RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Date : 29 avril 2025
Version : 1
Nombre de pages : 7

CIBLAGE ET COMPROMISSION D'ENTITÉS FRANÇAISES AU MOYEN DU MODE OPÉRATOIRE D'ATTAQUE APT28

ACTIVITÉS ASSOCIÉES À APT28 DEPUIS 2021

TLP:CLEAR

Contexte

L'ANSSI et ses partenaires du Centre de Coordination des Crises Cyber (C4) ont observé le ciblage et la compromission d'entités françaises au moyen du mode opératoire d'attaque (MOA) APT28. **Depuis 2021, ce MOA a été mis en œuvre à des fins de collecte de renseignements stratégiques contre de nombreuses entités en France, en Europe, en Ukraine et en Amérique du Nord**. Les campagnes d'espionnage associées au MOA APT28 contre l'Ukraine et les pays de l'Organisation du traité de l'Atlantique nord et de l'Union européenne se poursuivent dans le contexte de la guerre d'agression déclenchée par la Russie contre l'Ukraine le 24 février 2022.

Le mode opératoire d'attaque APT28

Le MOA APT28[1], actif depuis au moins 2004, est attribué publiquement par l'Union Européenne à la Russie [1]. Ce MOA est régulièrement employé pour cibler des organisations gouvernementales et militaires, ainsi que les secteurs de la défense, de l'énergie et des médias, notamment en Europe et en Amérique du Nord.

Dans le contexte de la guerre d'agression déclenchée par la Russie contre l'Ukraine le 24 février 2022, ce MOA est régulièrement mis en oeuvre lors d'attaques informatiques à des fins de collecte de renseignement contre des entités ukrainiennes gouvernementales, militaires, des infrastructures critiques, des entités médiatiques et financières, des collectivités territoriales et des individus [2, 3, 4].

D'autre part, des campagnes récentes d'espionnage associées à APT28 ont ciblé des entités gouvernementales de pays européens, des partis politiques, des entités du secteur de la défense, de la logistique, de l'armement, de l'industrie aérospatiale, de l'informatique ainsi que des fondations et associations [1, 5, 6, 7].

Chaînes de compromission et infrastructure

Les investigations de l'ANSSI et de ses partenaires du Centre de coordination des crises cyber (C4)[2], s'appuyant notamment sur des rapports publics, des analyses d'infrastructures et des éléments collectés et analysés durant le traitement d'incidents, ont permis d'identifier plusieurs chaînes de compromission associées au MOA APT28 utilisées à des fins d'espionnage. Les membres du C4 suivent l'évolution des techniques, tactiques et procédures (TTP) du MOA, qui ont été adaptées à de nouveaux contextes sans être entièrement renouvelées depuis 2021. L'analyse des TTP employées lors des campagnes d'attaque du MOA APT28 depuis 2021 ainsi que des recommandations ont été publiées en octobre 2023 sur le site Internet du CERT-FR, et restent toujours d'actualité[3] [8].

Au début de la chaîne de compromission, les opérateurs du MOA APT28 conduisent ainsi des campagnes d'hameçonnage, d'attaques par force brute notamment contre des messageries *web (webmails)*, et d'exploitation de vulnérabilités y compris jour-zéro telle que la CVE-2023-23397[9]. Les investigations de l'ANSSI et de ses partenaires du C4 ont par ailleurs souligné la compromission d'équipements situés en bordure de systèmes d'information et généralement peu supervisés[4], afin de réduire les risques de détection.

1. Ce MOA est également documenté par les éditeurs de sécurité sous les noms de UAC-0028, Fancy Bear, FrozenLake, Sednit, Sofacy ou encore Pawn Storm.
2. Le C4 est une instance interministérielle traitant de l'analyse de la menace informatique. Le C4 rassemble l'ANSSI, le COMCYBER, la DGA, la DGSE et la DGSI.
3. https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf
4. Routeurs, VPN, passerelles et serveurs de messagerie, pare-feux, *etc.*

Certaines campagnes, lors desquelles les attaquants chercheraient à collecter des informations stratégiques (conversations, carnets d'adresses, authentifiants de connexion), sont notables par l'absence d'installation de mécanisme spécifique destiné à maintenir un accès persistant sur des systèmes d'information [8]. L'objectif premier des attaquants pourrait être dans ces cas spécifiques d'accéder directement à des informations d'intérêt à des fins d'espionnage.

Les opérateurs du MOA APT28 s'appuient de manière notable sur des infrastructures infogérées à moindre coût et prêtes à l'emploi, de la phase de reconnaissance à l'exfiltration de données. Ces infrastructures peuvent être composées de serveurs loués, de services d'hébergement gratuits, de services VPN et de services de création d'adresses de messagerie temporaires. L'utilisation de ces services offre une grande flexibilité dans la création et l'administration de nouvelles ressources et améliore la discrétion. En effet, nombre de ces services sont également utilisés de manière légitime par des particuliers ou des entreprises, rendant complexes la détection et le suivi de ces infrastructures par les équipes de sécurité.

Campagnes notables

L'ANSSI et ses partenaires du C4 ont par exemple observé l'utilisation du MOA APT28 pour cibler à de nombreuses reprises des serveurs de messagerie RoundCube, par la distribution de kits d'exploitation de vulnérabilités *via* des courriels d'hameçonnage. Ces attaques visaient à exfiltrer le contenu des comptes de messagerie et à identifier de nouvelles cibles [10].

Au cours de l'année 2023, les opérateurs du MOA ont également déployé une chaîne d'attaque s'appuyant sur l'utilisation de services *web* gratuits. Ces campagnes consistaient à envoyer des courriels d'hameçonnage contenant un lien de redirection vers un sous domaine fourni par le service InfinityFree pour délivrer des archives ZIP malveillantes contenant la porte dérobée HeadLace. Cette porte dérobée reposait sur la distribution de commandes depuis des points de terminaison *web* du service Mocky.io. Les commandes distribués par les points de terminaisons Mocky.io visaient à récupérer des informations sur le système d'information ainsi que des authentifiants de connexion, ou encore à déployer des outils offensifs. Dans certains cas, les opérateurs du MOA ont tenté d'établir des moyens de persistance en créant une tâche planifiée [11].

En outre, entre décembre 2023 et février 2024, le CERT ukrainien a documenté l'utilisation d'une mise à jour du *stealer* OceanMap par les opérateurs du MOA [12]. Ce code malveillant, déjà observé entre 2021 et 2022 par l'éditeur de sécurité Security Score Card [13], s'appuie sur le protocole IMAP pour exfiltrer les authentifiants stockés dans des navigateurs. Cette nouvelle version aurait été déployée grâce aux codes malveillants SteelHook et MasePie.

Enfin, depuis le début de l'année 2023, les opérateurs du MOA APT28 ont également conduit des campagnes d'hameçonnage visant à rediriger des utilisateurs des services de messagerie UKR.NET et Yahoo vers des fausses pages de connexion afin de voler leurs authentifiants. Dans le cadre de ces campagnes, les opérateurs du MOA ont à nouveau utilisé des services *web* gratuits comme Mocky.io, des routeurs compromis et plus récemment des services de résolution de noms de domaines dynamiques afin de dissimuler leurs serveurs d'exfiltration. Cette technique d'attaque a parfois été adaptée afin de déployer de fausses pages de connexion ZimbraMail ou Outlook Web Access afin d'élargir le ciblage [14].

Victimologie

Depuis 2021, des campagnes associées au MOA APT28 ont ciblé ou compromis[5] plusieurs organisations françaises parmi lesquelles :

- des entités ministérielles, des collectivités territoriales et des administrations ;
- des entités du secteur de la BITD[6] ;
- des entités du secteur de l'aérospatial ;
- des entités du secteur de la recherche et des groupes de réflexions (*think-tank*) ;
- des entités du secteur de l'économie et de la finance.

En 2024, la victimologie des campagnes associées au MOA APT28 comprend des entités appartenant majoritairement aux secteurs gouvernemental, diplomatique, et de la recherche ou des think tanks. Certaines campagnes ont notamment été dirigées contre des entités françaises du secteur gouvernemental.

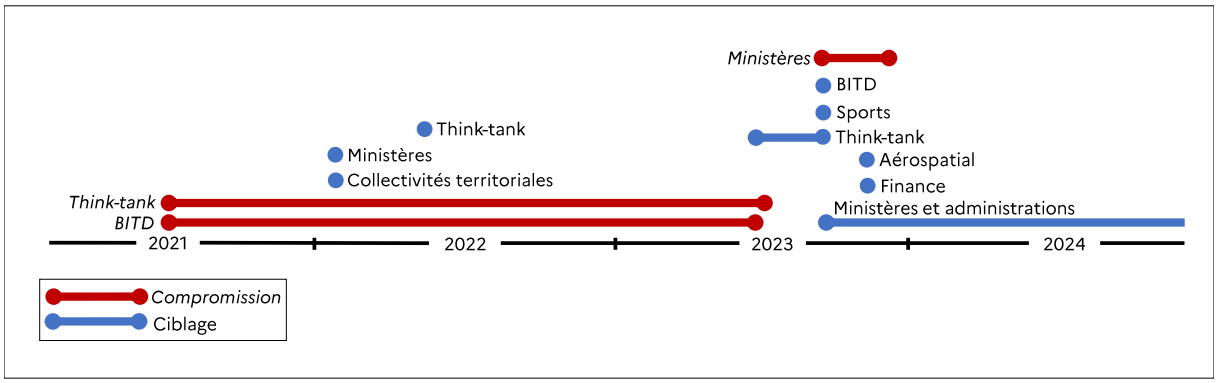

FIGURE 1 – Ciblage et compromission d'entités françaises depuis 2021 par les opérateurs du MOA APT28

5. Le terme ciblage renvoie à une tentative de compromission non aboutie.
6. Base industrielle et technologique de défense.

1 Références

[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*. 3 mai 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*. 27 avril 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)*. 25 octobre 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*. 5 septembre 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*. 8 mai 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*. 3 mai 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*. 3 mai 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*. 26 octobre 2023.
URL : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf.

[9] CERT-FR. *[MàJ] Vulnérabilité dans Microsoft Outlook*. 11 mai 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*. 20 juin 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*. 4 septembre 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)*. 29 décembre 2023.
URL : https://cert.gov.ua/article/6276894.

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

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

Version : 1 – 29 avril 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