# France says Russian state hackers breached numerous critical networks

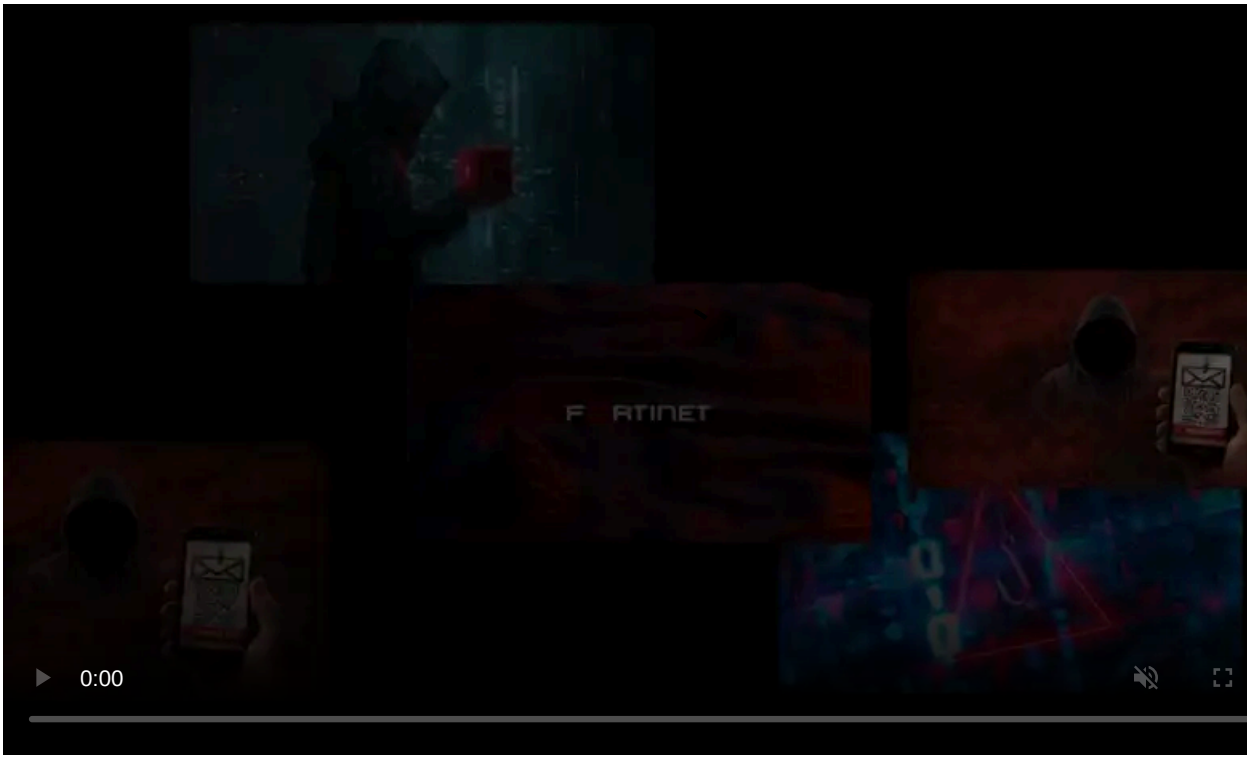
By Bill Toulas

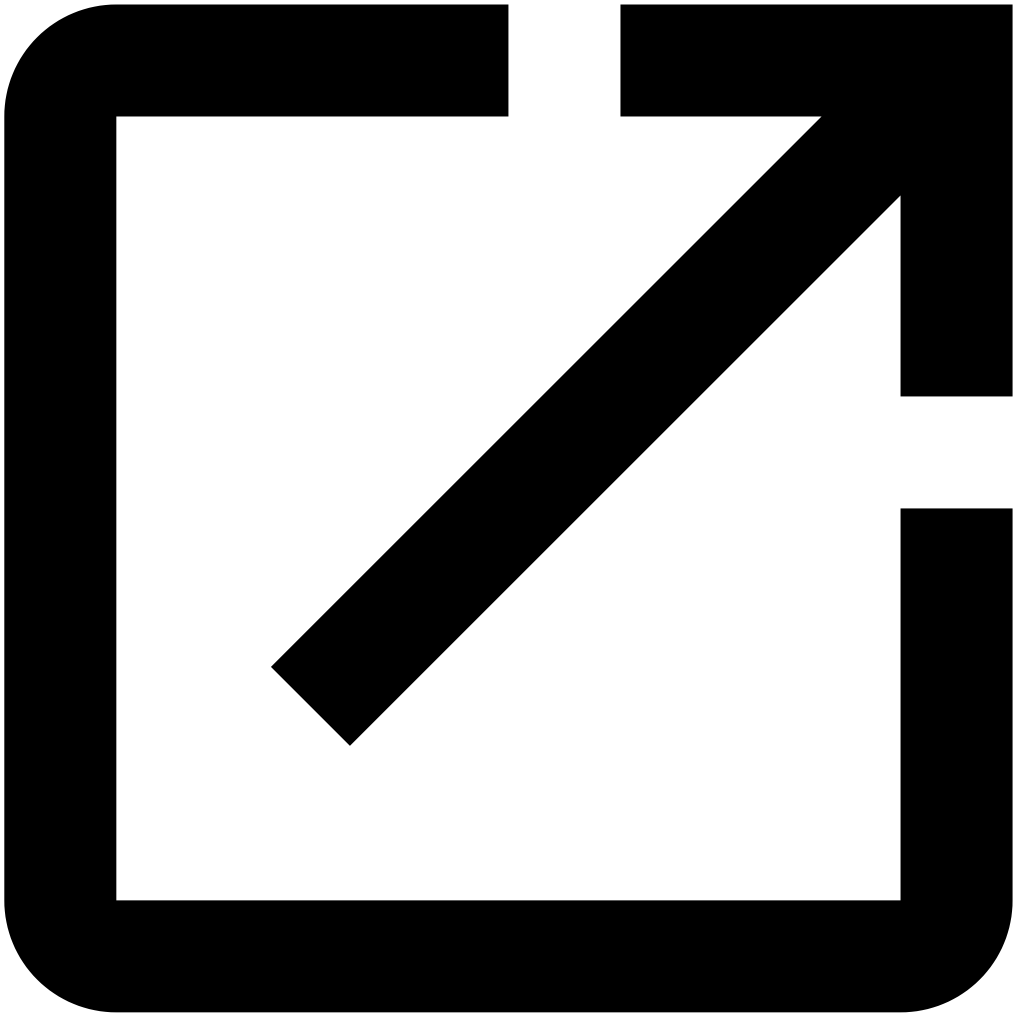
Published: 2023-10-26 · Archived: 2026-04-05 22:44:10 UTC

The Russian APT28 hacking group (aka 'Strontium' or 'Fancy Bear') has been targeting government entities, businesses, universities, research institutes, and think tanks in France since the second half of 2021.

The threat group, which is considered part of Russia's military intelligence service GRU, was recently linked to the exploitation of CVE-2023-38831, a remote code execution vulnerability in WinRAR, and CVE-2023-23397, a zero-day privilege elevation flaw in Microsoft Outlook.

The Russian hackers have been compromising peripheral devices on critical networks of French organizations and moving away from utilizing backdoors to evade detection.


F RTINET
0:00



This is according to a newly published report from ANSSI (Agence Nationale de la sécurité des systèmes d'information), the French National Agency for the Security of Information Systems, that conducted investigations on the activities of the cyber-espionage group.

## Network reconnaissance and initial access

ANSSI has mapped the TTPs (techniques, tactics, and procedures) of APT28, reporting that the threat group uses brute-forcing and leaked databases containing credentials to breach accounts and Ubiquiti routers on targeted networks.

In one case from April 2023, the attackers ran a phishing campaign that tricked the recipients into running PowerShell that exposed their system configuration, running processes, and other OS details.

Between March 2022 and June 2023, APT28 sent emails to Outlook users that exploited the then zero-day vulnerability now tracked as CVE-2023-23397, placing the initial exploitation a month earlier than what was recently reported.

During this period, the attackers also exploited CVE-2022-30190 (aka "Follina") in the Microsoft Windows Support Diagnostic Tool and CVE-2020-12641, CVE-2020-35730, CVE-2021-44026 in the Roundcube application.

The tools used in the first stages of the attacks include the Mimikatz password extractor and the reGeorg traffic relaying tool, as well as the Mockbin and Mocky open-source services.

ANSSI also reports that APT28 uses a range of VPN clients, including SurfShark, ExpressVPN, ProtonVPN, PureVPN, NordVPN, CactusVPN, WorldVPN, and VPNSecure.

| Émetteur | MD5 du fichier | Date d'envoi | URI | Routeur compromis |
|---|---|---|---|---|
| maint[@]goldenloafuae[.]com | 9f4172d554bb9056c8ba28e32c606b1e | 2022-03-18 | \\5.199.162.132\SCW | 5.199.162.132 |
| accounts[@]regencyservice[.]in | 3d4362e8fe86d2f33acb3e15f1dad341 | 2022-04-14 | \\101.255.119.42\event\2431 | 101.255.119.42 |
| vikram.anand[@]4ginfosource[.]com | f60350585fbfc5dc968f45c6ef4e434d | 2022-05-17 | \\101.255.119.42\mail\a5b3553d | 101.255.119.42 |
| *Inconnu* | 92e22b7e96aca3f9d733ca609ab0b589 | 2022-10-05 | *Inconnu* | 213.32.252.221 |
| franch1.lanka[@]bplanka[.]com | 43a0441b35b3db061cde412541f4d1e1 | 2022-10-25 | \\168.205.200.55\test | 168.205.200.55 |
| mdelafuente[@]ukwwfze[.]com | 9a97c56c9ea6d9ebde0968580ea28ea9 | 2022-10-25 | *Inconnu* | 213.32.252.221 |
| karina[@]bhpcapital[.]com | e68cbd4930e2781e0c1b19eb72ec0936 | 2022-10-26 | *Inconnu* | 213.32.252.221 |
| m.salim[@]tsc-me[.]com | b21dde4c19e2f6fc08a922e25de38cf5 | 2022-12-01 | \\185.132.17.160\aojv43 | 185.132.17.160 |
| ashoke.kumar[@]hbclife[.]in | b5d82be5813c7dacbd97ef5df073b260 | 2022-12-14 | \\69.51.2.106\report | 69.51.2.106 |
| jayan[@]wizzsolutions[.]com | 2bb4c6b32d077c0f80cda1006da90365 | 2022-12-29 | \\113.160.234.229\istanbul | 113.160.234.229 |
| m.yasser[@]egymatec[.]ae | 238334590d0f62d2a089bd87ad71b730 | 2023-03-15 | \\85.195.206.7\lrmng | 85.195.206.7 |
| commercial[@]vanadrink[.]com | 7ee19e6bd9f55ebc0dd6413c68346de6 | 2023-03-17 | \\85.195.206.7\power | 85.195.206.7 |
| commercial[@]vanadrink[.]com | 3b698278f225f1e5bace9d177a1a95e0 | 2023-03-21 | \\61.14.68.33\rem | 61.14.68.33 |
| *Inconnu* | ce65c51078b7c69a6f50b0b37a36293f | 2023-03-28 | \\24.142.165.2\req | 24.142.165.2 |
| m.nash[@]islandsailors[.]com | 65fdbc35bc8c3a2f0e872dbbfd32c7a7 | 2023-03-29 | \\42.98.5.225\ping | 42.98.5.225 |

**Addresses that disseminated emails exploiting CVE-2023-23397** *(ANSSI)*

## Data access and exfiltration

As a cyber-espionage group, data access and exfiltration are at the core of Strontium's operational goals.

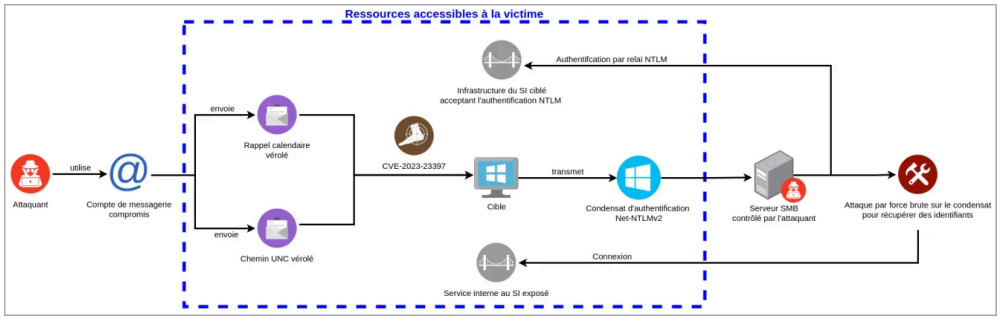
ANSSI has observed the threat actors retrieving authentication information using native utilities and stealing emails containing sensitive information and correspondence.

Specifically, the attackers exploit CVE-2023-23397 to trigger an SMB connection from the targeted accounts to a service under their control, allowing the retrieval of the NetNTLMv2 authentication hash, which can be used on other services, too.

APT28's command and control server (C2) infrastructure relies on legitimate cloud services, such as Microsoft OneDrive and Google Drive, to make the exchange less likely to raise any alarms by traffic monitoring tools.

Finally, ANSSI has seen evidence that the attackers collect data using the CredoMap implant, which targets information stored in the victim's web browser, such as authentication cookies.

Mockbin and the Pipedream service are also involved in the data exfiltration process.




**APT28 attack chain** *(ANSSI)*

## Defense recommendations

ANSSI emphasizes a comprehensive approach to security, which entails assessing risks. In the case of the APT28 threat, focusing on email security is crucial.

The agency's key recommendations around email security include:

- Ensure the security and confidentiality of email exchanges.
- Use secure exchange platforms to prevent email diversions or hijacks.
- Minimize the attack surface of webmail interfaces and reduce risks from servers like Microsoft Exchange.
- Implement capabilities to detect malicious emails.

For more details on ANSSI's findings and defense tips, check out the full report here.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

---