ANSSI warns of Russia-linked APT28 attacks on French entities

By Pierluigi Paganini

Published: 2023-10-27 · Archived: 2026-04-05 12:41:10 UTC

France National Agency for the Security of Information Systems warns that the Russia-linked APT28 group has breached several critical networks.

The French National Agency for the Security of Information Systems ANSSI (Agence Nationale de la sécurité des systèmes d'information) warns that the Russia-linked APT28 group has been targeting multiple French organizations, including government entities, businesses, universities, and research institutes and think tanks.

The French agency noticed that the threat actors used different techniques to avoid detection, including the compromise of low-risk equipment monitored and located at the edge of the target networks. The Government experts pointed out that in some cases the group did not deployed any backdoor in the compromised systems.

The report published by ANSSI is based on technical reports published in open source and elements collected during incident response operations carried out by the agency.

The document provides details about the tactics, techniques and procedures (TTP) associated with threar actors since the second half of 2021. The document also includes a series of recommendations to protect against this type of attack.

The APT28 group (aka Fancy Bear, Pawn Storm, Sofacy Group, Sednit, BlueDelta, and STRONTIUM) has been active since at least 2007 and it has targeted governments, militaries, and security organizations worldwide. The group was involved also in the string of attacks that targeted 2016 Presidential election.

The group operates out of military unity 26165 of the Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS).

Most of the APT28s' campaigns leveraged spear-phishing and malware-based attacks.

ANSSI observed at least three attack techniques employed by APT28 in the attacks against French organizations:

- searching for zero-day vulnerabilities [T1212, T1587.004];
- compromise of routers and personal email accounts [T1584.005, T1586.002];
- the use of open source tools and online services [T1588.002, T1583.006]. ANSSI investigations confirm that APT28 exploited the Outlook 0-day vulnerability CVE-2023-23397. According to other partners, over this period, the MOA also exploited other vulnerabilities, such as that affecting Microsoft Windows Support Diagnostic Tool (MSDT, CVE-2022-30190, also called Follina) as well as than those targeting the Roundcube application (CVE-2020-12641, CVE-2020-35730, CVE-2021-44026).

The attackers build and maintain part of their attack infrastructure by compromising routers and personal email accounts of individuals and businesses. APT28 used the compromised email accounts to send malicious emails and compromised routers to recover exfiltrated data.

Incident response investigations conducted by ANSSI confirmed the use of the Mimikatz and reGeorg tools by APT28, the former is a popular collector of sensitive information and the latter is a tunnel creation tool.

"In a campaign documented at the end of April 2023, APT28 operators distributed phishing emails instructing users to update their system by executing instructions in PowerShell language." reads the report. "These instructions downloaded and ran a script containing two commands:

- tasklist, which allows you to list all the processes currently running;
- systeminfo, which allows you to display detailed configuration information about a computer and its system operating. This information contains, for example, the list of installed security patches."

The script was hosted on "mocky[.]io," while the output of the commands was sent to "mockbin[.]org". Both MOCKY and MOCKBIN are public services used to generate web endpoints to test, track, and simulate an HTTP request or response. The experts believe that the attackers were using the command as part of a reconnaissance phase in an attempt to retrieve information about the target IT environment.

The command and control (C2) infrastructure used by the Russia-linked APT group relies on legitimate services to avoid detection.
The researchers noticed that APT28 hosted the Graphite and DriveOcean implants respectively on OneDrive and Google Drive services.

ANSSI recommends admins increase the level of cyber security of their networks by implementing additional defense measures.

Additional technical details about the attacks and the agency's recommendations are included in the report.

Follow me on Twitter: **@securityaffairs** and **Facebook** and **Mastodon**

Pierluigi Paganini

(SecurityAffairs – hacking, Russia)
