 campaign are urged to report the incident to ANSSI via email.

APT31 (also known as Zirconium and Judgment Panda) is a hacking group working at the behest of the Chinese Government known for its numerous espionage and information theft operations.

This threat has been linked in the past to the theft and repurposing of the EpMe NSA exploit years before Shadow Brokers publicly leaked it in April 2017.

Last year, Microsoft observed APT31 attacks targeting the international affairs community and high-profile individuals associated with the Joe Biden presidential campaign.

APT31 was also spotted by Google while targeting "campaign staffers' personal emails with credential phishing emails and emails containing tracking links."

Chinese cyberespionage operations under the spotlight

These attacks come after the US and its allies, including the European Union, the United Kingdom, and NATO, have formally accused China of this year's Microsoft Exchange hacking campaign.

The cyberattacks took place in early 2021 and targeted more than a quarter of a million Microsoft Exchange servers, belonging to tens of thousands of organizations worldwide.

The Biden administration attributed "with a high degree of confidence that malicious cyber actors affiliated with PRC's MSS conducted cyber espionage operations utilizing the zero-day vulnerabilities in Microsoft Exchange Server disclosed in early March 2021."

The same day, the UK added that the Chinese Ministry of State Security (MSS) is behind Chinese state-backed hacking groups tracked as APT40 and APT31.

The NSA, CISA, and FBI also issued a joint advisory with more than 50 tactics, techniques, and procedures (TTPs) Chinese state-sponsored cyber actors have used in attacks against the US and allied networks.

Four Ministry of State Security intelligence officers believed to be part of the APT40 threat group were also charged on the same day by the Department of Justice regarding a multi-year campaign targeting governments and organizations from critical sectors worldwide.

Source: https://www.bleepingcomputer.com/news/security/france-warns-of-apt31-cyberspies-targeting-french-organizations/