RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Date: April 29, 2025
Version: 1
Number of pages: 7

TARGETING AND COMPROMISE OF FRENCH ENTITIES USING THE APT28 INTRUSION SET

ACTIVITIES ASSOCIATED WITH APT28 SINCE 2021

TLP:CLEAR

Context

ANSSI, alongside its partners at the Cyber Crisis Coordination Centre (C4), has observed the targeting and compromise of French entities by the APT28 intrusion set. **Since 2021, this intrusion set has been used to gather strategic intelligence from entities located in France, Europe, Ukraine, and North America.** In the context of the war of aggression started by Russia against Ukraine on the 24th of February 2022, espionage campaigns associated with the APT28 intrusion set and targeting Ukraine, North Atlantic Treaty Organisation countries, or European Union member states have been observed.

The APT28 intrusion set

Active since at least 2004, the APT28 intrusion set[1] is publicly attributed to the Russian Federation [1]. This intrusion set is regularly used to target military and governmental organisations, as well as the defence, energy, and media sectors in Europe and the United States.

In the context of the war of aggression started by Russia against Ukraine on the 24th of February 2022, this intrusion set has frequently been used to carry out cyberattacks aimed at intelligence-gathering, against Ukrainian governmental and military entities, critical infrastructure, media or financial entities, local authorities, and individuals [2, 3, 4].

Recent espionage campaigns associated with APT28 have targeted governmental entities in European countries, including foreign affairs departments, political parties, foundations and associations, and entities from the sectors of defence, logistics, arms industry, aerospace, and IT [1, 5, 6, 7].

Infection chains and infrastructure

Drawing on public reports, infrastructure analyses and elements collected and analysed during incident response, the investigations conducted by ANSSI and its C4 partners led to the identification of several infection chains associated with the APT28 intrusion set and used for espionage purposes. C4 members are monitoring the evolution of the intrusion set's techniques, tactics and procedures (TTP), which have been adapted to new contexts without having been entirely renewed . The analyses of the TTPs used during APT28 campaigns since 2021 and the recommendations published in October of 2023 remain relevant and may be consulted on the website of the CERT-FR [2] [8].

At the beginning of the infection chain, operators of the APT28 intrusion set are conducting phishing campaigns, exploiting vulnerabilities – including the 0-day vulnerability CVE-2023-23397 – and carrying out brute-force attacks, notably against webmail [9]. ANSSI and its C4 partners analyses have furthermore revealed the compromise of generally poorly-supervised edge devices[3], intended to minimise the risks of detection.

Some campaigns – during which attackers might seek to gather strategic information (conversations, address books, login credentials) – are characterised by the absence of a specific mechanism intended to maintain persistent access to the concerned information systems [8]. In these specific cases, the primary objective of attackers may be to gain direct access to information of interest for espionage purposes.

[1] This intrusion set is also documented by security vendors as UAC-0028, Fancy Bear, FrozenLake, Sednit, Sofacy, or Pawn Storm.

[2] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf

[3] Routers, VPNs, e-mailing gateways and servers, firewalls, etc.

From the reconnaissance phase to the exfiltration of data, operators of the APT28 intrusion set heavily rely on low-cost and ready-to-use outsourced infrastructure. Such infrastructure may be made up of rented servers, free hosting services, VPN services, and temporary e-mail address creation services. The use of such services provides greater flexibility in the creation and administration of new resources, and enhances stealth. Indeed, a number of these services are also legitimately used by individuals and enterprises – which further complexifies the detection and monitoring of such infrastructure by security teams.

Notable campaigns

ANSSI and C4 members have, for instance, observed the use of the APT28 intrusion set in the repeated targeting of Roundcube e-mail servers, with the distribution of exploitation kits *via* phishing e-mails. These attacks aimed to exfiltrate the contents of e-mail accounts, and to identify new targets [10].

In 2023, APT28 operators also deployed an attack chain based on the use of free web services. These campaigns consisted in sending out phishing e-mails containing links redirecting users towards a domain provided by InfinityFree service, to deliver malicious ZIP archives containing the HeadLace backdoor. This backdoor relied on the distribution of commands from web endpoints of the Mocky.IO service. The commands distributed *via* Mocky.IO web endpoints aimed at gathering login credentials and information on the information system, and even to deploy offensive tools. In some cases, operators of the intrusion set attempted to establish a means of persistence by creating a scheduled task [11].

Additionally, between December 2023 and February of 2024, the CERT-UA documented the use by APT28 operators of an OceanMap stealer update[12]. Already observed in 2021 and 2022 by the security vendor Security Score Card [13], this malicious code relies on the IMAP protocol to exfiltrate the credentials stored on web browsers. This new version was reportedly deployed by using through the SteelHook and MasePie malicious codes .

Lastly, since the beginning of 2023, operators of the APT28 intrusion set have also been conducting phishing campaigns aimed at redirecting UKR.NET and Yahoo e-mail service users towards false login pages, with the intention of stealing their login details. In this context, the operators have once again used free web services such as Mocky.IO, compromised routers and, more recently, dynamic domain name resolution services to conceal their exfiltration servers. In order to broaden its targeting, this attack technique has, at times, been adapted to deploy false ZimbraMail or Outlook Web Access login pages [14].

Victimology

Since 2021, campaigns associated with the APT28 intrusion set have targeted or compromised[4] several French organisations including:

- Ministerial entities, local governments, and administrations;
- Entities of the DTIB[5] sector;
- Entities of the aerospace sector;
- Entities of the research sector and think-tanks;
- Entities of the economic and financial sector.

[4]The term “targeting” refers to cases of attempted but unsuccessful compromise.
[5]Defence Technological and Industrial Base.

In 2024, the victimology of the campaigns associated with the APT28 intrusion set primarily includes governmental, diplomatic, and research entities, as well as think-tanks. Some campaigns have notably been conducted against French governmental entities.

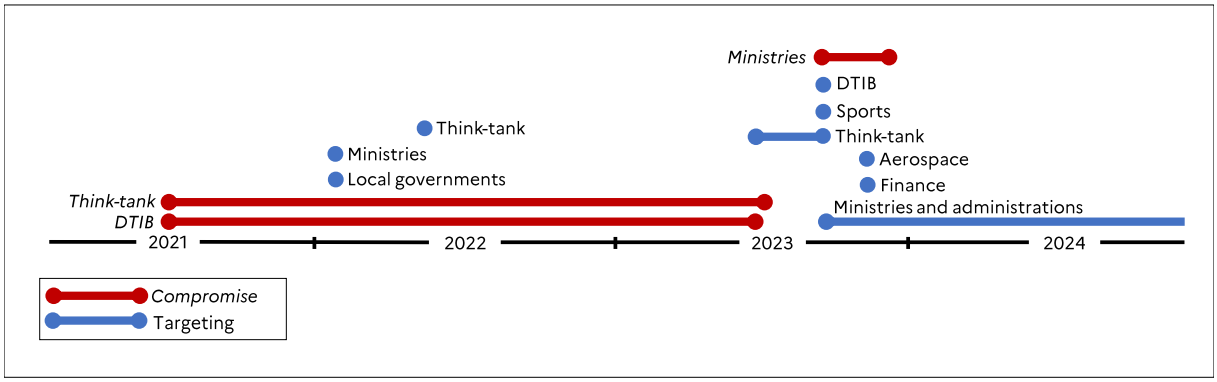

Figure 1: Targeting and compromise of French entities by operators of the APT28 intrusion set, since 2021

A References

[1] Conseil de l'Union européenne. *Cyber: Statement by the High Representative on behalf of the EU on continued malicious behaviour in cyberspace by the Russian Federation*. May 3, 2024.
URL: https://www.consilium.europa.eu/en/press/press-releases/2024/05/03/cyber-statement-by-the-high-representative-on-behalf-of-the-eu-on-continued-malicious-behaviour-in-cyberspace-by-the-russian-federation/.

[2] Microsoft. *Special Report : Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine*. April 27, 2022.
URL: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[3] CERT-UA. *Cyberattaque au moyen du MOA UAC-0001 (APT28) : utilisation d'une commande PowerShell dans le presse-papiers comme « point d'entrée » (CERT-UA11689)*. October 25, 2024.
URL: https://cert.gov.ua/article/6281123.

[4] Service d'État pour les communications spéciales et la protection de l'information de l'Ukraine. *The APT28 hacking group associated with russian special services attempts an attack on critical power infrastructure facility of Ukraine*. September 5, 2023.
URL: https://cip.gov.ua/en/news/khakerske-ugrupuvannya-art28-yake-pov-yazuyut-zi-specsluzhbami-rf-namagalosya-atakuvati-ob-yekt-kritichnoyi-energetichnoyi-infrastrukturi-ukrayini.

[5] CERT-PL. *APT28 campaign targeting Polish government institutions*. May 8, 2024.
URL: https://cert.pl/en/posts/2024/05/apt28-campaign/.

[6] Ministère tchèque des Affaires étrangères. *Statement of the MFA on the Cyberattacks Carried by Russian Actor APT28 on Czechia*. May 3, 2024.
URL: https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_of_the_mfa_on_the_cyberattacks.html.

[7] Ministère fédéral allemand de l'Intérieur. *Cyber attacks traced to Russian military intelligence agency*. May 3, 2024.
URL: https://www.bmi.bund.de/SharedDocs/kurzmeldungen/EN/2024/05/schutzmassnahmen-cyberangriffe-en.html.

[8] ANSSI. *Campagnes d'attaques du mode opératoire APT28 depuis 2021*. October 26, 2023.
URL: https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf.

[9] CERT-FR. *[MàJ] Vulnérabilité dans Microsoft Outlook*. May 11, 2023.
URL: https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-002/.

[10] Recorded Future. *BlueDelta Exploits Ukrainian Government Roundcube Mail Servers to Support Espionage Activities*. June 20, 2023.
URL: https://go.recordedfuture.com/hubfs/reports/cta-2023-0620.pdf.

[11] CERT-UA. *Attaque informatique par APT28 : msedge utilisé comme loader, TOR et les services mockbin.org / website.hook utilisés comme C2*. September 4, 2023.
URL: https://cert.gov.ua/article/5702579.

[12] CERT-UA. *APT28: From Initial Attack to Creating Threats to a Domain Controller in an Hour (CERT-UA#8399)*. December 29, 2023.
URL: https://cert.gov.ua/article/6276894.

[13] SecurityScorecard. *A Deep Dive Into the APT28's Stealer Called CredoMap*. September 28, 2022.
URL: https://securityscorecard.com/research/apt28s-stealer-called-credomap/.

[14] Sekoia. *APT28 Leverages Multiple Phishing Techniques to Target Ukrainian Civil Society*. May 5, 2023.
URL: https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/.

Version: 1 – April 29, 2025

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI – 51, boulevard de la Tour-Maubourg – 75700 PARIS 07 SP
cyber.gouv.fr • cert.ssi.gouv.fr