France warns of Nobelium cyberspies attacking French orgs

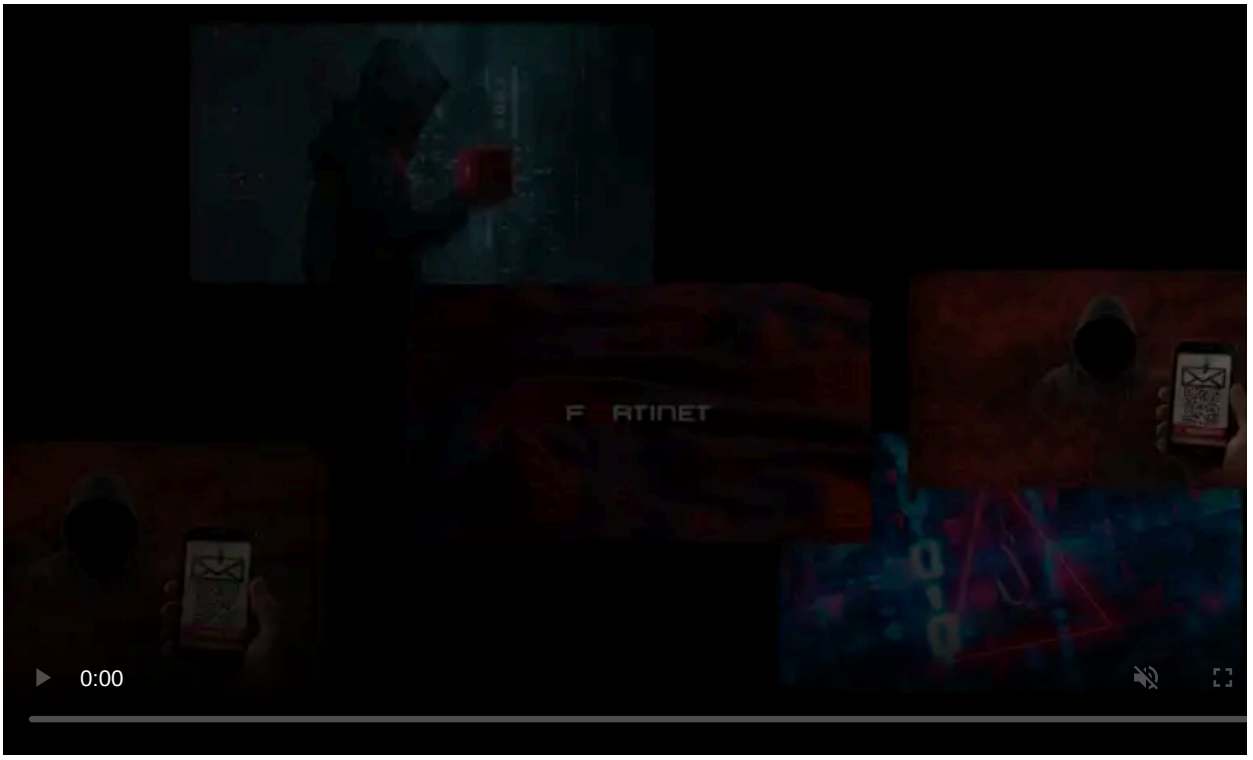
By Sergiu Gatlan

Published: 2021-12-06 · Archived: 2026-04-06 00:29:03 UTC

The French national cyber-security agency ANSSI said today that the Russian-backed Nobelium hacking group behind last year's SolarWinds hack has been targeting French organizations since February 2021.

While ANSSI (short for Agence Nationale de la Sécurité des Systèmes d'Information) has not determined how Nobelium compromised email accounts belonging to French orgs, it added that the hackers used them to deliver malicious emails targeting foreign institutions.

In turn, French public orgs were also the targets of spoofed emails sent from servers belonging to foreign entities, believed to be compromised by the same threat actor.


F RTINET
0:00

The infrastructure used by Nobelium in the attacks against French entities was mainly set up using virtual private servers (VPS) from different hosting companies (favoring servers from OVH and located close to the targeted countries).

"Overlaps have been identified in the tactics, techniques & procedures (TTP) between the phishing campaigns monitored by ANSSI and the SOLARWINDS supply chain attack in 2020," ANSSI explained in a report published today.

To defend against this hacking group's attacks, ANSSI recommends restricting the execution of email attachments to block malicious files delivered in phishing campaigns.

The French cyber-security agency also advises at-risk organizations to tighten Active Directory security (and AD servers in particular) using its Active Directory security hardening guide.

Nobelium and its high profile targets

Nobelium, the hacking group behind last year's SolarWinds supply-chain attack, which led to the breach of multiple US federal agencies, is the hacking division of the Russian Foreign Intelligence Service (SVR), also tracked as APT29, The Dukes, or Cozy Bear.

The US government formally accused the SVR division in April of orchestrating the "broad-scope cyber espionage campaign" that hit SolarWinds.

Cybersecurity firm Volexity also linked the attacks to the same threat actor based on tactics observed in incidents starting with 2018.

In May, the Microsoft Threat Intelligence Center (MSTIC) shared info on a Nobelium phishing campaign targeting government agencies from 24 countries worldwide.

As further reported by Microsoft in recent months, Nobelium is still targeting the global IT supply chain, having attacked 140 managed service providers (MSPs) and cloud service providers and breached at least 14 since May 2021.

Nobelium also targeted Active Directory Federation Services (AD FS) servers, attempting to compromise governments, think tanks, and private companies from the US and Europe using a new passive and highly targeted backdoor dubbed FoggyWeb.

Microsoft revealed in October that Nobelium was the most active Russian hacking group between July 2020 and June 2021, coordinating the attacks behind 92% of alerts Microsoft sent to customers regarding Russia-based threat activity.

Earlier today, Mandiant linked the hacking group to attempts to breach government and enterprise networks around the world by targeting their MSPs with a new backdoor dubbed Ceeloader designed to deploy further malware and harvest sensitive info of political interest to Russia.

Source: https://www.bleepingcomputer.com/news/security/france-warns-of-nobelium-cyberspies-attacking-french-orgs/