yuno By xmco

BILAN DES ACTIVITÉS 2024

par le CERT-XMCO

Fort d'une trentaine d'experts, le CERT-XMCO analyse les menaces émergentes pour fournir des bulletins techniques et environnementaux à ses clients. Intégrée à Yuno, cette expertise vous aide à identifier les vulnérabilités critiques et les menaces en cours, tout en orientant vos priorités pour renforcer votre posture de sécurité et allouer efficacement vos ressources.

Cette production s'appuie sur la collecte et l'analyse de données issues de sources ouvertes et fermées, enrichies par le CERT-XMCO. La plateforme Yuno rend ces informations immédiatement exploitables : vous recevez des recommandations précises pour prioriser les correctifs et renforcer vos défenses face aux attaques. Avec Yuno, la veille devient un outil concret pour protéger durablement votre organisation.

Direction de la publication : XMCO
Conception : plusdebleu.com
Date de publication : Février 2025
Crédit photo : AdobeStock

Avant-propos

Pour cette seconde édition du bilan annuel YUNO, le CERT-XMCO revient sur les évènements marquants de l'année passée. L'objectif de ce document est de fournir une vision globale du paysage et de l'évolution des cybermenaces, par un travail de synthèse et d'analyse des informations collectées au quotidien par nos analystes.

EN 2024, LE SERVICE YUNO A AINSI ENVOYÉ À CHACUN DE SES CLIENTS :

5403

Bulletins techniques, de type :
- **PATCH** - Publication d'un correctif
- **VULN** - Découverte d'une vulnérabilité sans correctif
- **EXPLOIT** - Publication d'un code d'exploitation

Dont :

68
Bulletins critiques

+1600
Technologies suivies par Yuno

1005

Bulletins environnementaux de type **INFO**, relatifs à :
- Des attaques et campagnes d'attaques
- Des analyses de modes opératoires et de malware
- L'évolution des normes et du cadre réglementaire de la cybersécurité

Dont :

10
Bulletins critiques

+1000
Labels à suivre

316

Bulletins environnementaux de type **XMCO**, qui comprennent :
- **12** Observatoires des ransomware mensuels
- **52** Résumés de la semaine hebdomadaires
- **252** Revues de presse quotidiennes

Dont :

+130
Groupes ransomware suivis

Synthèse

Au cours de l'année 2024, le CERT-XMCO a identifié plusieurs tendances, structurantes ou émergentes, relatives aux activités des acteurs de la menace, ainsi qu'à leurs modes opératoires. Ce livrable vise à dresser un état des lieux des attaques observées ainsi que des vulnérabilités identifiées tout au long des douze derniers mois dans le cadre du service de veille Yuno.

DÉCOUVERTE ET EXPLOITATION DE VULNÉRABILITÉS

L'année 2024 a été marquée par l'exploitation de multiples vulnérabilités 0-day[1] et de failles récemment corrigées. Généralement exploitées par des modes opératoires sophistiqués, la divulgation rapide d'un PoC[2] a permis de faciliter leur exploitation, en particulier par des groupes criminels disposant de faibles ressources techniques.

Les produits visés restent majoritairement des solutions situées en périphérie de réseaux, à l'instar des pare-feu[3] et VPN[4] populaires tels que ceux fournis par Fortinet et Ivanti. La chaîne d'approvisionnement logicielle a également été largement ciblée car elle permet aux attaquants d'exploiter une plus grande surface d'attaque ainsi que d'étendre leurs opportunités de compromission, une tendance illustrée en 2024 par l'exploitation d'une vulnérabilité dans la bibliothèque XZ Utils ou au sein de la solution de gestion d'accès de BeyondTrust.

LES GROUPES RANSOMWARE

Les groupes ransomware ont continuellement amélioré leurs tactiques, techniques et procédures (TTPs)[5] via **l'exploitation de vulnérabilités de type 0-day, l'utilisation d'outils de contournement des solutions de sécurité mais aussi par la mise en place de schémas d'extorsion simplifiés**. Les forces de l'ordre ont intensifié leur lutte afin d'endiguer cette menace, principalement symbolisée par le démantèlement de l'infrastructure du groupe ransomware LockBit.

L'écosystème cybercriminel a toutefois su s'adapter à ces opérations, à l'instar du groupe Ransomhub, apparu en février 2024, qui a profité du démantèlement de LockBit et de la disparition volontaire du groupe ALPHV/BlackCat pour monter en puissance et s'imposer comme le nouveau ransomware le plus actif.

L'ÉCOSYSTÈME CYBERCRIMINEL

Au cours de l'année, les acteurs criminels se sont appuyés sur de **multiples plateformes de Phishing-as-a-Service (PaaS) ainsi que sur des outils diversifiés promus sur des forums criminels** pour faciliter leurs attaques et échapper plus efficacement à la détection. Par ces différents intermédiaires, ils ont pu compromettre de nombreuses entités notamment françaises telles que SFR, France Travail ou Cap Emploi.

La finalité reste le vol des données et leur revente sur les différentes marketplaces criminelles. À l'instar des groupes ransomware, les forces de l'ordre ont tenté de limiter la portée et la sophistication des acteurs criminels avec un succès difficilement mesurable, comme en témoigne l'opération policière Endgame, qui n'était pas parvenue à prévenir la résurgence de plusieurs des malware dont l'infrastructure avait été saisie à l'instar de IceID ou SmokeLoader.

LES MENACES APT (ADVANCED PERSISTENT THREAT)

Les modes opératoires parrainés par des États ont **poursuivi leurs activités d'influence, d'espionnage, voire de sabotage**, notamment sur des infrastructures critiques, à l'image de la compromission d'organismes de télécommunications commerciales américaines par des acteurs affiliés à la Chine.

Motivés par des objectifs politiques, économiques ou financiers, **certains groupes APT se sont appuyés sur des proxies criminels et sur des collectifs hacktivistes dans le but de dissimuler leur implication** dans les attaques qu'ils ont opérées. Cette tendance s'observe particulièrement au sein des modes opératoires parrainés par la Russie et l'Iran dans un contexte de guerre en Ukraine et de l'intensification des conflits au Moyen-Orient. Ces derniers ont régulièrement ciblé les États-Unis et l'Europe dans un contexte politique animé par des échéances électorales.

LES GROUPES HACKTIVISTES

Les collectifs hacktivistes se sont illustrés par des **attaques perturbatrices à faible impact afin de promouvoir leurs revendications politiques**. Dans certains cas, ils ont pu bénéficier d'un parrainage étatique qui est intervenu dans le choix des cibles ou la sophistication des attaques.

En raison de sa posture diplomatique et de l'accueil des Jeux Olympiques sur son sol, la France a été massivement ciblée, en particulier par des groupes pro-russes. Toutefois, **l'arrestation du fondateur de la messagerie chiffrée Telegram, Pavel DOUROV, est venue bouleverser l'écosystème hacktiviste** qui s'était structuré autour la plateforme. L'impact de cet événement est encore à mesurer, mais il est probable qu'il force les groupes à s'orienter vers d'autres plateformes de communications.

(1) Une vulnérabilité 0-day est une vulnérabilité qui est activement exploitée par des attaquants avant d'être découverte et corrigée par l'éditeur du logiciel ou du matériel affecté.
(2) Un PoC (Proof of Concept) est un code d'exploitation permettant d'exploiter une vulnérabilité sans nécessiter de connaissances techniques approfondies. Sa disponibilité augmente donc la probabilité qu'une vulnérabilité donnée soit exploitée massivement.
(3) Un pare-feu est un système de sécurité de réseau informatique qui limite le trafic Internet entrant, sortant ou à l'intérieur d'un réseau privé.
(4) Les réseaux privés virtuels permettent d'établir une connexion réseau protégée lors de l'utilisation de réseaux publics. Ils permettent de chiffrer le trafic Internet et anonymiser l'identité en ligne.
(5) https://attack.mitre.org/

Sommaire

yuno By xmco

1. INFORMATIONS DÉLIVRÉES EN 2024

1.1 Vulnérabilités massivement exploitées en 2024

L'exploitation de vulnérabilités logicielles reste l'un des principaux vecteurs d'attaques exploités par les groupes d'attaquants. Parmi l'ensemble des failles identifiées en 2024, le CERT-XMCO revient sur plusieurs d'entre elles qui ont particulièrement impacté l'écosystème de la cybersécurité, en raison de leur criticité, de leur exploitation massive et des compromissions qu'elles ont entraînées.

CVE-2023-46805
CVE-2024-21887
CVE-2024-21893
Affectant des produits Ivanti

Exploitées dès le 3 décembre 2023, ces vulnérabilités 0-day n'ont été divulguées par l'éditeur que le 10 janvier 2024. Référencées CVE-2023-46805 (CVSS3.1 de 8.2) et CVE-2024-21887 (CVSS3.1 de 9.1), elles affectaient les solutions Connect Secure et Policy Secure d'Ivanti et ont progressivement reçu des correctifs entre les mois de janvier et de juin 2024 en fonction des versions des produits affectés.

Ces deux vulnérabilités permettaient respectivement à un attaquant de contourner le processus d'authentification et d'injecter des commandes arbitraires via des requêtes spécifiquement conçues [1]. **Elles ont été exploitées dès le mois de décembre 2023 par le groupe APT UTA0178 lié à Chine** pour distribuer plusieurs malware personnalisés [2][3][4]. Le 16 janvier, un code d'exploitation a été rendu public pour la CVE-2023-46805, ce qui a accru leur exploitation, conduisant notamment à la compromission du MITRE mais également à la distribution de ransomware ainsi que de malware tels que le botnet Mirai[5][6][7].

Elles ont également été exploitées conjointement avec une autre vulnérabilité de contournement de sécurité affectant la solution Policy Secure, référencée CVE-2024-21893 et révélée le 31 janvier 2024 par Ivanti[8][9]. **Suite à la publication d'un PoC le 3 février, elle a été massivement exploitée** par des groupes APT sponsorisés par la Chine à des fins d'espionnage ainsi que par des groupes criminels à la recherche de gain financier[10][11].

Impacts :
- Espionnage via le déploiement de backdoors, webshell, loader, Remote Access Trojan (RAT) et botnets
- Déploiement de ransomware

CVE-2024-3400

Affectant GlobalProtect de Palo Alto

Révélée le 12 avril 2024, la vulnérabilité 0-day référencée CVE-2024-3400 (CVSS:3.1 de 10) affectait la solution de sécurité réseau pour Endpoints GlobalProtect de Palo Alto et a été corrigée par l'éditeur le 15 avril 2024[12].

Elle permettait à un attaquant distant et non authentifié d'exécuter du code arbitraire et a été exploitée comme 0-day par le mode opératoire APT UTA0218 associé à la Chine pour tenter de distribuer la backdoor Upstyle[13][14]. La publication de plusieurs codes d'exploitation le même mois que la publication d'un correctif a entrainé son exploitation massive par d'autres groupes APT également associés à la Chine à des fins d'espionnage ainsi qu'a l'Iran dans des opérations au cours desquelles ils ont collaboré avec des groupes ransomware tels que NoEscape, Ransomhouse et ALPHV/BlackCat[15][16][17].

Impacts :

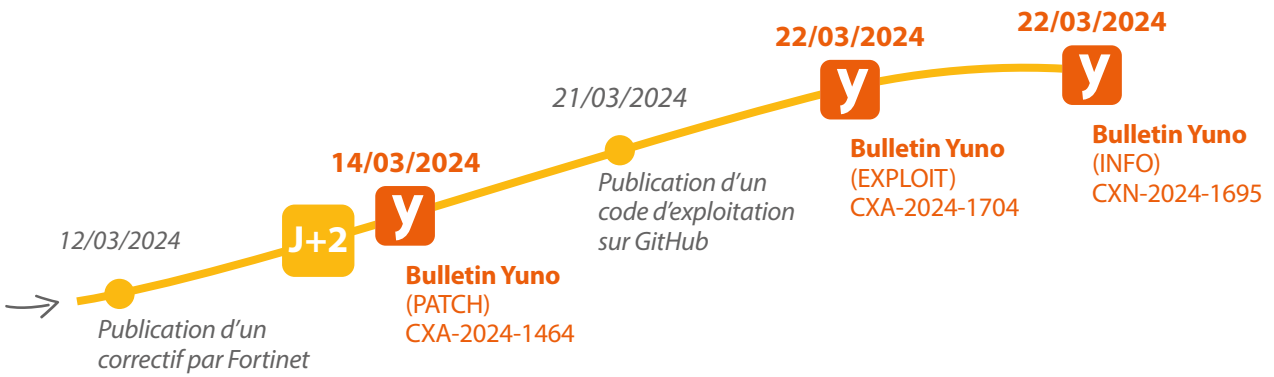
- Déploiement de ransomware
- Espionnage via déploiement de backdoors et de payloads Cobalt Strike

CVE-2023-48788

Affectant FortiClientEMS de Fortinet

Révélée le 12 mars 2024, la vulnérabilité référencée CVE-2023-48788 (CVSS:3.1 de 9.8) affectait la solution de gestion de sécurité pour Endpoints FortiClientEMS de Fortinet et a été corrigée par l'éditeur le 12 mars 2024[18].

La CVE-2023-48788, qui permettait à un attaquant distant non authentifié d'exécuter des injections SQL arbitraires et de prendre le contrôle du système via une requête spécialement conçue, **a été exploitée pour obtenir un accès initial par plusieurs groupes ransomware** dont RansomHub, MedusaLocker et Akira[19][20][21].



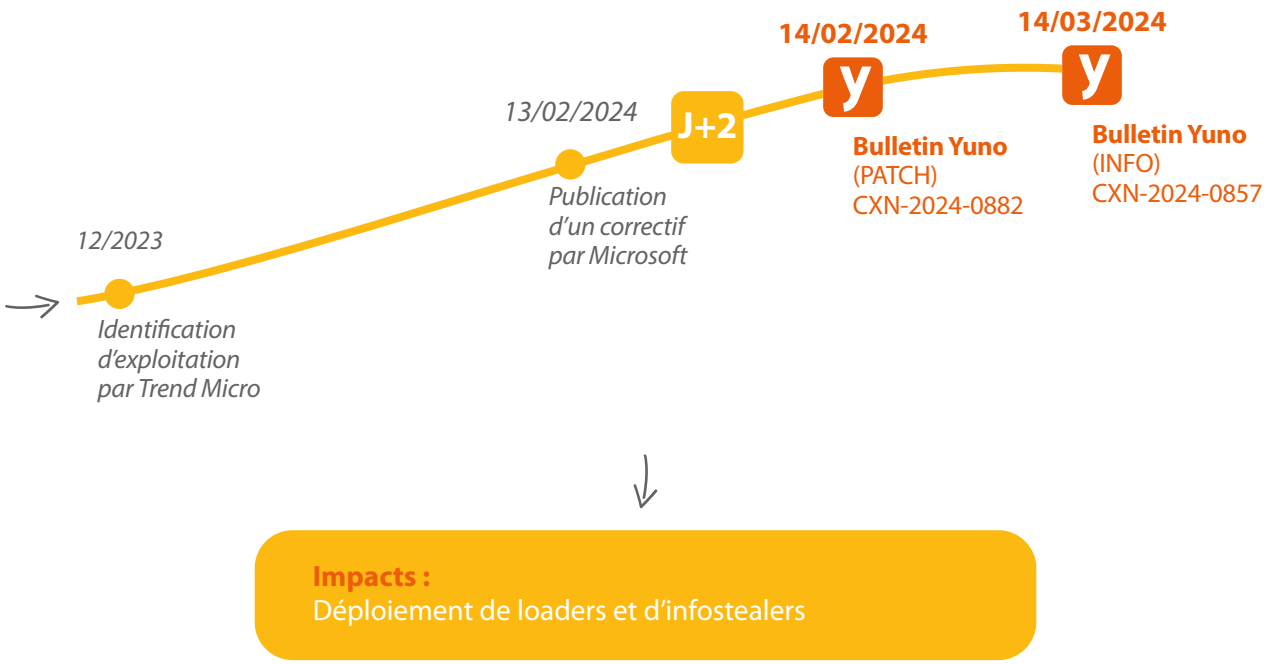
Impacts :
- Déploiement de ransomware

CVE-2024-21412

Affectant Microsoft Defender SmartScreen

Exploitée dès le mois de décembre 2023, elle a été révélée le 13 février 2024. La vulnérabilité 0-day référencée CVE-2024-21412 (CVSS:3.1 de 8.1) affectait Microsoft Defender SmartScreen et a été corrigée par l'éditeur le 13 février 2024. Elle permettait à un attaquant distant ayant incité sa victime à ouvrir un fichier spécifiquement conçu de contourner les contrôles de sécurité normalement affichés à l'utilisateur, et ainsi le rediriger vers un site arbitraire[22].

La vulnérabilité a été exploitée comme 0-day par le mode opératoire APT Water Hydra, par l'intermédiaire de campagnes de phishing pour distribuer les loaders DarkMe et potentiellement DarkGate[23][24]. **D'autres acteurs de la menace l'ont exploité après la publication du correctif** par l'intermédiaire de campagnes de phishing ciblant des pays occidentaux mais aussi la Thaïlande[25][26]. Les campagnes d'attaques avaient pour objectif la distribution d'infostealers notamment Lumma, Meduza et ACR Stealer.



1.2 Évènements marquants de 2024

YUNO COUVRE L'ESSENTIEL DE L'ACTUALITÉ DE L'ÉCOSYSTÈME CYBER À TRAVERS SES BULLETINS INFOS.

Chaque jour, nos clients reçoivent un concentré des évènements marquants du moment, qu'ils concernent des attaques et campagnes d'attaques, l'analyse de modes opératoires et de malware, ou encore des informations relatives à l'évolution du cadre réglementaire.

En 2024, les consultants du CERT-XMCO ont produit **1 005 bulletins environnementaux de type INFO**, dont vous retrouverez dans les pages suivantes, une courte sélection relatant des évènements notables.

Jeux Olympiques & Paralympiques Paris 2024

Une organisation marquée par la proactivité des hacktivistes

À l'occasion des Jeux Olympiques et Paralympiques (JOP) de Paris 2024, les équipes du CERT-XMCO ont établi un dispositif de surveillance renforcé dans l'objectif d'assurer une meilleure prévention et détection d'évènements susceptibles d'avoir un impact sur les activités de nos clients. Cette activité de veille quotidienne a ainsi permis d'identifier des campagnes d'attaques réalisées par divers attaquants cherchant à perturber l'événement pour des raisons idéologiques, financières ou géopolitiques[27].

DE NOMBREUSES ATTAQUES HACKTIVISTES AUX IMPACTS LIMITÉS

Le plus grand nombre d'incidents résultait d'attaques par déni de service distribué (DDoS), consistant à rendre indisponible le site Web de la cible par l'envoi d'un nombre important de requêtes simultanées. Elles ont été réalisées par des groupes hacktivistes à l'encontre d'organisations en lien avec l'événement sportif ou le pays hôte, et ont été guidées par une motivation idéologique qui consistait à protester contre la participation de l'Ukraine et d'Israël aux JO ainsi que contre la position diplomatique de la France relative aux conflits israélo-palestinien et russo-ukrainien.

Certains groupes ont également opéré des attaques avec un impact plus critique portant sur le vol de données, à l'instar de Lulzsec Muslims et Beregini, qui ont respectivement revendiqué le piratage d'un des sites Web liés à l'organisation des Jeux Olympiques et la compromission de documents confidentiels appartenant à l'Agence polonaise Anti-dopage (POLADA).

DES CAMPAGNES DE FRAUDES OPERÉES PAR DES CYBERCRIMINELS

Au niveau de l'écosystème cybercriminel, **les acteurs de la menace cherchant à réaliser des escroqueries sur le thème des Jeux Olympiques ont été les plus actifs**. Une seule attaque par ransomware a été revendiquée contre un lieu accueillant des rencontres sportives mais n'aurait engendré aucun impact opérationnel. Les cybercriminels ont principalement cherché à tirer profit des JOP via des campagnes de phishing prétendant vendre des billets pour les épreuves sportives. Des attaquants ont également développé une application se présentant comme un programme d'investissement Olympique officiel lié aux cryptomonnaies.

DES CAMPAGNES D'INFLUENCE ET DE DÉSINFORMATION SPONSORISÉES PAR DES ÉTATS

La majorité des attaques parrainées par des États proviennent de tentatives d'ingérences réalisées par des groupes associés à la Russie. Principalement opérées en amont de l'événement sportif, les campagnes Doppelgänger et Matriochka avaient pour objectif de discréditer la réputation du Comité International Olympique (CIO) sur la scène internationale et de produire du contenu sur les réseaux sociaux dénigrant l'événement sportif ou la France.

L'Azerbaïdjan a également cherché à déstabiliser la France et les JOP via une campagne visant la Nouvelle-Calédonie pendant les émeutes en mai 2024. En raison du soutien que la France a apporté

à l'Arménie suite au conflit de septembre 2023 autour du Haut-Karabagh, des utilisateurs associés à Bakou ont propagé des contenus trompeurs sur les réseaux sociaux en utilisant notamment le hashtag #BoycottParis2024.

CONCLUSION

Les menaces ayant ciblé les Jeux Olympiques et Paralympiques de Paris 2024 n'ont pas eu d'impact significatif sur le déroulement de l'événement. Les observations du CERT-XMCO concordent de ce fait avec les informations partagées par l'ANSSI, qui a indiqué avoir dénombré un total de 83 incidents affectant des entités en lien avec les JOP, dont la plupart consistaient en du DDoS.
Le reste provenait de tentatives de compromission ou de compromissions, de divulgations de données ou de signalements de vulnérabilités. Cette faible activité malveillante serait notamment due aux actions effectuées en matière de protection, de coopération, de coordination, mais aussi de prévention. En amont des jeux, l'ANSSI et Viginum avaient publié des guides, des marqueurs et des règles de détections permettant d'anticiper au mieux les potentielles attaques informatiques et informationnelles durant l'événement[28][29][30].

CHRONOLOGIE DES INCIDENTS DE SÉCURITÉ AYANT MARQUÉ LES JEUX OLYMPIQUES ET PARALYMPIQUES DE PARIS 2024

Date	Type	Description
17/05/2024	Désinformation	L'Azerbaïdjan mène une campagne de désinformation en Nouvelle-Calédonie.
02/06/2024	Désinformation	Le cluster *Doppelgänger* mène une campagne de désinformation.
07/06/2024	Désinformation	Le cluster *Matrioshka* mène une campagne de désinformation.
10/06/2024	Fraude	Campagne de fraude «Ticket Heist» visant les utilisateurs russophones souhaitant acheter des billets pour les JO de Paris 2024.
13/06/2024	Fraude	Campagne de malvertising et de phishing redirigeant ves un site frauduleux vendant de faux billets pour les JO de Paris 2024.
23/06/2024	DDoS	Attaque DDoS par HackNet visant le grand Palais de Paris.
25/07/2024	Désinformation	Le cluster *Doppelgänger* mène une campagne de désinformation.
25/07/2024	Fraude	Fraude à la promotion de faux forfaits 4G utilisant l'image des JO de Paris 2024.
26/07/2024		**Cérémonie d'ouverture des JO de Paris 2024.**
27/07/2024	Fraude	Campagne de phishing utilisant l'IA pour générer de faux sites de cryptomonnaies sur le thème des JO de Paris 2024.
29/07/2024	DDoS	Cyber Army of Russia Reborn vise des entreprises liées aux JO de Paris 2024, telles que : Fnac Darty, ArcelorMittal, Aquatic Show, ArenaGroup (…).
29/07/2024	Leak	L'utilisateur Zeus divulgue des données personnelles d'athlètes israéliens.
29/07/2024	DDoS	Keymous + cible le Conseil olympique israélien.
29/07/2024	DDoS	Hacker Council Global cible le site web de la Fédération ukrainienne de football.
29/07/2024	DDoS	NetForceZ cible plusieurs villes françaises.
30/07/2024	Fraude	Des applications malveillantes promouvant des cryptomonnaies frauduleuses utilisant l'image des JO de Paris 2024 ont été identifiées.
30/07/2024	DDoS	Le collectif Anonymous cible l'association israélienne d'athlétisme.
31/07/2024	Leak	LulzSec Muslims revendique une fuite de données à l'encontre du Comité olympique.
05/08/2024	DDoS	SN Blackmeta revendique une attaque DDoS contre LaPoste, partenaire des JO de Paris 2024.
07/08/2024	Leak	Le groupe hacktiviste Beregini publie des documents médicaux d'athlètes polonais.
27/08/2024	Leak	7lef compromet une base de données de la fédération espagnole de handball sur BreachForums.
29/08/2024	Leak	7lef divulgue une base de données de la Fédération espagnole d'athlétisme sur BreachForums.
29/08/2024	Ransomware	Le groupe de ransomware Brain Cipher affirme avoir compromis la Réunion des musées nationaux - Grand Palais
08/09/2024		**Cérémonie de clôture des JO de Paris 2024.**

Publication des données de nombreuses entités françaises

sur le forum cybercriminel BreachForums

Tout au long de l'année 2024, les consultants du CERT-XMCO ont assuré une veille sur les principaux forums cybercriminels russophones, anglophones et francophones. Ces plateformes se sont révélées être de véritables places marchandes, facilitant la vente d'accès initiaux et de bases de données pouvant être exploitées dans le cadre d'attaques ultérieures.

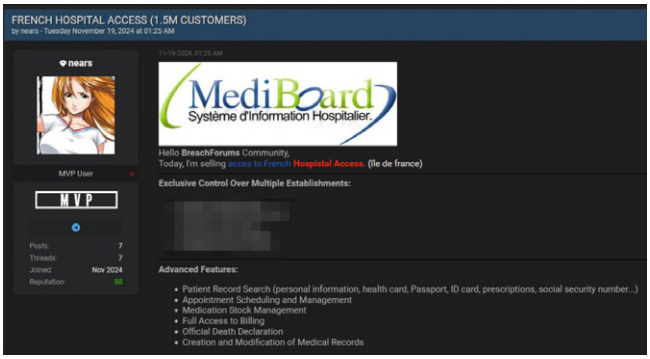
L'OMNIPRÉSENCE DE BREACHFORUMS DANS LE PAYSAGE DE LA MENACE CYBER

Parmi ces forums, **BreachForums a maintenu une position majeure au sein de la communauté cybercriminelle, malgré de nombreuses tentatives des forces de l'ordre pour le démanteler**. La plus récente est survenue à la suite de la publication sur le forum de plusieurs ensemble de données sensibles, en particulier celles dérobées à Europol par le cybercriminel IntelBroker, lorsque le FBI a saisi le domaine de BreachForums le 15 mai 2024[31].

S'en est suivi un bras de fer entre les forces de l'ordre et les administrateurs du forum qui sont parvenus à reprendre le contrôle du site. Depuis lors, BreachForums a été le théâtre de la publication de données appartenant à de nombreuses entreprises françaises, avec un pic d'activité observé au mois de **novembre 2024, au cours duquel le CERT-XMCO a recensé neuf revendications d'attaques contre des entreprises françaises**, sept d'entre elles ayant été revendiquées par le même groupe cybercriminel nommé Nears.

NEARS : UN ACTEUR CRIMINEL PROLIFIQUE EN 2024

Utilisant le pseudonyme near2tlg sur BreachForums ou Near Database sur Telegram, il s'agirait d'un groupe plutôt que d'un individu isolé. **D'origine francophone, il ciblerait spécifiquement des entreprises et institutions françaises**, parmi lesquelles figurent la Banque de France, Le Point, SFR ou encore les logiciels Mediboard et Osiris[32][33].



Nears revendique la compromission de MediBoard sur BreachForums

La vente de ces bases de données a entraîné la diffusion d'informations personnelles sensibles (nom, prénom, e-mail, téléphone, IBAN), qui peuvent être exploitées dans des attaques de phishing ciblé (spear-phishing) ultérieures. Par leur intermédiaire, des cybercriminels pourraient usurper l'identité des entreprises compromises et exploiter les données exposées pour renforcer la crédibilité de leurs attaques. Ces fraudes pourraient également entraîner des pertes financières pour les clients et les entreprises, ainsi qu'une dégradation de leur image de marque.

Les attaques de Nears semblent opportunistes et guidées par des objectifs financiers plutôt que pour promouvoir une revendication politique. L'accès aux données a été constamment vendu pour plusieurs centaines d'euros, un prix bas permettant d'attirer les potentiels acheteurs et ainsi de maximiser ses profits.

Toutes les attaques de Nears ont eu lieu en novembre 2024 et le groupe semble désormais inactif, son canal Telegram et son compte Breach Forums ayant été supprimés. Juste avant sa disparition, Nears avait affirmé que la SNCF serait sa prochaine cible, mais rien n'indique qu'elle ait été réellement compromise depuis lors.

Il reste envisageable que Nears réapparaisse à l'avenir, sous le même pseudonyme ou sous une nouvelle identité numérique. Du fait de son activité intense sur cette courte période, il est probable que le groupe ait souhaité rester discret et protéger ses membres de potentielles opérations des forces de l'ordre.

1.2.3 ÉVÈNEMENTS MARQUANTS DE 2024

La chute du Ransomware-as-a-Service (RaaS) LockBit

et la montée en puissance de RansomHub

Les équipes du CERT-XMCO assurent quotidiennement le suivi des attaques revendiquées par plus de 130 groupes ransomware. Cette activité de veille a permis de mettre en lumière les grandes tendances de cet écosystème cybercriminel qui a connu des évolutions majeures en 2024.

LE DÉMANTÈLEMENT DE L'OPÉRATION LOCKBIT

En février 2024, **une opération policière internationale nommée Opération Cronos** a conduit à l'arrestation de plusieurs membres, à la publication d'un outil de déchiffrement ainsi qu'à la saisie d'une partie importante de l'infrastructure et des ressources du groupe LockBit, qui figurait jusqu'alors parmi les groupes ransomware les plus actifs[34][35]. Au-delà des conséquences financières, **cette opération a porté un coup majeur à la crédibilité et aux moyens de ce groupe** ayant marqué le paysage de la menace depuis 2020[36][37][38][39]. Elle s'inscrit également dans une dynamique plus large d'intensification de la lutte contre l'écosystème ransomware, illustrée par le démantèlement du groupe ALPHV/BlackCat par le département de la justice américain en décembre 2023[40][41].

L'ÉMERGENCE DE RANSOMHUB

C'est dans ce contexte que **les opérateurs d'une nouvelle opération ransomware baptisée RansomHub ont pu recruter de nouveaux affiliés**, à l'instar du groupe Scattered Spider, anciennement associé à ALPHV/BlackCat, et CosmicBeetle au sein de leur programme de RaaS[42][43]. Ces derniers auraient notamment été attirés par les promesses d'une répartition avantageuse des rançons payées par les victimes.

Actif depuis le mois de février 2024, le groupe RansomHub s'est rapidement imposé dans l'écosystème cybercriminel, prenant la relève de LockBit avec la revendication de **569 entités compromises, dont 12 organismes français**, sur son site vitrine en 2024[44].

Dès le mois de juillet 2024, il devenait le groupe ransomware le plus actif, dépassant pour la première fois LockBit et en novembre 2024, il revendiquait plus d'une centaine de victimes à l'international[45].

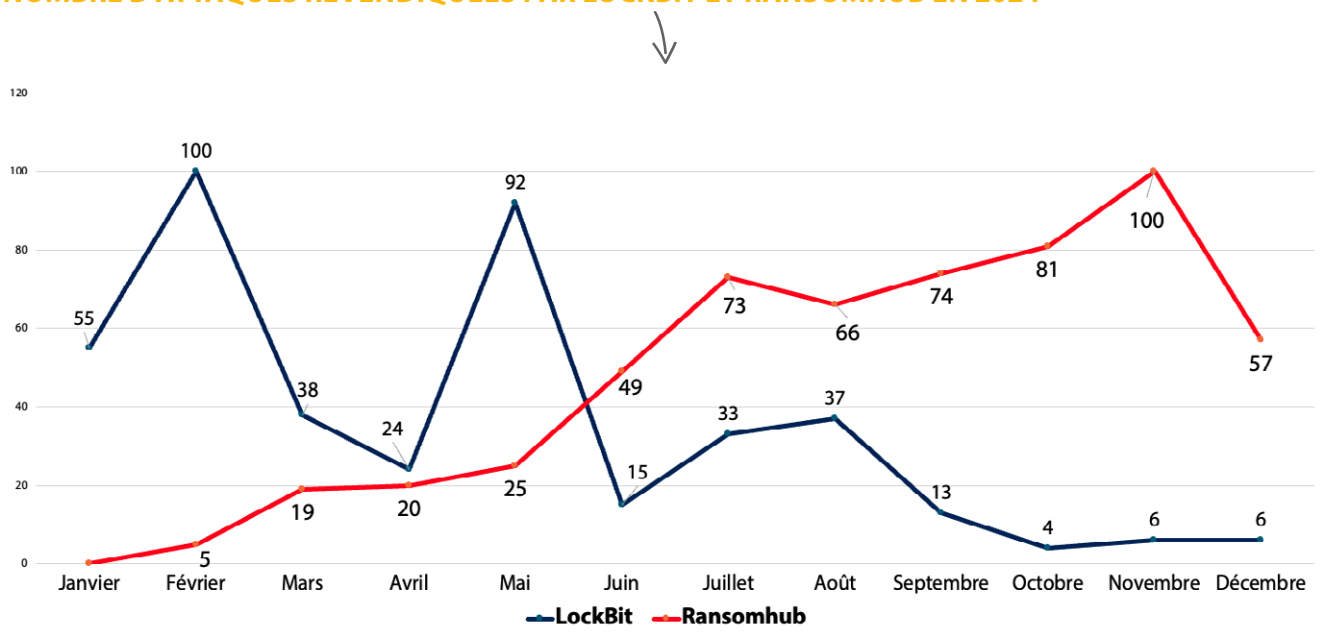
RansomHub s'impose ainsi comme une des principales menaces de l'écosystème ransomware et est susceptible de le rester une 2025. Ce dernier se démarque en outre par un certain degré de sophistication par l'exploitation de nombreuses vulnérabilités, le développement d'un chiffreur multiplateforme, ou encore par le recours à divers outils qui lui permettent d'échapper à la détection lors de ses tentatives d'intrusion.

L'EFFACEMENT PROGRESSIF DE LOCKBIT

Dans les mois qui suivirent son démantèlement, **le groupe LockBit a continué de revendiquer des victimes** mais un nombre croissant d'entre elles n'avaient pas réellement été compromises ou avaient déjà été revendiquées auparavant par d'autres groupes ransomware. Il est probable que ces fausses revendications aient été un moyen pour LockBit de gonfler artificiellement le nombre de victimes du groupe afin de maintenir une impression d'efficacité et de succès de ses opérations.

Il poursuit néanmoins ses activités malveillantes, illustrées par la publication d'une quatrième version de son programme de RaaS publié au début du mois de décembre 2024, démontrant ainsi sa forte capacité de résilience[46]. L'arrestation le 29 novembre 2024 d'un de ses administrateurs par les forces de l'ordre russes pourrait cependant présager de l'arrêt définitif de cette opération ransomware[39].

NOMBRE D'ATTAQUES REVENDIQUÉES PAR LOCKBIT ET RANSOMHUB EN 2024



1.3 Observatoire des ransomware 2024

DANS LE CADRE DE SON SERVICE YUNO, LE CERT-XMCO PROPOSE CHAQUE MOIS UN ÉTAT DE LA MENACE RANSOMWARE.
IL SOULIGNE LES PRINCIPAUX ÉVÈNEMENTS RELATIFS À CET ÉCOSYSTÈME CYBERCRIMINEL ET PRÉSENTE LES GROUPES D'ATTAQUANTS LES PLUS ACTIFS, LA TYPOLOGIE DES VICTIMES AINSI QUE L'ÉVOLUTION DES MODES OPÉRATOIRES OBSERVÉS.

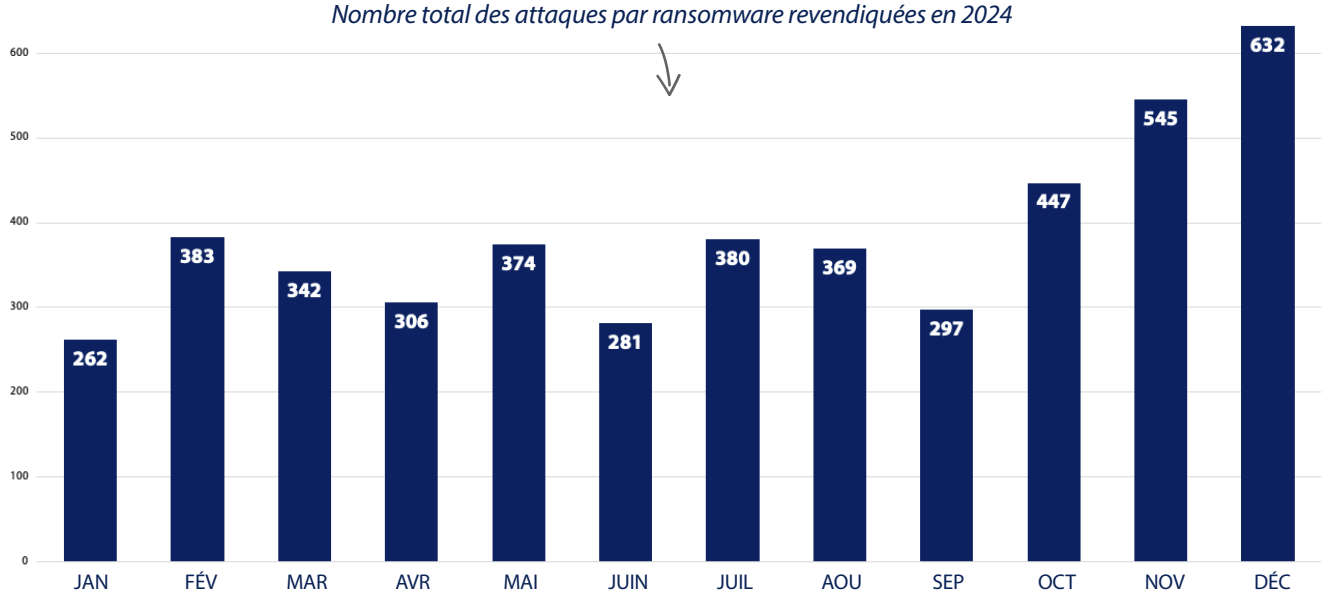
Cette production du CERT-XMCO s'appuie sur la collecte et l'analyse de données issues de sources ouvertes effectuées quotidiennement, qui permettent de dépeindre les évolutions de cet écosystème sur l'ensemble de l'année 2024. Le nombre de victimes peut néanmoins s'avérer non exhaustif car il est basé sur les compromissions revendiquées par les groupes ransomware eux-mêmes.

Tendances relatives aux attaques ransomware à l'international

Au cours de l'année 2024, les consultants du CERT-XMCO ont identifié **la compromission de 4 618 entités** à l'international par plus d'une cinquantaine de groupes criminels disposant d'un site vitrine de revendication. Malgré les opérations policières internationales de lutte contre la cybercriminalité organisée, ces groupes criminels ont poursuivi leurs activités malveillantes en 2024[47][48][49].

L'essentiel d'entre eux est resté concentré sur la poursuite d'objectifs financiers avec une victimologie géographiquement homogène, **ciblant principalement des entités localisées en Amérique du Nord et en Europe de l'Ouest**. RansomHub se démarque comme le programme de RaaS ayant revendiqué le plus d'attaques en 2024, suivi par LockBit et Play.

Nombre total des attaques par ransomware revendiquées en 2024



Répartition des attaques en Europe par ransomware en 2024

Répartition géographique des attaques par ransomware en 2024

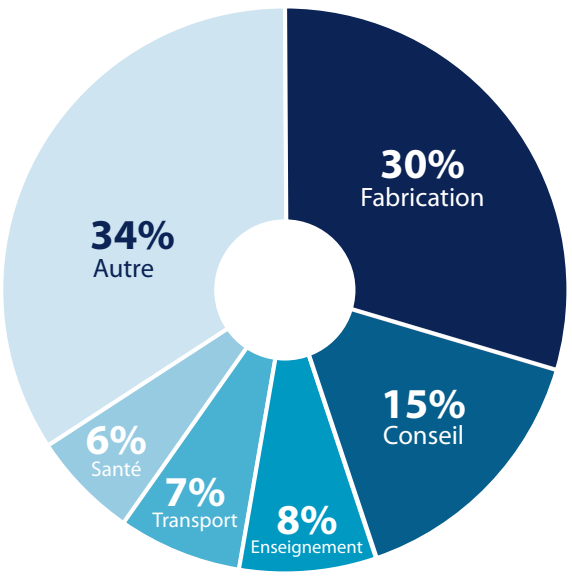
Répartition sectorielle et géographique
des attaques ransomware en 2024

Sur l'ensemble de l'année 2024, **les États-Unis sont restés le pays le plus ciblé** par les groupes ransomware avec la revendication de **2 266 victimes** par plus d'une cinquantaine de groupes criminels. Les compromissions de Blue Yonder par Termite et de l'aéroport de Seattle par Rhysida figurent parmi les plus significatives de 2024[50][51].

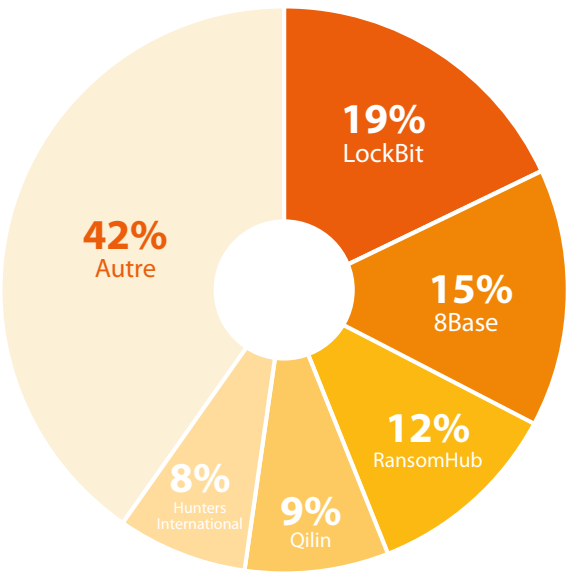
En France, 112 attaques ont été recensées et **les secteurs d'activités les plus ciblés sont ceux du conseil, de l'enseignement et de la santé**, illustré par la compromission de l'hôpital de Cannes par LockBit et de celle du Centre Hospitalier d'Armentières par le ransomware Blackout[52][53].

Malgré le démantèlement de son infrastructure via l'opération policière Cronos, **c'est LockBit qui est resté le groupe ransomware le plus prolifique en France**, suivi ensuite des opérateurs de 8Base et de RansomHub[34].

Répartition sectorielle des attaques en France en 2024



Nombre de revendications d'attaques en France par les groupes de ransomware



Chronologie des attaques par ransomware
les plus marquantes en France

Compromission de Schneider Electric par les groupes ransomware Cactus et Hellcat

DATE : 29/01/2024
SOURCES : **Bulletin CXN-2024-0551**[54] **/ Bulletin CXN-2024-1004**[55] **/ Bulletin CXN-2024-6294**[56]

La division chargée du développement durable de **Schneider Electric a annoncé avoir été victime d'une cyberattaque par ransomware revendiquée le 19 février par Cactus**. Selon l'entreprise, la compromission s'est limitée à sa division chargée du développement durable et les autres entités de la firme n'étaient pas affectées. L'analyse des échantillons des données volées a notamment révélé des passeports d'employés ainsi que des documents internes à l'entreprise.

Schneider Electric a été compromise une seconde fois durant l'année par le groupe criminel Hellcat. Le 2 novembre 2024, ce dernier a revendiqué la compromission de 40 GB de données liées à la multinationale française. D'après les informations publiées sur son site vitrine, le groupe aurait accédé au serveur Jira Atlassian de Schneider Electric, permettant d'exfiltrer des données sensibles, incluant plus de 400 000 lignes de données utilisateur.

Attaque contre le Centre Hospitalier d'Armentières par le ransomware Blackout

DATE : 27/02/2024
SOURCE : **Bulletin CXN-2024-1177**[53]

Le groupe Blackout a revendiqué la compromission d'un centre hospitalier d'envergure nationale. Le groupe aurait chiffré plus de 100 serveurs et postes de travail. Comme preuve de l'attaque, les acteurs de la menace ont publié une base de données médicales relatives à plus de 900 000 patients.

Le groupe ransomware Hunters International revendique la compromission d'Intersport

DATE : 03/04/2024
SOURCE : **Bulletin CXN-2024-1941**[59]

Le groupe de ransomware **Hunters International a revendiqué la compromission d'Intersport** et l'exfiltration de plus de 400 GB de données qui comprendraient notamment des informations personnelles d'employés et de clients. Le ransomware **Hunters International présente néanmoins de fortes similitudes avec le ransomware Hive, qui avait déjà revendiqué la compromission** du groupe français en décembre 2022[57][58]. Il est donc probable que cette nouvelle revendication ne soit en réalité qu'une récupération de cette première compromission.

Revendication de la compromission de la Réunion des musées nationaux - Grand Palais par le groupe ransomware Brain Cipher

DATE : 06/08/2024
SOURCES : **Bulletin CXN-2024-4936**[60] **/ Bulletin CXN-2024-4491**[61]

La Réunion des musées nationaux - Grand Palais a annoncé avoir fait l'objet d'une cyberattaque **revendiquée le 29 août par le groupe ransomware Brain Cipher**. Cette attaque qui a eu lieu durant les Jeux Olympiques n'a eu aucun impact opérationnel sur le déroulement des épreuves dans le grand Palais mais aurait permis de voler de plus de 300 GB de données.

Chiffrement d'un térabit de données de l'université Paris-Saclay par RansomHouse

DATE : 12/08/2024
SOURCES : **Bulletin CXN-2024-4580**[62] **/ Bulletin CXN-2024-5764**[63]

L'Université Paris-Saclay a annoncé avoir été victime d'une cyberattaque par ransomware qui a été **revendiquée le 9 octobre par RansomHouse**. Plus d'un térabit de données aurait été chiffré par les opérateurs du groupe ransomware. La nature des données traitées par cet établissement de recherche et d'enseignement aurait pu inciter d'autres acteurs malveillants à télécharger les données compromises pour mener des attaques ultérieures.

Compromission du groupe Althays par Qilin

DATE : 01/11/2024
SOURCE : **BULLETIN CXN-2024-6284**[64]

Le groupe ransomware Qilin a revendiqué la compromission d'une firme française, spécialisée dans la fourniture de logiciels de paie, de comptabilité, de gestion RH ainsi que des logiciels de gestion intégrée (ERP). Cette attaque avait entrainé la fuite de données impactant de nombreux clients de la société.

Vol de données par le groupe Termite contre le département français de la Réunion

DATE : 13/11/2024
SOURCE : **BULLETIN CXN-2024-6579**[65]

Le groupe ransomware Termite a revendiqué le vol de données appartenant à un département français d'outre-mer. Le département en question avait fait état publiquement d'une « fuite de données limitée ». Tous les réseaux informatiques avaient été temporairement interrompus pour endiguer cette menace.

Cicada3301 revendique la compromission du constructeur automobile français Peugeot

DATE : 15/12/2024
SOURCE : **Bulletin CXN-2024-7127**[67]

Les opérateurs **du groupe de RaaS Cicada3301 ont revendiqué la compromission** de 35Gb de données relatives aux concessions du **constructeur automobile français Peugeot**. Sur le site vitrine du groupe criminel, un échantillon des documents volés a été publié. Les concessions Peugeot n'ont pas encore communiqué publiquement au sujet de cet incident de sécurité informatique.

Hunters International revendique la compromission du fournisseur français Ecritel

DATE : 17/12/2024
SOURCE : **Bulletin CXN-2024-7147**[66]

Les opérateurs **du groupe ransomware Hunters International ont revendiqué la compromission d'un fournisseur français spécialisé dans l'hébergement cloud.** Sur son site vitrine, le collectif criminel a publié un échantillon des 135 GB de données volées, incluant des informations sensibles sur les clients, les activités commerciales et les projets du fournisseur.

Revendication par le groupe ransomware SpaceBears de la compromission d'Atos

DATE : 28/12/2024
SOURCE : **Bulletin CXN-2024-7306**[68]

Le groupe ransomware Spacebears a revendiqué sur son site de fuite de données **la compromission de la multinationale française de conseil en technologie de l'information, Atos.** Le 29 décembre, l'entreprise a déclaré n'avoir relevé aucune preuve de compromission ou de ransomware affectant ses systèmes ainsi qu'aucune demande de rançon. Une enquête a néanmoins été ouverte.

2. ANALYSE DES PRINCIPALES TENDANCES 2024

Les tendances développées dans ce rapport ont été modélisées à partir des données collectées quotidiennement par le CERT-XMCO et partagées par l'intermédiaire du service Yuno. Bien qu'elles s'inscrivent dans la continuité de l'année 2023, nous relevons ici les principales menaces ou évolutions observées durant l'année 2024.

2.1
Des vulnérabilités exploitées plus rapidement dans des produits plus variés

Des vulnérabilités de type 0-day exploitées
par des groupes APT et ransomware

L'exploitation de vulnérabilités 0-day est une tendance toujours largement répandue chez les acteurs de la menace, qui les instrumentalisent activement dans leurs attaques[69][70][71]. **Elles leur ont permis de conduire des campagnes massives et indétectables, augmentant l'impact sur les organisations compromises**, à l'image de l'opération Lunar Peek réalisée via l'exploitation des CVE-2024-0012 et CVE-2024-9474 affectant Palo Alto Interface Management[72].

En raison des ressources nécessaires à leur identification et à leur instrumentalisation, les vulnérabilités 0-day ont été **exclusivement exploitées par des groupes sophistiqués, en particulier par les menaces APT affiliées à des États**. Le groupe APT chinois Velvet Ant a par exemple utilisé la vulnérabilité 0-day CVE-2024-20399 au sein de Cisco NX-OS pour distribuer une backdoor personnalisée à des fins de collecte de renseignements stratégiques[73].

Certains groupes criminels disposant d'importantes ressources techniques utilisent également cette technique, à l'image du groupe ransomware Termite qui a exploité la vulnérabilité 0-day référencée CVE-2024-50623 affectant Cléo afin de compromettre au moins 10 organisations opérant dans des secteurs d'activité variés[74][75].

FOCUS VULNÉRABILITÉ
CVE-2024-21338 AFFECTANT WINDOWS APPLOCKER

Le 28 février 2024, les chercheurs d'Avast ont révélé **l'exploitation d'une vulnérabilité 0-day affectant Windows AppLocker par le groupe APT associé à la Corée du Nord Lazarus**, afin de distribuer un Remote Access Trojan (RAT) non communiqué[76]. Corrigée dans le cadre du Patch Tuesday de Microsoft du 13 février 2024, la CVE-2024-21338 permettait à un attaquant local authentifié d'élever ses privilèges[22].

Le groupe APT Lazarus a **exploité cette vulnérabilité pour créer une primitive de noyau en lecture / écriture dans une version mise à jour de son rootkit FudModule** qui intègre de nouvelles fonctionnalités plus furtives ainsi que des capacités avancées.

Avast indique que cette nouvelle technique d'exploitation est un tournant majeur dans la capacité des acteurs malveillants à accéder au noyau. Par cette intermédiaire, ils peuvent effectuer des attaques plus furtives et persister durablement sur des systèmes compromis.

La réduction du temps d'exploitation
de vulnérabilités récemment corrigées

Les acteurs de la menace ont **profité du délai de mise à jour des logiciels** par les utilisateurs pour exploiter des vulnérabilités déjà corrigées[77][78][79]. Cette tendance a été **exacerbée par la publication d'un PoC ou d'analyses de chercheurs** qui peuvent être partagées peu de temps après la publication du bulletin de sécurité de l'éditeur[80][81][82][83][84].
La CVE-2024-27198 affectant JetBrains TeamCity a ainsi été massivement exploitée deux jours après la publication d'un correctif et d'une analyse technique le jour même[85].

L'accès à des éléments techniques complémentaires facilite l'exploitation de ces vulnérabilités par des acteurs n'ayant pas ou peu de compétences techniques[86][87]. Dans certains cas, les acteurs de la menace ont pu exploiter de vulnérabilités disposant d'un correctif disponible depuis plusieurs années, mais non appliqué par les utilisateurs[69][88][89][90].

Aux États-Unis des universités et institutions publiques ont été compromises via l'exploitation de vulnérabilités datant de 2018[91]. Ce délai d'application peut s'expliquer par l'impact opérationnel que peut engendrer certains processus de mises à jour sur de vastes parcs informatiques. En outre, des mises à jour défectueuses peuvent être distribuées par les éditeurs, comme ce fut le cas en juillet 2024 lors de la diffusion d'une nouvelle version de la solution antivirus Crowdstrike Falcon, qui a entraîné une panne majeure ayant lourdement impacté les opérations de nombreux de ses clients[92].

FOCUS VULNÉRABILITÉ
CVE-2024-23897 AFFECTANT JENKINS

Corrigée le 24 janvier, la vulnérabilité référencée CVE-2024-23897 provenait d'une erreur de traitement des commandes dans l'interface de ligne de commande de Jenkins. Des attaquants distants l'auraient employée pour envoyer des commandes spécifiquement conçues et lire des fichiers arbitraires sur des serveurs Jenkins vulnérables[93][94].

C'est notamment le cas d'un acteur malveillant connu sous le pseudonyme **IntelBroker, qui aurait exploité cette faille de sécurité près de 6 mois après la publication du correctif de sécurité afin de compromettre le fournisseur de services informatiques BORN Group**[95]. Cette attaque ciblant la chaîne d'approvisionnement logicielle avait affecté en cascade les clients de la firme, compromettant les données sensibles de plus de 196 000 de ses clients dont Bank of Ireland, Mont-Blanc, Cartier, Hitachi, Lindt Chocolate ou Nestlé.

L'exploitation de la CVE-2024-23897 a également permis à des affiliés du groupe ransomware RansomEXX de perturber l'écosystème bancaire indien, dans une attaque ayant ciblé Brontoo Technology Solution, un partenaire de la société C-Edge qui fournit des services et infrastructures aux institutions financières indiennes[96].

Une diversification
des produits ciblés

Les acteurs de la menace ont continué d'exploiter des vulnérabilités affectant des **produits situés en périphérie de réseaux**. Les groupes criminels ont particulièrement visé des technologies de sécurité telles que des pare-feu ou des VPN qui permettent de prendre pied dans l'infrastructure d'une organisation et d'accéder à des données sensibles exploitables pour se latéraliser ensuite au sein du réseau[13][79][97][98][99][100].

Pour ces mêmes raisons, les **outils d'accès à distance sont également régulièrement ciblés**, à l'instar des CVE-2024-1708 et CVE-2024-1709 affectant ScreenConnect, exploitées par le groupe APT nord-coréen Kimsuky pour déployer le malware ToddlerShark [101] [102] [103]. En outre, **les environnements virtuels et en particulier ceux de VMware ESXI sont privilégiés** par les attaquants en raison de la visibilité limitée de ces instances par les solutions de sécurité mais aussi de la possibilité de compromettre massivement les machines virtuelles vulnérables[104][105].

À travers la compromission d'un nombre varié de technologies, les attaquants ont cherché à étendre leur surface d'attaque pour obtenir le vecteur d'accès initial. **Dans certains cas, ils ont ciblé des solutions tierces pour compromettre la chaine d'approvisionnement logicielle**[95][106][107]. L'objectif étant de contourner les systèmes de sécurité des organisations ciblées et réaliser des attaques à grande échelle, comme l'illustre de la compromission de la solution de gestion d'accès BeyondTrust via les CVE-2024-12356 et CVE-2024-12686[108][109]. Cet accès a ensuite été exploité pour compromettre son client, le département du Trésor américain, à des fins d'espionnage[110].

FOCUS VULNÉRABILITÉ
CVE-2024-12356 ET CVE-2024-12686 AFFECTANT REMOTE SUPPORT ET PRIVILEGED REMOTE ACCESS DE BEYONDTRUST

Le 18 décembre 2024, la société de cybersécurité américaine **BeyondTrust a annoncé avoir fait l'objet d'une intrusion informatique via l'exploitation de 2 vulnérabilités** affectant ses produits Remote Support et Privileged Remote Access[108][109].

Référencées CVE-2024-12356 et CVE-2024-12686, les deux failles de sécurités ont permis aux attaquants d'accéder à une clé d'API permettant de réinitialiser les mots de passe de plusieurs comptes d'applications locales et de prendre le contrôle des instances SaaS de support à distance.

Les attaquants ont ensuite **utilisé cet accès pour obtenir une clé utilisée pour fournir une assistance technique aux utilisateurs du département du Trésor américain**[110]. Par cet intermédiaire, ils ont pu contourner les mesures de sécurité et accéder à distance à certains postes de travail ainsi qu'à certains documents non classifiés conservés par les utilisateurs.

L'agence gouvernementale américaine a révélé que le piratage de ses systèmes avait été effectué par un mode opératoire APT associé à la Chine à des fins d'espionnage. En outre, elle a affirmé que les instances compromises ont depuis été fermées et la clé API volée révoquée, laissant supposer que les acteurs de la menace n'ont plus accès aux ordinateurs.

2.2
Des groupes ransomware résilients et sophistiqués intégrés à un écosystème concurrentiel

L'exploitation de vulnérabilités comme vecteur d'accès initial et de forum de piratage *à des fins promotionnelles*

Les groupes ransomware ont tiré parti de **failles de sécurité récemment découvertes comme vecteur d'accès initial** aux réseaux ciblés[88][77][105][111]. Le recours à ces vulnérabilités, conjointement à l'exploitation d'outils personnalisés et de logiciels légitimes de supervision (RMM – Remote Monitoring and Management), a permis à ces acteurs criminels de prendre pied dans les réseaux ciblés puis de se latéraliser au sein de leur système pour distribuer des ransomware[44][84][112].

D'une part, les opérateurs de ransomware **se sont appuyés sur les forums du Deep/Dark web pour recruter de nouveaux courtiers d'accès initiaux (IAB – Initial Access Brokers)(6) et faire la promotion de leurs programmes d'affiliation**[113][114]. Pour attirer de nouveaux affiliés, le groupe ransomware Mallox leur propose une redistribution de 70% à 80% du total des rançons payées par les victimes ainsi qu'une grande autonomie concernant le choix du vecteur de compromission initiale[115].

Les vulnérabilités exploitées par les groupes ransomware en 2024

Références CVE	Technologies	Groupes ransomware	Sources
CVE-2024-1708 et CVE-2024-1709	ScreenConnect	Black Basta, Bl00dy et XWorm	CXN-2024-1188
CVE-2024-27198, CVE-2024-27199 et CVE-2023-42793	JetBrains TeamCity	Bianlian et Jasmin	CXN-2024-1404 et CXN-2024-1633
CVE-2023-22518	Atlassian Confluence	Cerber	CXN-2024-2313
CVE-2023-41266, CVE-2023-41265 et CVE-2023-48365	Qlink SE	Cactus	CXN-2024-2521
CVE-2024-4577	PHP	TellYouThePass	CXN-2024-3345
CVE-2024-26169	Windows	Black Basta	CXN-2024-3406
CVE-2020-1472	Netlogon (Microsoft)	RansomHub	CXN-2024-3248
CVE-2024-37085	VMware ESXI	Akira et Black Basta	CXN-2024-4345
CVE-2023-27532	Veeam Backup	Akira et EstateRansomware	CXN-2024-4032 et CXN-2024-3996
CVE-2024-37085	VMware ESXi	BlackByte	CXN-2024-4924
CVE-2023-3519	Citrix ADC	RansomHub	CXN-2024-4934
CVE-2023-27997	FortiOS	RansomHub	CXN-2024-4934
CVE-2024-40766	SonicWall	Akira	CXN-2024-5138
CVE-2024-6670 et CVE-2024-6671	WhatsUp Gold	-	CXN-2024-5227
CVE-2022-47966	Zoho ManageEngine	Embargo	CXN-2024-5542
CVE-2023-4966	Citrix NetScaler	Embargo	CXN-2024-5542
CVE-2023-29300	ColdFusion	Embargo	CXN-2024-5542
CVE-2023-38203	ColdFusion	Embargo	CXN-2024-5542
CVE-2024-51378	CyberPanel	PSAUX	CXN-2024-6223
CVE-2024-40766	SonicOS	Akira et Fog	CXN-2024-6177
CVE-2024-40711	Veeam B&R	Akira et Fog	CXN-2024-5819 et CXN-2024-6413
CVE-2024-11667	Zyxel	Helldown	CXN-2024-6797 et CXN-2024-6560
CVE-2024-50623	Produits Cleo	Cl0p et Termite	CXN-2024-7117 et CXN-2024-7001

D'autre part, **ces collectifs ont également instrumentalisé des vulnérabilités 0-day, démontrant la sophistication de certains acteurs** composant l'écosystème criminel, tel que le groupe à motivation financière Cardinal qui a exploité la CVE-2024-26169 affectant Windows Error Reporting[116]. Dans une campagne réalisée à partir de décembre 2023, les acteurs de la menace ont tenté d'exploiter la CVE-2024-26169 pour distribuer le ransomware Black Basta, déjà déployé en France sur des hôpitaux et gouvernements locaux notamment[75][117].

En outre, la fin d'année a été marquée par le retour du groupe criminel Cl0p, très actif en 2023, via l'exploitation de la 0-day référencée CVE-2024-50623 affectant Cleo[107][118].

FOCUS MENACE
LE RETOUR DE CL0P

La fin d'année 2024 a été marquée par le **retour du groupe criminel Cl0p via l'exploitation d'une nouvelle vulnérabilité 0-day affectant des solutions de transfert de fichiers commercialisées par Cleo** (produits Harmony, VLTrader et LexiCom) [107][118]. Référencée CVE-2024-50623, cette faille de sécurité aurait permis aux attaquants de télécharger des fichiers à distance sans restriction, leur permettant en conséquence d'exécuter du code arbitraire.

L'exploitation de la CVE-2024-50623 comme 0-day avait été ensuite confirmée par les opérateurs de Cl0p , dans un premier temps auprès des journalistes de Bleeping Computer, puis sur leur site vitrine. Quelques jours plus tard, les affiliés du groupe ransomware faisaient **mention de 66 nouvelles organisations compromises, majoritairement situées aux États-Unis** à l'image de la société de logiciel Blue Yonder.

Le groupe Cl0p s'était déjà illustré au cours des quatre dernières années par sa capacité à identifier et instrumentaliser des vulnérabilités 0-day au sein de diverses solutions de transfert de fichiers, telles que File Transfert Appliance d'Accellion en 2021, puis de SolarWinds Serv-U, GoAnywhere MFT et MOVEit Transfer en 2023[119][120].

Il n'est pas à exclure que d'autres technologies similaires deviennent la cible de ce groupe criminel sophistiqué. De manière notable, un autre groupe ransomware nommé Termite aurait également détourné la CVE-2024-50623 mais aucune information publiquement disponible n'indique un éventuel lien d'affiliation entre ces deux collectifs criminels[74].

2.2.2 DES GROUPES RANSOMWARE RÉSILIENTS ET SOPHISTIQUÉS INTÉGRÉS À UN ÉCOSYSTÈME CONCURRENTIEL

Un ciblage accru des infrastructures de virtualisation et une simplification des schémas d'extorsion

pour maximiser les opportunités de compromission

Les opérateurs de ransomware ont continué de **développer des outils ciblant divers systèmes d'exploitation et plus particulièrement les hyperviseurs**[121][122][123]. Ce ciblage a pu s'effectuer via l'exploitation de vulnérabilités fournies par des courtiers d'accès initiaux comme Storm-0506, Storm-1175, Octo Tempest, et Manatee Tempest, menant dans certains cas à la distribution des ransomware Akira et Black Basta[104][105]. La sophistication des TTPs employées s'est aussi mesurée par le recours à des outils

sur mesure promus sur les marketplaces du Deep/Dark Web, permettant **d'arrêter les systèmes de sécurité EDR et ainsi d'échapper plus efficacement à la détection**[124][125][126].

Ces évolutions contrastent avec **l'abandon de plus en plus fréquent par les groupes ransomware du chiffrement des données pour se concentrer sur un schéma d'extorsion simplifié**. BianLian, Medusa ou encore Rhysida ont abandonné le chiffrement pour se concentrer sur le vol des données et la menace de leur divulgation publique ultérieure sur un site vitrine[127][128]. Cette pratique en croissance pourrait répondre à un développement de chiffreurs trop coûteux, à une volonté d'échapper à la détection voire à une volonté d'optimiser les opportunités de compromission[129].

2.2.3 DES GROUPES RANSOMWARE RÉSILIENTS ET SOPHISTIQUÉS INTÉGRÉS À UN ÉCOSYSTÈME CONCURRENTIEL

La résilience de l'écosystème des RaaS
malgré les actions des forces de l'ordre

Les forces de l'ordre ont cherché à endiguer la portée et la sophistication des groupes criminels, en s'attaquant à leurs ressources techniques, financières et humaines. Cette approche s'est traduite par **l'arrestation d'affiliés, le démantèlement de réseau de financement ainsi que par la saisie d'infrastructures** à l'image de celle de LockBit via l'opération Cronos ou d'ALPHV/BlackCat, dont la saisie a entrainé l'exit scam(7) de l'opérateur[48][49][130][131][132]. Les autorités ont pu également compter sur des acteurs privés qui ont publié des outils permettant d'entraver la propagation de codes malveillants populaires et de faciliter leur détection par les outils de sécurité[35][133][134].

Les groupes criminels ont néanmoins su s'adapter rapidement en exploitant ces démantèlements pour recruter de nouveaux affiliés comme Scattered Spider, un ancien partenaire du groupe ALPHV/BlackCat qui est désormais associé à RansomHub[42][38]. **Le développement de nouvelles souches de ransomware sur la base du code source d'ancien malware ou la création de nouvelles variantes ont aussi participé** au phénomène de prolifération et de résilience de l'écosystème, à l'instar de Hunters International qui a basé son ransomware sur le code source de Hive, ou de LockBit qui a annoncé la 4ème version de son RaaS en décembre 2024[46][66][135].

(6) Un courtier d'accès initial (Initial Access Broker - IAB) est un acteur de la menace spécialisé dans l'infiltration de systèmes et de réseaux informatiques, puis dans la vente de cet accès à d'autres acteurs malveillants.

(7) Un exit scam désigne une escroquerie lors de laquelle une entité cesse de fournir son service tout en s'accaparant l'argent de ses partenaires. En l'occurrence, APLHV/BlackCat a mis fin à ses activités en conservant les rançons de ses victimes sans les redistribuer à ses affiliés au préalable.

2.3
Un écosystème cybercriminel qui s'adapte à une clientèle en recherche d'outils furtifs et variés

L'accès initial simplifié par des services *promus sur le Deep Dark Web*

Le phishing reste un des vecteurs de compromission les plus employés pour distribuer des malware. Pour cibler un large public, les cybercriminels se sont **appuyés sur de multiples plateformes de type Phishing-as-a-Service** (PaaS)[136][137][138][139].

Ces dernières facilitent la production clé en main de leurres distribués via diverses techniques de malvertising(8), de SEO poisoning(9), ou qui sont envoyés à leurs cibles en s'appuyant sur des plateformes légitimes telles que YouTube, Telegram, OneNote, LinkedIn et Microsoft Teams[140][141][142][143].

FOCUS MENACE
PROGRAMME DE PHISHING-AS-A-SERVICE

Le 21 novembre 2024, **Microsoft a annoncé la saisie de 240 domaines frauduleux associés à des activités de Phishing-as-a-Service** commercialisés par un groupe localisé en Égypte[144]. Référencé ONNX, ce service populaire aurait été opéré par Abanoub Nady depuis 2017, un acteur de la menace connu sous le pseudonyme MRxC0DER au sein de l'écosystème cybercriminel.

D'après Microsoft, **le programme ONNX figurait parmi les 5 kits de phishing les plus prolifiques en termes de volume de courriels malveillants** au cours du premier semestre de l'année 2024. Ce service aurait usurpé diverses entités privées et organisations internationales, menant à la distribution d'infostealers, de ransomware et au détournement d'actifs financiers. Commercialisé par MRxC0DER sur Telegram, le programme proposait divers niveaux d'abonnements (Basic, Professional, Enterprise) allant de 150 à 550 dollars par mois.

En outre, ONNX proposait à ces clients des pages de phishing exploitant des techniques sophistiquées de type Adversary-in-the-middle (AiTM), permettant de contourner les nouvelles mesures de sécurité et les protections par authentification multifactorielle (MFA).

L'accès à ces PaaS est généralement **obtenu par l'intermédiaire de forums et marketplaces présents sur le Deep/Dark Web** où des acteurs de la menace en font la promotion. En outre, ces infrastructures criminelles **permettent d'acheter d'autres types de services et produits comme des bases de données** offrant des accès à des entreprises compromises. Par exemple, le collectif d'acteurs malveillants Nears a pour activité la monétisation d'accès initiaux et de bases de volées dont il fait la promotion sur les plateformes BreachForums et Telegram. Ce dernier, qui a une victimologie opportuniste, a revendiqué la compromission de données relatives à des firmes françaises évoluant dans les secteurs des télécommunications, de l'assurance, des médias, de la finance et de la santé.

(8) Cette technique désigne l'utilisation de publicités en ligne conçues pour apparaître légitime mais qui délivrent en réalité un code malveillant ou qui invitent les utilisateurs à fournir des informations sensibles afin de les voler.
(9) Cette technique souvent couplée avec le malvertising vise à accroître la visibilité de sites web malveillants en exploitant des méthodes destinées à améliorer leur référencement.

Le développement d'outils variés
pour contourner les outils de sécurité

Afin de faciliter le **contournement de solutions de sécurité, les acteurs de la menace se sont appuyés sur différents malware et plus particulièrement les loaders**. Ces derniers, principalement promus sur les marketplaces criminelles, sont très populaires au sein de l'écosystème, tels que le Loader-as-a-Service (LaaS) DarkGate qui dispose d'une fonctionnalité de contournement de la solution de sécurité Windows SmartScreen[24].

Les loaders apportent une couche d'obfuscation supplémentaire aux activités menées par les attaquants et **permettent de distribuer en cascade des ransomware, des Remote Access Trojan (RAT) ou des infostealers**[145][146][147][26]. Certains ont intégré de nouvelles fonctionnalités comme la capacité de désactiver des outils de sécurité de type EDR ou antivirus tels qu'HijackLoader, qui est en mesure de contourner la solution de détection de virus Windows Defender[124][125][148].

FOCUS MENACE
OUTIL EDRSILENCER

Dans un rapport publié le 15 octobre 2024, les chercheurs de Trend Micro ont analysé un **outil légitime de Red Team nommé EDRSilencer**. Ce dernier est conçu à l'origine pour tester les solutions EDR mais serait désormais **détourné par les acteurs de la menace afin d'échapper à la détection des solutions de sécurité**[149].

L'outil identifie dynamiquement les processus EDR et crée des filtres WFP (Windows Filtering Platform) persistants qui bloquent leur trafic sortant, coupant ainsi la télémétrie ou les alertes que les solutions EDR envoient généralement aux consoles de gestion.
Les attaquants qui l'utilisent peuvent étendre leur liste de cibles en mettant en place des règles spécifiques, ce qui le rend efficace contre un large éventail d'outils de sécurité, parmi lesquels Microsoft Defender, SentinelOne et Palo Alto Networks Traps.

Un autre outil similaire avait été identifié par les chercheurs de Trend Micro au mois de septembre dernier. **Référencé sous le nom EDRKillShifter, cet outil permettait de désactiver les solutions EDR en exploitant les pilotes vulnérables**. Le groupe criminel RansomHub l'aurait utilisé dans le cadre de ses attaques afin de persister dans les réseaux compromis même après avoir été détecté, en s'adaptant dynamiquement[125].

Des opérations de lutte contre le cybercrime *aux impacts modérés*

Des affiliés jusqu'aux infrastructures de commande et de contrôle, les forces de police internationales ont tenté **d'endiguer les activités cybercriminelles en s'attaquant à chaque intermédiaire humain et technique responsable d'opérations malveillantes**[150][151][152][153][144](10).

L'une des plus marquantes reste la saisie d'une centaine de serveurs associés à plusieurs Malware-as-a-Service (MaaS), notamment IceID, SystemBC, SmokeLoader et Bumblebee, lors d'une opération de lutte contre la cybercriminalité nommée Operation Endgame[154].

FOCUS MENACE
OPÉRATION MAGNUS

Le 28 octobre 2024, la police nationale néerlandaise, en collaboration avec le FBI, le NCIS, la NCA et d'autres forces de l'ordre européennes, a annoncé la **saisie des infrastructures numériques associées aux Infostealers-as-a-Service Redline et Meta (variante de Redline) dans le cadre d'une campagne de lutte contre la cybercriminalité, nommée Opération Magnus**[155].

D'après la déclaration publique, un accès complet aux serveurs aurait été obtenu par les enquêteurs, leur permettant de mettre la main sur le code source des deux malware, ainsi que d'accéder à la liste des clients ayant employé ces outils criminels. Par ailleurs, le ministère américain de la Justice a lancé des **poursuites contre Maxim Rudometov, l'un des développeurs et administrateurs de RedLine, tandis qu'Eurojust a placé deux personnes en garde à vue en Belgique**.

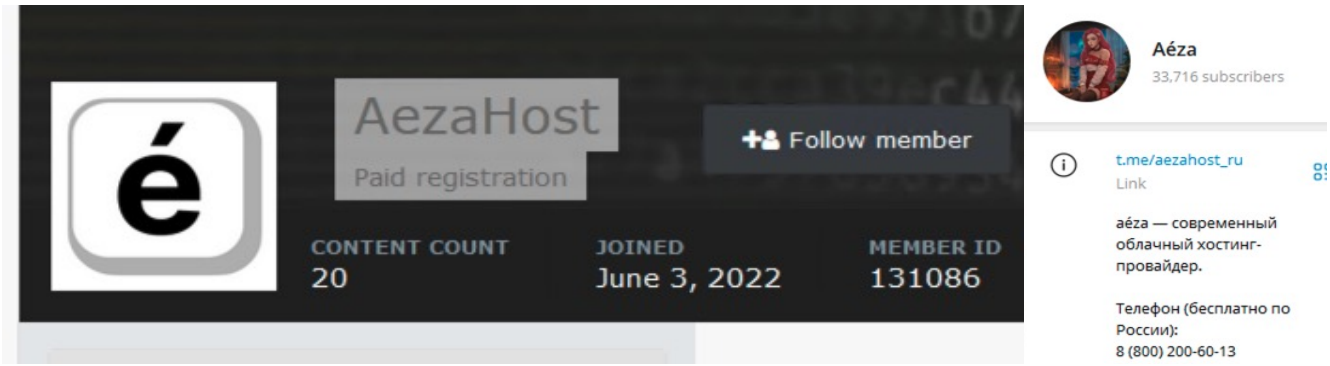
Observés respectivement pour la première fois en 2020 et 2022, Redline et Meta sont des outils populaires au sein de l'écosystème cybercriminel, y compris chez les opérateurs de ransomware [156]. En début d'année 2024, les opérateurs de l'infostealer Meta avaient développé une **version macOS, démontrant la capacité d'adaptation des acteurs de la menace pour s'adapter aux besoins exprimés par leurs clients**[157].

Bien que l'opération Magnus puisse endiguer temporairement les activités malveillantes associées à l'utilisation de Redline et Meta, il n'est pas à exclure que ces deux outils soient remplacés par d'autres infostealers promus sur les marketplaces criminelles comme Lumma ou Atomic Stealer[158][159].

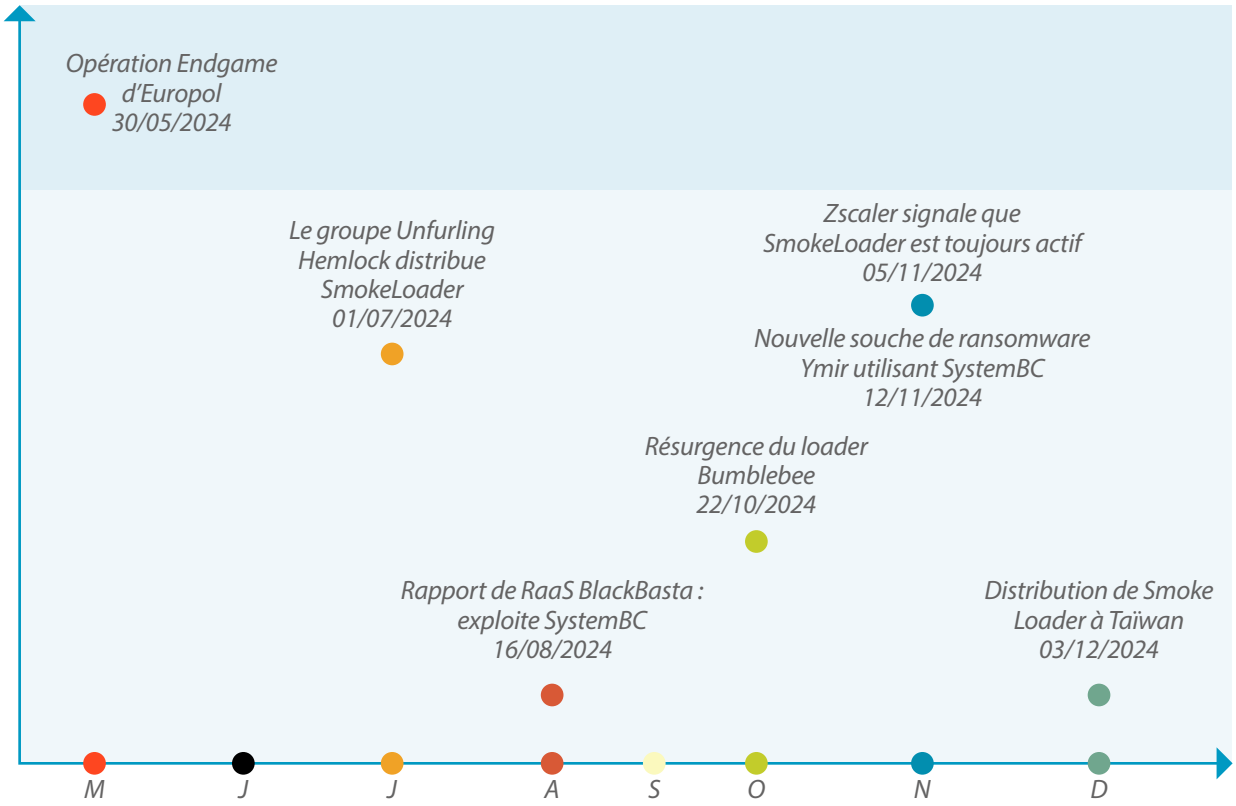
Malgré ces efforts, **l'écosystème a démontré une forte capacité de résilience** illustrée par la poursuite des détections de SmokeLoader ou de Plugx, distribués quelques mois plus tard après leur démantèlement[160][161][162]. Les actions des forces de l'ordre ont également été **contournées par le développement de nouvelles variantes** comme c'est le cas pour Pikabot et Zloader[163][164][165].

En outre, les opérateurs ont **exploité des solutions d'hébergement «Bulletproof(11)»** permettant d'héberger du code malveillant et des serveurs C2 pour complexifier la saisie d'infrastructures et bénéficier d'un certain degré d'anonymat[166][167].

Aéza est un service d'hébergement Bulletproof populaire au sein de l'écosystème criminel et promu sur Exploit et Telegram



Résurgence de MaaS faisant suite à l'opération de police Endgame



(10) C.f. Annexe 1 : Synthèse des operations marquantes de lutte contre le cybercrime en 2024 traitées dans Yuno.

(11) Les hébergeurs bulletproof, dits pare-balles, sont des solutions peu regardantes sur l'identité du client ainsi que sur l'utilisation du service par ce dernier. En outre, ils sont situés dans des pays où la collaboration avec les autorités n'est pas systématiquement appliquée.

2.4
Des modes opératoires APT aux objectifs pluriels établis par les États auxquels ils sont associés

La Russie poursuit ses opérations
en Ukraine et en Occident

2.4.1.1 L'ESPIONNAGE ET LA DÉSINFORMATION CONTRE LES PAYS MEMBRES DE L'OTAN ET LES ALLIÉS DE KIEV

Les services de sécurité russes ont poursuivi leur collecte de renseignements stratégiques au sein des pays membres de l'OTAN et de leurs alliés, à l'instar des opérateurs d'APT29 qui ont ciblé des partis politiques allemands en amont des élections européennes de juin 2024[168][169][170][171]. Ce groupe d'attaquants s'est également distingué par l'usurpation de services légitimes dans des campagnes de spear-phishing ciblant plusieurs entités européennes, dont plusieurs en France[172].

FOCUS MENACE
APT28

Au cours de l'année 2024, le mode opératoire APT28 associé au renseignement militaire russe (GRU) a régulièrement opéré des **campagnes d'attaques ciblant l'Ukraine et les pays occidentaux à des fins d'espionnage**. Le groupe a compromis des organisations évoluant dans des secteurs stratégiques comme celui de la défense, de l'aérospatiale ou de l'énergie via l'exploitation de TTPs sophistiquées et diversifiées[173][174].

Par l'intermédiaire de la vulnérabilité critique référencée CVE-2023-23397 affectant Microsoft Outlook, **APT28 a compromis des partis politiques allemands, des institutions tchèques ainsi que plusieurs autres agences et entités membres de l'Union européenne**[171]. Il a également utilisé des campagnes de phishing pour distribuer les backdoors MASEPIE et OCEANMAP afin de compromettre des organisations gouvernementales en Pologne, en Azerbaïdjan, mais aussi en Ukraine[175]. Ce dernier reste une cible prioritaire pour le mode opératoire comme en témoigne sa campagne ayant ciblé le personnel diplomatique en activité dans le pays[176]. Il a exploité des méthodes avancées de spear-phishing qu'il a combiné avec le détournement de services légitimes pour distribuer la backdoor Headlace.

Dans le cadre de ses activités d'espionnage, il exploite également des routeurs compromis via des botnets tels que Moobot, démantelé en février 2024 par le Département de la Justice américain[177][173]. **En outre, ses opérations ne reposent pas uniquement sur des opérations de collecte de renseignement.** Les autorités polonaises ont attribué la cyberattaque menant à la publication de 2 articles de presse mensongers annonçant la mobilisation de 200 000 soldats polonais au groupe APT28[178]. Cette campagne s'inscrit dans la continuité des tentatives de russe d'influencer les opinions publiques européennes sur le soutien apporté à l'Ukraine.

Au-delà de ses activités d'espionnage, la Russie a parrainé des **opérations de désinformation propageant des narratifs tirant parti des fractures internes des pays membres de l'OTAN et de l'Union européenne**[179][180][178][181]. Le cluster d'influence russe Doppelgänger s'est prépositionné en amont des grands évènements politiques et sportifs de 2024 afin de remettre en question l'aide financière et militaire apportée à l'Ukraine[182][183][184][185]. Les opérateurs russes se sont également **appuyés sur les outils d'IA générative afin de produire et diffuser à grande échelle des articles mensongers** en amont de l'élection présidentielle américaine[186][187].

2.4.1.2

VERS UN ÉLARGISSEMENT DES OPÉRATIONS DE SABOTAGE EN EUROPE DE L'EST

Le service de renseignement militaire russe (GRU) a **continué ses opérations de sabotage en Ukraine**. Il s'est notamment **concentré sur des infrastructures critiques** comme l'illustre l'exploitation du wiper AcidPour par le groupe russe APT Sandworm pour cibler des services de télécommunications[188]. Les services ukrainiens avaient déjà observé l'APT Sandworm en 2023 à la suite du sabotage des infrastructures de l'opérateur mobile Kyïvstar[189][190].

Dans un contexte d'escalade des tensions en raison de l'aide supplémentaire apportée à l'Ukraine, des **opérations de sabotage russes ont également ciblé des pays d'Europe de l'Est**. Palo Alto a identifié la **compromission de systèmes de contrôle industriel en Roumanie** par le malware FrostyGoop, déjà observé en avril dernier lors d'une attaque informatique où 600 immeubles d'habitation ukrainiens avaient été privés d'alimentation électrique[191][192].

Des opérations cyber au service des ambitions régionales *et internationales de la Chine*

2.4.2.1 LA RÉUNIFICATION DE TAÏWAN AU SEIN DE LA RPC COMME OBJECTIF PRIORITAIRE

Pékin a poursuivi son projet de **réunification de Taïwan au sein de la RPC (République Populaire de Chine) via des opérations d'espionnage et d'influence**. Dès le mois de janvier, les chercheurs de Graphika ont identifié une campagne de désinformation chinoise, opérée en marge des élections présidentielles taïwanaises afin de promouvoir le parti pro-chinois Kuomintang et dénigrer ses adversaires politiques[193]. Ce type d'opérations a perduré tout au long de l'année, notamment via la campagne GLASSBRIDGE critiquant les velléités d'indépendance de l'île[194].

Les groupes APT ont également tiré parti du contexte électoral pour cibler diverses entités localisées à Taïwan à l'instar de Mustang Panda, par l'intermédiaire d'une version customisée du malware PlugX[195]. Durant cette même période, des organisations stratégiques taïwanaises liées à des cercles de réflexion, au secteur universitaire, à celui des télécommunications, ou encore à l'industrie de défense ont été la cible d'opérations d'espionnage[196][195][197][198][199][200].

Ces campagnes d'attaques se sont également étendues à la région Asie-Pacifique pour collecter du renseignement stratégique et économique sur des pays que Pékin considère comme partie intégrante de sa zone d'influence, mais aussi de son projet économique de Route de la Soie[201][202][203][17][201].

FOCUS MENACE APT EARTH LUSCA

En marge des élections présidentielles taïwanaises du 13 janvier 2024, **le groupe APT associé à la Chine Earth Lusca a réalisé une campagne de spear-phishing ciblant un groupe de réflexion universitaire privé basé à Taïwan**, spécialisé dans l'étude des relations politiques et économiques internationales.
Afin d'obtenir un accès initial, les attaquants ont envoyé des e-mails de phishing avec comme thématique des questions sur les relations sino-taïwanaises. En cliquant sur le fichier joint, la chaine d'infection entrainait la distribution d'une payload Cobalt Strike communiquant avec un serveur de Commande et de Contrôle (C2) et usurpant le nom de la société de cybersécurité Cybereason.

Par l'intermédiaire de cette campagne, **il a été possible d'établir un lien entre le mode opératoire et l'entreprise privée I-Soon** (aka I-S00n, Anxun) victime d'une fuite de données publiée en 2024 ayant révélé ses liens avec le régime de Pékin[204]. Selon les documents publiés sur GitHub, cette société aurait ainsi obtenu des contrats du ministère de la Sécurité d'État (MSE) et du ministère de la Sécurité publique (MSP) **pour réaliser des campagnes d'espionnage dans plus de 70 pays, dont la France, pour le compte du gouvernement chinois** (Hack-for-Hire)[205][206]. En outre, I-Soon utilise et vend des accès à plusieurs malware personnalisés tels que Hector, Winnti et la backdoor ShadowPad, qui a déjà été exploitée par l'APT Earth Lusca en Asie[207].

2.4.2.2

LE PRÉPOSITIONNEMENT DE PÉKIN SUR DES INFRASTRUCTURES STRATÉGIQUES OCCIDENTALES

Dans un contexte de relation politique tendue avec les États-Unis, notamment en région indo-pacifique, la Chine a prolongé en 2024 ses **activités d'espionnage politique sur des infrastructures stratégiques, en particulier dans des pays soutenant Taïwan**[208][100][209][210][211]. En mars 2024, la Lituanie a alerté sur l'intensification des campagnes d'espionnage ciblant ses agences gouvernementales et opérées par des groupes APT chinois[212]. Ces opérations se sont intensifiées, en particulier depuis l'ouverture d'une représentation diplomatique lituanienne à Taïwan en 2021.

Tout au long de l'année 2024, des clusters APT chinois ont **employé des botnets pour compromettre divers objets connectés (IoT - Internet of Things) et technologies en périphérie de réseaux**, tels que des routeurs et des pare-feu, à des fins d'espionnage massif[210][213][214]. **Cette collecte de renseignement a pris une dimension politique en amont des élections présidentielles américaines** lorsqu'un mode opératoire nommé Salt Typhoon a intercepté les données de plusieurs fournisseurs d'accès à Internet et firmes de télécommunications américaines afin d'espionner les membres des partis républicain et démocrate américains[209][210].

L'Iran dans une quête d'hégémonie régionale

via des opérations cyber offensives

2.4.3.1 LA POURSUITE DES ACTIVITÉS D'ESPIONNAGE EN OCCIDENT ET AU MOYEN-ORIENT

Les velléités d'hégémonie régionale de Téhéran ont poussé les modes opératoires qui lui sont associés à mener **des campagnes d'espionnage à des fins politiques**[215]. Ces groupes ont continuellement amélioré leurs campagnes d'attaques via du spear-phishing ciblé sur les réseaux sociaux, la distribution de code malveillant personnalisé et le recours à des outils légitimes de surveillance et de gestion à distance (RMM)[216][217].

Les opérateurs iraniens ont **ciblé des universitaires, des instituts de recherche, des personnalités politiques et des think tanks à l'international** en usurpant l'identité d'organismes légitimes et en établissant une relation de confiance avec leurs cibles[218][219]. Ils ont également **ciblé des infrastructures stratégiques au Moyen-Orient dans un contexte de tension croissante avec Israël**[220][221][222][223].

Le groupe APT34 a par exemple exploité la vulnérabilité CVE-2024-30088 affectant le kernel Windows pour distribuer la backdoor StealHook sur des entités gouvernementales et des infrastructures critiques aux Émirats Arabes Unis (EAU) et dans plusieurs pays du Moyen-Orient[224].

FOCUS MENACE L'ENTREPRISE EMENNET PASARGAD

En marge des Jeux-Olympiques de Paris 2024, une entreprise iranienne proche de l'IRGC (Corps des gardiens de la révolution islamique), nommée Emennet Pasargad (aka Aria Sepehr Ayandehsazan), **aurait compromis un fournisseur d'affichage commercial français en juillet 2024 afin de dénoncer la participation des athlètes israéliens aux Jeux Olympiques et paralympiques**. Cette opération se serait inscrite dans le cadre d'une campagne d'influence plus large, revendiquée sous la bannière d'un faux groupe d'extrême droite français nommé Regiment GUD[225].
Cette entreprise a fait l'objet d'un avis de sécurité publié par le FBI, le département du Trésor américain et l'INCD pour dénoncer le recours à cette société-écran par Téhéran pour camoufler les opérations des clusters APT Cotton Sandstorm, Marnanbridge et Haywire Kitten.
L'entreprise iranienne aurait depuis développé un réseau de fournisseurs d'hébergement, en ayant notamment recours aux services d'hébergement bulletproof proposés par BAcloud et Stark Industries Solutions, populaires au sein de l'écosystème cybercriminel pour leur complaisance sur l'identité des clients, l'utilisation et le contenu hébergé sur leur plateforme. **Les attaques de ces groupes peuvent s'inscrire dans le cadre du concept de «guerre douce»** introduit dans une série de déclarations officielles iraniennes publiées depuis août 2009 **consistant à faire la guerre à moindre cout via l'utilisation de tactiques coercitives non cinétiques**[226].

2.4.3.2

LE RECOURS À DES PROXIES CRIMINELS ET HACKTIVISTES POUR CAMOUFLER LES OPÉRATIONS DE TÉHÉRAN

Dans un contexte de confrontation avec Israël, les autorités iraniennes ont poursuivi leurs **opérations perturbatrices**[227][228]. Ils ont également **utilisé des proxies criminels et des collectifs hacktivistes** tels que Handala Hack pour réaliser leurs attaques[229][230].

Dans certains cas, les autorités iraniennes ont **collaboré avec des groupes ransomware à l'instar de NoEscape et Ransomhouse** en se positionnant comme des courtiers d'accès initiaux pour cibler des organisations basées aux États-Unis, en Azerbaïdjan, aux Émirats arabes unis et en Israël[15].

L'Iran a également cherché à promouvoir ses intérêts par des **opérations d'influence au sein des États considérés comme étant des adversaires géopolitiques** de Téhéran[231]. Il a été proactif en France durant les élections législatives ainsi qu'en amont des élections présidentielles américaines via la création de sites d'information cherchant à promouvoir les intérêts iraniens et à semer la discorde ainsi que la controverse chez les électeurs[232][233][234].

Les campagnes exploitent des événements opportunistes comme en témoigne la compromission d'un fournisseur d'affichage commercial français afin de dénoncer la participation des athlètes israéliens aux Jeux Olympiques et Paralympiques de 2024[225].

La Corée du Nord détourne des actifs financiers

et consolide ses capacités militaires

2.4.4.1 LE SOUTIEN AU RÉGIME DE PYONGYANG PAR DES OPÉRATIONS À MOTIVATION FINANCIÈRE

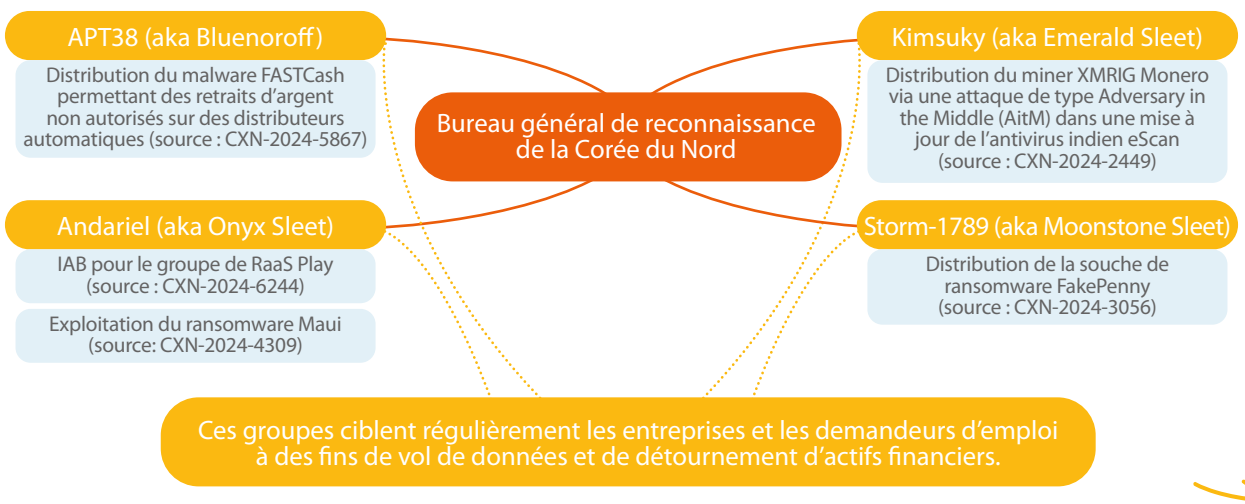
Le financement du régime est resté une priorité pour les opérateurs APT nord-coréens. Ces derniers ont développé leurs capacités cyber, via **l'exploitation de vulnérabilités 0-day, le détournement de services légitimes, ainsi que le développement de diverses souches de malware** ciblant les instances macOS, Windows et Linux.

Leur victimologie s'est principalement **axée sur les développeurs informatiques spécialisés dans les technologies de blockchain et sur les institutions financières**, comme en témoigne la campagne DEV#POPPER[235][236][237]. Opérée par le groupe Lazarus, elle a ciblé des développeurs via LinkedIn et des plateformes de recherche d'emplois afin de distribuer des malware, dont une nouvelle version macOS de BeaverTail conçue pour collecter les portefeuilles de cryptomonnaie ainsi que les données bancaires[238].
Dans d'autres cas, les attaquants ont directement **ciblé des plateformes d'échange de cryptomonnaies**. La compromission de la société indienne WazirX par exemple, avait abouti au détournement d'environ 235 millions de dollars en cryptoactifs[239].

Les groupes nord-coréens ont également exploité **des souches de ransomware personnalisées dans leurs attaques**, à l'image du groupe APT Moonstone Sleet (aka Storm-1789) qui a distribué une souche de ransomware nommée FakePenny via de fausses offres d'emploi et l'exploitation de versions compromises d'outils légitimes[240]. Dans certains cas, ils **collaborent directement avec des groupes ransomware** tels que Play et Maui, notamment pour cibler des entités américaines et sud-coréennes[241][242].

La finalité peut être financière, mais aussi politique en ajoutant au rançonnage la destruction des données.

Synthèse des operations criminelles associées a Pyongyang en 2024



2.4.4.2 LA CONSOLIDATION DES CAPACITÉS MILITAIRES NORD-CORÉENNES VIA L'ESPIONNAGE INTENSIF

Les modes opératoires APT parrainés par la Corée du Nord ont mené des campagnes d'espionnage sophistiquées visant à assurer la sécurité de Pyongyang à travers l'amélioration de ses capacités militaires et le développement de son programme nucléaire. Les groupes APT ont ponctuellement **ciblé la Corée du Sud en 2024, en adoptant une approche opportuniste via une collecte de renseignement multisectorielle**[243][244][245][246].

À l'international, les groupes nord-coréens se sont illustrés par **des campagnes de phishing ciblées à l'encontre d'employés d'organisations opérant dans des secteurs stratégiques**. Les chercheurs de Kaspersky avaient ainsi identifié une campagne de phishing qui avait visé des employés d'une organisation du secteur du nucléaire[247]. Cette attaque s'inscrivait dans une campagne plus vaste baptisée Operation Dreamjob, opérée par le mode opératoire UNC2970. La victimologie de ce dernier ne s'est toutefois pas limitée au secteur nucléaire, comme l'illustre une autre de ses campagnes qui avait utilisé des techniques similaires pour cibler des professionnels de l'industrie aérospatiale occidentale via de fausses offres d'emploi, afin de distribuer la backdoor MISTPEN et de collecter des renseignements stratégiques[248].

Malgré le rapprochement entamé entre les autorités russes et nord-coréennes depuis février 2022, **Pyongyang a continué de cibler des entités sensibles russes à des fins d'espionnage**. Une attaque notable aurait impliqué la distribution d'une backdoor référencée KONNI via un exécutable imitant un logiciel utilisé par les représentations consulaires russes pour communiquer avec le ministère des Affaires étrangères[249].

FOCUS MENACE
UNC5267

Le 23 septembre 2023, Mandiant a alerté sur **des travailleurs nord-coréens cherchant à occuper des postes dans le secteur informatique au sein d'entreprises occidentales**, afin de financer le régime de Pyongyang, voire de conduire des opérations d'espionnage. Observée depuis 2018, cette opération est suivie sous le nom d'UNC5267[250].

Les chercheurs indiquent que la majorité de ces travailleurs nord-coréens sont envoyés en Russie ou en Chine, une minorité étant cependant active en Afrique et en Asie du Sud-Est. Ils cherchent principalement à occuper des postes intégralement en distanciel au sein d'entreprises du secteur informatique américain et s'appuient sur des sociétés-écrans qui usurpent l'identité de vrais travailleurs étrangers ou en fabriquent de fausses de toute pièce.

Une fois les travailleurs recrutés, ils installent généralement sur leur ordinateur professionnel des outils de gestion à distance tels que GoToRemote / LogMeIn, GoToMeeting, Chrome Remote Desktop, AnyDesk, TeamViewer ou encore RustDesk. Ils sont également caractérisés par un refus de procéder à des appels vidéo afin de ne pas montrer leur visage et ainsi révéler la supercherie.

Cette méthode utilisée par la Corée du Nord a récemment été observée par la firme KnowBe4 qui avait indiqué en juillet 2024 avoir recruté un travailleur nord-coréen qui avait alors tenté d'installer des logiciels non autorisés, de transférer des fichiers potentiellement sensibles et de télécharger des malware.

2.5
Des groupes hacktivistes de plus en plus instrumentalisés par les États

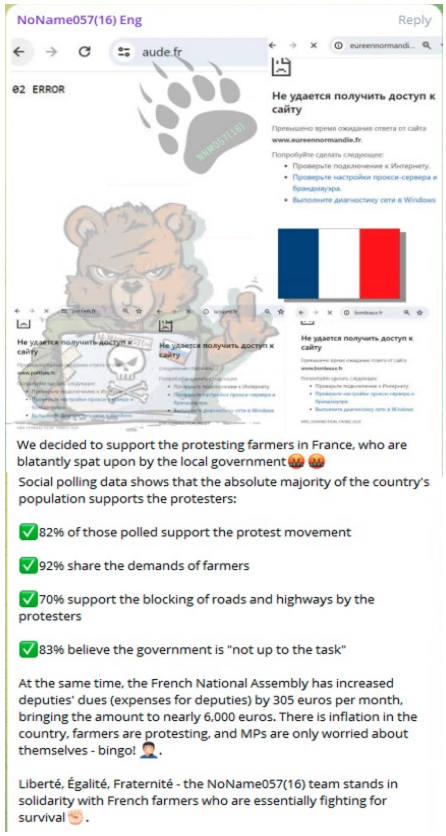
La France, cible prioritaire
de l'hacktivisme

En 2024, la France a été au centre de plusieurs campagnes hacktivistes en raison de **ses positions diplomatiques et des différents événements ayant eu lieu sur son territoire**[251][252][253]. Les Jeux Olympiques de Paris ont participé à la multiplication des opérations hacktivistes qui se sont traduites dans leur majorité par des attaques de déni de service à faible impact pendant l'événement sportif[27][254][255].

L'arrestation du fondateur de Telegram par la France le 24 août dernier a également été la cause d'une réaction de l'écosystème qui s'est exprimée par le ciblage massif du pays[256][257].

Revendication d'une attaque DDoS contre la France menée par RipperSec le 28 août 2024
Source : Telegram

Les groupes hacktivistes pro-russes ont été les plus actifs, avec l'objectif de faire la promotion d'un narratif favorable à Moscou, en ciblant en particulier les pays apportant un soutien à l'Ukraine[258]. Ces derniers ont **exploité un vaste panel d'évènements politiques et géopolitiques afin d'exacerber les tensions sociales internes**, comme les manifestations des agriculteurs de janvier 2024 ainsi que les différentes échéances politiques telles que les élections européennes et législatives françaises.
Ce faisant, leurs attaques par déni de service ont pu gagner en visibilité et bénéficier d'une amplification de la perception des dommages réellement causés[259][260][261].



NoName057(16) mène des activités de DDoS contre la France en soutien aux manifestations des agriculteurs
Source : Telegram

2.5.2 DES GROUPES HACKTIVISTES PARRAINÉS PAR DES INSTANCES ÉTATIQUES

Les groupes hacktivistes ont été instrumentalisés par des États qui ont la volonté d'effectuer des attaques informatiques tout en dissimulant leur implication et ainsi leur permettre d'éviter des représailles potentielles. En marge du conflit armé opposant **la Russie à l'Ukraine, les deux belligérants ont, via des groupes hacktivistes, réalisé des campagnes sophistiquées à des fins d'influence et de sabotage**[262][263]. Les collectifs hacktivistes pro-ukrainiens Blackjack ou BO Team ont ciblé plusieurs infrastructures critiques russes via la distribution de wiper comme Fuxnet.

Selon certains chercheurs, ils seraient directement affiliés aux services de renseignement ukrainiens[264][265]. De la même manière, par l'intermédiaire de groupes tels que XakNet Team, CyberArmyofRussia_Reborn1 et Solntsepek, le groupe russe APT44 a collecté et divulgué des informations sensibles de personnels ukrainiens[262].

Le Corps des gardiens de la révolution islamique (IRGC) a également exploité plusieurs groupes hacktivistes dans des opérations ciblant des entités hostiles à son régime. Plus ou moins structurés, **les collectifs pro-Téhéran ont mené diverses activités d'influence basées sur des attaques par déni de service, Hack&Leak et via des campagnes de désinformation**. Le groupe Homeland Justice a notamment perturbé les ressources de plusieurs services albanais en marge de la dégradation des relations entre les deux pays[266][267]. D'autres groupes, tels que Lord Nemesis et Handala Hack, ont également ciblé les institutions publiques et privées israéliennes en marge du conflit armé dans la bande de Gaza[289][268][269].

2.5.3 DES GROUPES HACKTIVISTES RÉSILIENTS FACE AUX NOUVELLES POLITIQUES DE TELEGRAM

À la suite de **l'arrestation du fondateur de Telegram**, Pavel Dourov, par les autorités françaises en raison du manque de régulations de sa plateforme sociale, des **mesures ont été prises pour limiter la diffusion des contenus associés aux comptes de collectifs hacktivistes**[270][271][272]. Toutefois, les groupes ont continué de revendiquer des attaques, à l'instar des groupes NoName057(16), Narodnaya Cyber Armia et UserSec qui ont ouvert de nouveaux canaux suite à leur démantèlement, afin de poursuivre la coordination et la revendication des attaques par déni de service[258].

Dans la perspective de **nouveaux durcissements de la politique de modération de Telegram, ces collectifs hacktivistes seraient susceptibles de s'orienter vers de nouvelles plateformes plus conciliantes**, telles que Twitter (aka X), Discord ou encore VK, bien que ces dernières puissent nuire à leur sécurité opérationnelle(12) et les empêcher de retrouver les fonctionnalités jusqu'à aujourd'hui garanties sur Telegram[273]. C'est notamment les cas des groupes NoName057(16), sudo rm-RF et d'Anonymous TV qui disposent d'un compte Twitter pour atteindre des audiences européennes[274][275][276].

(12) La sécurité opérationnelle désigne l'ensemble des dispositions numériques prises par un attaquant afin de maintenir son anonymat.

SYNTHÈSE DES OPÉRATIONS HACKTIVISTES AYANT CIBLÉ LA FRANCE EN 2024

JANVIER

Acteur : NoName057(16)
Impact : Déni de service
Cibles : Orano, Enercoop et EDF
Référence : **CXN-2024-0268**

Acteur : NoName057(16)
Impact : Déni de service
Cibles : Collectivités territoriales
Référence : **CXN-2024-0491**

FÉVRIER

Acteur : LulzSec
Impact : Dataleak
Cibles : Total Energies et CAF
Référence : **CXN-2024-0829**

Acteur : LulzSec
Impact : Dénie de service
Cibles : Secteur public, gendarmerie et JOP2024
Référence : **CXN-2024-0920**

MARS

Acteur : KyotoSH, Alixsec, GLORIAMIST, Athena et Team 1916
Impact : Déni de service
Cible : Multisectorielle
Référence : **CXN-2024-1425**

Acteur : Anonymous Sudan
Impact : Déni de service
Cible : Réseau interministériel
Référence : **CXN-2024-1399**

JUIN

Acteur : NoName057(16)
Impact : Déni de service
Cible : Multisectorielle
Référence : **CXN-2024-3272**

Acteur : NoName057(16)
Impact : Déni de service
Cible : Multisectorielle
Référence : **CXN-2024-3542**

JUILLET

Acteur : NoName057(16)
Impact : Déni de service
Cible : Multisectorielle
Référence : **CXN-2024-3861**

Acteur : NCA et HackNeT
Impact : Déni de service
Cible : Multisectorielle
Références : **CXN-2024-4068** et **CXN-2024-4333**

Acteur : LulzSec Muslims
Impact : Hack
Cible : Entités sportives
Référence : **CXN-2024-4376**

AOÛT

Acteur : Beregini
Impact : Hack&Leak
Cible : Agence polonaise Antidopage
Référence : **CXN-2024-4496**

Acteurs : Multiples
Impact : Déni de service
Cibles : Multiples
Références : **CXN-2024-4849** et **CXN-2024-4930**

SEPTEMBRE

Acteur : NoName057(16)
Impact : Déni de service
Cibles : Multiples
Référence : **CXN-2024-5098**

AOÛT

Acteurs : NoName057(16), AnonymousGuys, Hunt3r Kill3rs, Holy League et UserSec
Impact : Déni de service et Hack&Leak
Cibles : Multiples
Référence : **CXN-2024-6949**

yuno By xmco

3. ANNEXE

Synthèse des opérations marquantes de luttre contre le cybercrime en 2024 et traitées dans Yuno.

Synthèse des opérations marquantes de lutte contre le cybercrime en 2024

traitées dans Yuno

Ressources ciblées	Description	Temporalité	Référence
Infrastructures	Opération Synergia d'Interpol	Février	CXN-2024-0673
Infrastructures	Saisie de l'infrastructure de LockBit	Février	CXN-2024-1011
MaaS	Démantèlement de Warzone RAT	Février	CXN-2024-0835
Ressources humaines	Arrestation des opérateurs de SugarLocker	Février	CXN-2024-1037
Marketplace	Saisie de la marketplace Crimemarket	Mars	CXN-2024-1250
Marketplace	Saisie de Nemesis Market	Mars	CXN-2024-1728
MaaS	Démantèlement de LabHost	Avril	CXN-2024-2348
Marketplace	Saisie de BreachForums	Mai	CXN-2024-2847
Infrastructures	Opération EndGame : IcedID, SystemBC, Pikabot, Smokeloader, Trickbot et Bumblebee	Mai	CXN-2024-3107
Infrastructures	Opération Morpheus contre des instances hébergeant Cobalt Strike	Juillet	CXN-2024-3834
Ransomware	Démantèlement du groupe Dispossessor	Août	CXN-2024-4582
Resosurces humaines	Arrestation d'un opérateur du RaaS Ransom Cartel	Août	CXN-2024-4634
Moyen de communication	Démantèlement de la plateforme de communication «Ghost»	Septembre	CXN-2024-5369
MaaS	Saisie des MaaS Redline et Meta	Octobre	CXN-2024-6202
Infrastructures	Saisie des infrastructures du kit de PaaS « ONNX »	Novembre	C XN-2024-6660
Ressources humaines	Extradition de l'administrateur de Phobos RaaS	Novembre	CXN-2024-6564
Infrastructures	Interpol démantèle 22 0000 adresses IP et arrête 41 personnes dans le cadre de l'opération Synergia II	Novembre	CXN-2024-6336
Marketplace	Démantèlement du site PopeyeTools	Décembre	CXN-2024-7029
Ressources financières	Démantèlement d'un réseau de blanchiment d'argent associé au groupe ransomware Ryuk	Décembre	CXN-2024-6919
Ressources humaines	Arrestation de Wazawaka, un opérateur de LockBit	Décembre	CXN-2024-6816

4. BIBLIOGRAPHIE

Bibliographie

[1] CERT-XMCO, «Prise de contrôle du système et contournement de sécurité via 2 vulnérabilités au sein de Connect Secure et Policy Secure Gateways,» 11 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-0185

[2] CERT-XMCO, «2 vulnérabilités 0-day exploitées dans Ivanti Connect Secure VPN par des acteurs chinois,» 11 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0187

[3] CERT-XMCO, «Distribution de malware personnalisés par des acteurs chinois via l'exploitation de deux 0-day dans Ivanti Connect Secure VPN,» 12 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0213

[4] CERT-XMCO, «Analyse technique du malware KrustyLoader distribué par APT UTA0178,» 31 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0557

[5] GitHub, «http/cves/2023/CVE-2023-46805.yaml,» 16 01 2024. [En ligne]. Available: https://github.com/projectdiscovery/nuclei-templates/blob/main/http/cves/2023/CVE-2023-46805.yaml

[6] CERT-XMCO, «Contournement de sécurité via une vulnérabilité au sein de Connect Secure et Policy Secure Gateways,» 19 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-0354

[7] CERT-XMCO, «Compromission de MITRE par un mode opératoire APT via les CVE-2023-46805 et CVE-2024-21887 dans Ivanti Connect Secure VPN,» 22 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2381

[8] CERT-XMCO, «Élévation de privilèges et contournement de sécurité via 2 vulnérabilités au sein de produits Ivanti (000090322),» 01 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-0583

[9] CERT-XMCO, «Élévation de privilèges et contournement de sécurité via 2 vulnérabilités au sein d'Ivanti Policy Secure (000090322),» 01 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-0611

[10] GitHub, «http/cves/2024/CVE-2024-21893.yaml,» 03 02 2024. [En ligne]. Available: https://github.com/projectdiscovery/nuclei-templates/blob/main/http/cves/2024/CVE-2024-21893.yaml

[11] CERT-XMCO, «Distribution d'une backdoor furtive nommée DSLog via l'exploitation de la CVE-2024-21893 dans les produits Ivanti,» 13 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0823

[12] CERT-XMCO, «Prise de contrôle du système via une vulnérabilité au sein de Palo Alto GlobalProtect,» 12 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-2128

[13] CERT-XMCO, «Exploitation de la vulnérabilité 0-Day CVE-2024-3400 dans Palo Alto Networks par l'APT UTA0218,» 15 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2173

[14] GitHub, «nuclei-templates/http/cves/2024 /CVE-2024-3400.yaml,» 16 04 2024. [En ligne]. Available: https://github.com/projectdiscovery/nuclei-templates/blob/main/http/cves/2024/CVE-2024-3400.yaml

[15] CERT-XMCO, «Rapport conjoint de la CISA, du FBI et du DC3 sur la collaboration de l'Iran avec des opérateurs de ransomware,» 30 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4933

[16] CERT-XMCO, «Prise de contrôle du système via une vulnérabilité au sein de Palo Alto GlobalProtect,» 23 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-2417

[17] CERT-XMCO, «Exploitation de vulnérabilités affectant des dispositifs réseau par l'APT TAG-100 pour distribuer plusieurs malware à des fins d'espionnage,» 17 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4105

[18] CERT-XMCO, «Manipulation de données et divulgation d'informations via une vulnérabilité au sein de FortiClientEMS (FG-IR-24-007),» 14 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-1464

[19] CERT-XMCO, «Manipulation de données et divulgation d'informations via une vulnérabilité au sein de FortiClientEMS,» 22 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-1704

[20] CERT-XMCO, «Rapport sur les tactiques, techniques et procédures employées par le groupe de RaaS RansomHub (ex Knight),» 30 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4934

[21] CERT-XMCO, «Analyse des tactiques, techniques et procédures employées par les opérateurs du Ransomware-as-a-Service Medusa,» 12 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5218

[22] CERT-XMCO, «Résumé du Patch Tuesday de Microsoft (2024-Feb),» 14 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0882

[23] CERT-XMCO, «Le groupe APT Water Hydra exploite la CVE-2024-21412 dans Microsoft Defender SmartScreen pour cibler des entités financières,» 14 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0857

[24] CERT-XMCO, «Distribution du loader DarkGate par APT Water Hydra tirant parti de la CVE-2024-21412 dans Microsoft Windows SmartScreen,» 14 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1484

[25] CERT-XMCO, «Une campagne de phishing exploite la CVE-2024-21412 dans Windows SmartScreen pour distribuer des infostealers,» 08 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3864

[26] CERT-XMCO, «Distribution de Meduza Stealer et d'ACR Stealer via la CVE-2024-21412 affectant Windows SmartScreen de Microsoft,» 25 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4287

[27] CERT-XMCO, «Bilan du CERT-XMCO sur les menaces ayant ciblé les Jeux Olympiques de Paris 2024,» 17 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5256

[28] CERT-XMCO, «L'ANSSI partage des marqueurs liés à des attaques par wiper associées aux groupes APT russes Sandworm et UAC-0099,» 12 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4028

[29] CERT-XMCO, «Publication d'un guide sur les menaces informationnelles dans le cadre des Jeux olympiques 2024,» 21 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3571

[30] CERT-XMCO, «Rapport de l'ANSSI sur l'anticipation des menaces ciblant la France en marge des évènements sportifs de 2024,» 18 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2311

[31] CERT-XMCO, «Le forum cybercriminel BreachForums saisi par une opération policière internationale,» 17 Mai 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2847

[32] CERT-XMCO, «Un acteur malveillant revendique la compromission de données relatives à SFR sur BreachForums,» 18 Novembre 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6523

[33] CERT-XMCO, «Un acteur malveillant revendique la compromission de données médicales de 750 000 patients en France,» 21 Novembre 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6617
[34] CERT-XMCO, «Saisie de l'infrastructure du ransomware LockBit via une opération policière internationale,» 20 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1011
[35] CERT-XMCO, «Publication d'un outil de déchiffrement et de nouvelles informations relatives à la saisie des infrastructures de LockBit,» 21 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1043.
[36] CERT-XMCO, «Analyse des opérations du groupe LockBit et de la nouvelle version du ransomware baptisée LockBit-NG-Dev,» 22 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1072.
[37] CERT-XMCO, «Le groupe ransomware LockBit relance ses opérations et publie de nouvelles victimes,» 26 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1132.
[38] CERT-XMCO, «Des groupes de RaaS profitent de la saisie des infrastructures LockBit et ALPHV/BlackCat pour recruter de nouveaux affiliés,» 21 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1660.
[39] CERT-XMCO, «Arrestation de Mikhaïl Pavlovitch Matveyev, l'un des principaux opérateurs du groupe criminel de RaaS LockBit,» 02 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6816.
[40] CERT-XMCO, «Exit scam de l'opérateur de la franchise de Ransomware-as-a-Service ALPHV/BlackCat,» 06 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1295.
[41] CERT-XMCO, «Les autorités américaines saisissent l'infrastructure du ransomware ALPHV/BlackCat,» 20 12 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7039.
[42] CERT-XMCO, «Le mode opératoire Scattered Spider, ancien affilié de BlackCat/ALPHV, désormais associé au groupe ransomware RansomHub,» 13 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3409.
[43] CERT-XMCO, «Le mode opératoire CosmicBeetle est soupçonné d'être affilié au groupe de Ransomware-as-a-Service RansomHub,» 11 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5152.
[44] CERT-XMCO, «Analyse du groupe de Ransomware-as-a-Service RansomHub,» 28 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4902.
[45] CERT-XMCO, «Observatoire des ransomware - Novembre 2024,» 05 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6869.
[46] CERT-XMCO, «Le collectif criminel LockBit annonce la 4ème version de son programme de Ransomware-as-a-Service,» 19 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7186.
[47] CERT-XMCO, «APT Volt Typhoon distribue KV-botnet dans le cadre d'une campagne d'attaques ciblant des dispositifs IoT,» 14 12 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6919.
[48] Policia Nacional, «Detenido en Palma de Mallorca un joven ciberestafador responsable del ataque informático a 45 empresas de Estados Unidos,» 14 06 2024. [En ligne]. Available: https://www.policia.es/_es/comunicacion_prensa_detalle.php?ID=16236#.
[49] CERT-XMCO, «Arrestation des opérateurs du RaaS SugarLocker par les autorités russes,» 21 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1037.
[50] CERT-XMCO, «Le groupe de ransomware Termite revendique la compromission de la société américaine Blue Yonder,» 09 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6964.
[51] CERT-XMCO, «Compromission par Rhysida de l'agence gouvernementale américaine chargée de la supervision du port maritime et de l'aéroport de Seattle,» 16 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5267.
[52] CERT-XMCO, «Compromission de l'hôpital de Cannes - Simone Veil par LockBit 3.0,» 02 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2582.
[53] CERT-XMXO, «Compromission du Centre Hospitalier d'Armentières par le ransomware Blackout,» 28 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1177.
[54] CERT-XMCO, «La division chargée du développement durable chez Schneider Electric a été compromise par un ransomware,» 30 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0551.
[55] CERT-XMCO, «Le ransomware Cactus revendique la compromission de Schneider Electric et publie des échantillons des données volées,» 0 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1004.
[56] CERT-XMCO, «Le groupe criminel Hellcat revendique la compromission de 40GB de données liées à Schneider Electric,» 05 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6294.
[57] CERT-XMCO, «Hive revendique une attaque contre Intersport France,» 06 12 2022. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2022-5871.
[58] CERT-XMCO, «Confirmation des liens entre le ransomware Hunters International et Hive,» 13 11 2023 [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6175.
[59] CERT-XMCO, «Le groupe de ransomware Hunters International revendique la compromission d'Intersport,» 04 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1941.
[60] CERT-XMCO, «Revendication de compromission de la Réunion des musées nationaux - Grand Palais par le groupe ransomware Brain Cipher,» 30 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4936.
[61] CERT-XMCO, «Précisions sur la compromission par ransomware du Grand Palais de Paris,» 07 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4491.
[62] CERT-XMCO, «L'université Paris-Saclay aurait été compromise par un ransomware,» 13 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4580.
[63] CERT-XMCO, «Le groupe criminel RansomHouse a revendiqué la compromission de l'Université Paris Saclay,» 09 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5764.
[64] CERT-XMCO, «Le groupe ransomware Qilin revendique la compromission du fournisseur de logiciels français Groupe Althays,» 04 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6284.
[65] CERT-XMCO, «Le groupe de ransomware Termite revendique la compromission du département français de la Réunion,» 20 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6579.
[66] CERT-XMCO, «Le groupe de ransomware Hunters International revendique la compromission du fournisseur français Ecritel,» 17 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7147.

[67] CERT-XMCO, «Le groupe de Ransomware-as-a-Service Cicada3301 revendique la compromission de données relatives aux concessions Peugeot,» 16 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7127.
[68] CERT-XMCO, «Revendication par le groupe ransomware SpaceBears de la compromission d'Atos,» 30 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7306.
[69] CERT-XMCO, «Les quinze vulnérabilités les plus couramment exploitées en 2023 selon plusieurs agences de cybersécurité,» 14 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6481.
[70] CERT-XMCO, «Correction de 9 vulnérabilités 0-day dans le cadre du Patch Tuesday, dont 6 activement exploitées par des acteurs de la menace,» 14 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4613.
[71] CERT-XMCO, «Exploitation d'une vulnérabilité 0-day référencée CVE-2023-51467 affectant Apache OFBiz,» 03 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0045.
[72] CERT-XMCO, «Opération Lunar Peek : Exploitation massive des CVE-2024-0012 et CVE-2024-9474 affectant Palo Alto Interface Management,» 22 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6654.
[73] CERT-XMCO, «Exploitation de la 0-day CVE-2024-20399 dans Cisco NX-OS par le groupe chinois APT Velvet Ant,» 02 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3773.
[74] CERT-XMCO, «Exploitation d'une vulnérabilité 0-day (CVE-2024-50623) au sein des produits Cleo par le groupe de ransomware Termite,» 11 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7001.
[75] CERT-XMCO, «Exploitation de CVE-2024-26169 affectant Windows par le groupe Cardinal afin de distribuer Black Basta,» 13 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3406.
[76] CERT-XMCO, «Exploitation d'une vulnérabilité 0-day affectant Windows AppLocker par l'APT nord-coréen Lazarus,» 01 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1208.
[77] CERT-XMCO, «Exploitation de la CVE-2024-40711 dans Veeam par STAC 5881 pour distribuer le nouveau ransomware Frag,» 12 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6413.
[78] CERT-XMCO, «Exploitation massive de la CVE-2024-34102 dans Adobe Commerce pour voler les informations de paiement des utilisateurs de sites de e-commerce,» 03 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5621.
[79] CERT-XMCO, «Exploitation de la CVE-2024-40766 affectant SonicWall par le groupe ransomware Akira,» 10 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5138.
[80] CERT-XMCO, «Exploitation active d'une vulnérabilité critique au sein WhatsUp Gold de Progress (CVE-2024-4885),» 08 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4505.
[81] CERT-XMCO, «Exploitation active de la CVE-2024-8069 au sein de produits Citrix Virtual Apps and Desktops,» 13 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6416.
[82] CERT-XMCO, «Exploitation de la vulnérabilité corrigée CVE-2024-40711 affectant Veeam pour déployer les ransomware Akira et Fog,» 11 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5819.
[83] CERT-XMCO, «Exploitation active de la CVE-2024-45519 dans Zimbra,» 02 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5597.
[84] CERT-XMCO, «Exploitation active des CVE-2024-6670 et CVE-2024-6671 dans WhatsUp Gold,» 13 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5227.
[85] CERT-XMCO, «Exploitation active de la CVE-2024-27198 dans JetBrains TeamCity,» 07 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1322.
[86] CERT-XMCO, «Distribution de la backdoor GO par le groupe Bianlian via l'exploitation de vulnérabilités affectant Jetbrains TeamCity,» 12 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1404.
[87] CERT-XMCO, «Exploitation des CVE-2024-27198 et CVE-2024-27199 affectant JetBrains TeamCity pour distribuer de multiples malware,» 20 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1633.
[88] CERT-XMCO, «Analyse des nouvelles TTPs du groupe de Ransomware-as-a-Service Akira,» 22 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6077.
[89] CERT-XMCO, «Exploitation active des vulnérabilités critiques CVE-2024-38812 et CVE-2024-38813 au sein de VMware vCenter Server,» 19 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6549.
[90] CERT-XMCO, «Des acteurs de la menace exploitent la CVE-2017-0199 pour distribuer Remcos RAT,» 12 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6409.
[91] CERT-XMCO, «Distribution d'Agent Tesla et de Taskun contre le secteur de l'éducation et des entités gouvernementales aux États-Unis,» 06 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2560.
[92] CERT-XMCO, «Une panne affectant le logiciel Crowdstrike Falcon perturbe les opérations de nombreuses organisations dans le monde,» 19 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4203.
[93] CERT-XMCO, «Prise de contrôle du système et divulgation d'informations via 2 vulnérabilités au sein de Jenkins,» 25 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-0486.
[94] CERT-XMCO, «Divulgation d'informations via une vulnérabilité au sein de Jenkins,» 29 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-0527.
[95] CERT-XMCO, «Exploitation de la CVE-2024-23897 affectant Jenkins par Intelbroker pour compromettre Born Group dans une attaque supply chain,» 25 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4291.
[96] CloudSek, «Major Payment Disruption: Ransomware Strikes Indian Banking Infrastructure,» 01 08 2024. [En ligne]. Available: https://www.cloudsek.com/blog/major-payment-disruption-ransomware-strikes-indian-banking-infrastructure.
[97] CERT-XMCO, «RETEX du CERT-FR sur les vulnérabilités activement exploitées sur les équipements de sécurité,» 13 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3410.
[98] CERT-XMCO, «Campagne d'espionnage du groupe UAT4356 exploitant les CVE-2024-20353 et CVE-2024-20359,» 25 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2473.
[99] CERT-XMCO, «Exploitation de la CVE-2023-46747 dans F5 BIG-IP et de la CVE-2024-1709 affectant ScreenConnect par UNC5174, attribué à la Chine,» 25 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1730.
[100] CERT-XMCO, «Un groupe APT chinois cible des instances du ministère de la Défense néerlandais avec la CVE-2022-42475 dans FortiGate,» 07 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0712.
[101] CERT-XMCO, «Le groupe APT nord-coréen Kimsuky exploite les CVE-2024-1708 et CVE-2024-1709 dans ScreenConnect,» 05 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1270.

[102] CERT-XMCO, «Exploitation active de deux vulnérabilités critiques affectant ScreenConnect,» 22 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1075.
[103] CERT-XMCO, «Exploitation de vulnérabilités affectant ScreenConnect pour déployer Black Basta, Bl00dy et XWorm,» 28 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1188.
[104] CERT-XMCO, «Le groupe de RaaS BlackByte exploite la CVE-2024-37085 dans VMware ESXi,» 29 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4924.
[105] CERT-XMCO, «Exploitation de la CVE-2024-37085 dans les hyperviseurs ESXi par des opérateurs de ransomware,» 30 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4345.
[106] CERT-XMCO, «Distribution de code malveillant dans la bibliothèque de compression de données XZ Utils,» 15 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2180.
[107] CERT-XMCO, «Le groupe de ransomware Cl0p revendique la compromission de 66 organisations suite à l'exploitation d'une 0-day dans les produits Cleo,» 26 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7268.
[108] CERT-XMCO, «Le fournisseur de SaaS BeyondTrust a fait l'objet d'une intrusion via les CVE-2024-12356 et CVE-2024-12686,» 20 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7211.
[109] CERT-XMCO, «Prise de contrôle du système et manipulation de données via 2 vulnérabilités au sein de produits Beyond Trust (BT24-10 / BT24-11,» 20 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXA-2024-7223.
[110] CERT-XMCO, «Compromission du département du Trésor américain par un groupe APT lié à la chine via son fournisseur tiers BeyondTrust,» 31 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7316.
[111] CERT-XMCO, «Exploitation de la vulnérabilité CVE-2024-11667 dans les pare-feu Zyxel par le groupe ransomware Helldown,» 29 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6797.
[112] CERT-XMCO, «Le ransomware BlackBasta utilise des techniques d'ingénierie sociale via Microsoft Teams pour compromettre ses victimes,» 28 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6179.
[113] CERT-XMCO, «Analyse du groupe criminel de Ransomware-as-a-Service Cicada3301,» 18 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6015.
[114] CERT-XMCO, «Storm-0501 distribue le ransomware Embargo via l'exploitation de vulnérabilités corrigées,» 30 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5542.
[115] CERT-XMCO, «Analyse du groupe de Ransomware-as-a-Service Mallox (aka Tohnichi, Fargo et TargetCompany),» 17 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5299.
[116] CERT-XMCO, «Le groupe de ransomware Helldown développe une variante Linux et exploite des failles non documentées dans les pare-feu Zyxel,» 19 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6560.
[117] CERT-XMCO, «Une campagne de phishing et de malvertising distribue PikaBot, notamment en France,» 18 12 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6981.
[118] CERT-XMCO, «Le groupe criminel Cl0p pourrait être responsable de l'exploitation de la 0-day CVE-2024-50623 dans les produits Cleo,» 16 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7117.
[119] CERT-XMCO, «Retour sur l'exploitation de la «0-day» dans MOVEit Transfer par le groupe de ransomware Cl0p,» 12 06 2023. En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-3045.
[120] CERT-XMCO, «Des affiliés du ransomware Cl0p affirment avoir compromis le SI de 130 organisations en exploitant la faille 0-day affectant GoAnywhere MFT,» 16 02 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-0838.
[121] CERT-XMCO, «Analyse d'une double attaque par le groupe de ransomware Cactus,» 01 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1219.
[122] CERT-XMCO, «Le ransomware Agenda cible des hyperviseurs VMWare vCenters et ESXi via un script PowerShell personnalisé,» 27 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1794.
[123] CERT-XMCO, «Le groupe TargetCompany déploie la variante Linux de son ransomware dans une campagne ciblant les environnements ESXi en Asie,» 06 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3251.
[124] CERT-XMCO, «Les opérateurs du groupe RansomHub désactivent les systèmes EDR avec le loader EDRKillShifter,» 16 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4661.
[125] CERT-XMCO, «Utilisation de l'outil EDRKillShifter pour désactiver les EDR par le groupe de ransomware RansomHub,» 23 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5418.
[126] CERT-XMCO, «Le programme de RaaS Embargo exploite un toolkit sophistiqué incluant un EDR killer,» 24 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6128.
[127] CERT-XMCO, «Le ransomware Medusa exploite de nouvelles TTPs,» 15 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0227.
[128] CERT-XMCO, «Rapport sur le groupe de ransomware BianLian et son nouveau schéma d'extorsion,» 24 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0442.
[129] CERT-XMCO, «Le groupe Muddled Libra cible des environnements cloud et des SaaS à des fins d'extorsion,» 11 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2103.
[130] CERT-XMCO, «Arrestation de Maksim Silnikau, opérateur du RaaS Ransom Cartel et d'une vaste opération de malvertising,» 14 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4634.
[131] CERT-XMCO, «Le département de la Justice américain annonce l'extradition d'Evgenii Ptitsyn, l'administrateur du RaaS Phobos,» 19 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6564.
[132] Germany, BKA -, «Cybercrime: Erfolgreicher Schlag gegen die Infrastruktur von digitalen Geldwäschern der Underground Economy,» 11 09 2024. [En ligne]. Available: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240919_PM_finalexchange.html.
[133] CERT-XMCO, «Publication d'un outil de déchiffrement pour le ransomware HomuWitch,» 23 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1101.
[134] CERT-XMCO, «Publication d'un outil de déchiffrement pour le ransomware DoNex,» 09 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3890.
[135] CERT-XMCO, «Le RaaS Lynx dispose de chevauchements de code source avec le ransomware INCRansom,» 11 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5824.
[136] CERT-XMCO, «Détection d'une nouvelle version du kit de Phishing-as-a-Service Tycoon 2FA,» 26 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1755.

[137] CERT-XMCO, «Le kit Phishing-as-a-Service V3B employé dans une campagne ciblant les clients des banques européennes,» 06 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3227.
[138] CERT-XMCO, «Le kit Phishing-as-a-Service ONNX Store employé dans une campagne ciblant les institutions financières,» 22 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3526.
[139] CERT-XMCO, «Détournement des services d'hébergement légitimes par des acteurs de la menace à des fins de phishing,» 09 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5753.
[140] CERT-XMCO, «L'infostealer Rhadamanthys est distribué via des publicités Google Ads usurpant des logiciels de travail collaboratif,» 04 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1943.
[141] CERT-XMCO, «Distribution de la backdoor CleanUpLoader via des campagnes de malvertising opérées par les affiliés de Rhysida,» 10 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5793.
[142] CERT-XMCO, «Distribution du Loader-as-a-Service FakeBat via des techniques de SEO poisoning et du malvertising,» 03 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3798.
[143] CERT-XMCO, «Distribution des infostealers Vidar et LummaC2 via des tutoriels YouTube factices,» 08 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1995.
[144] CERT-XMCO, «Saisie par Microsoft de 240 domaines frauduleux associés au programme de Phishing-as-a-Service ONNX,» 22 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6660.
[145] CERT-XMCO, «Des affiliés du ransomware Black Basta distribuent le loader Pikabot via des campagnes de phishing,» 10 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0136.
[146] CERT-XMCO, «Analyse technique du loader Matanbuchus commercialisé sur le forum criminel Exploit,» 07 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2644.
[147] CERT-XMCO, «Détection d'une campagne d'attaques exploitant IDAT Loader et BruteRatel C4,» 29 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1855.
[148] CERT-XMCO, «Le malware HijackLoader disposerait de nouveaux modules d'évasion,» 07 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2634.
[149] CERT-XMCO, «Analyse de l'outil de red team EDRKillShifter employé par des acteurs malveillants afin de contourner les solutions de sécurité EDR,» 16 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5964.
[150] CERT-XMCO, «Opération Kraken: démantèlement de la plateforme de communication criminelle «Ghost» par Europol,» 19 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5369.
[151] CERT-XMCO, «L'opération internationale MORPHEUS conduit au démantèlement d'instances malveillantes hébergeant Cobalt Strike,» 04 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3834.
[152] CERT-XMCO, «Démantèlement de la plateforme de Phishing-as-a-Service LabHost,» 19 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2348.
[153] CERT-XMCO, «Démantèlement de l'infrastructure de Warzone RAT,» 14 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0835.
[154] CERT-XMCO, «Europol annonce le démantèlement d'une centaine de serveurs associés à plusieurs Malware-as-a-Service,» 30 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3107.
[155] CERT-XMCO, «Saisie des infrastructures des Infostealers-as-a-Service Redline et Meta dans le cadre de l'Opération Magnus,» 29 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6202.
[156] CERT-XMCO, «Les opérateurs des infostealer RedLine et Vidar distribuent désormais des ransomware,» 20 09 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5034.
[157] CERT-XMCO, «https://leportail.xmco.fr/watch/advisory/CXN-2023-4897,» 13 09 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-4897.
[158] CERT-XMCO, «Une campagne d'attaques distribue l'infostealer Lumma via des CAPTCHA malveillants,» 23 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6104.
[159] CERT-XMCO, «Distribution d'Atomic Stealer via le malvertising d'une version MacOS de Microsoft Teams,» 15 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4056.
[160] CERT-XMCO, «Une campagne de phishing distribue Smoke Loader à Taïwan via l'exploitation des CVE-2017-0199 et CVE-2017-11882 au sein de Microsoft Office,» 03 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6851.
[161] CERT-XMCO, «Campagne d'espionnage de l'APT chinois CeranaKeeper ciblant les institutions gouvernementales en Thaïlande,» 03 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5625.
[162] CERT-XMCO, «Identification d'une campagne d'espionnage chinoise multisectorielle en Asie du Sud-Est,» 12 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7059.
[163] CERT-XMCO, «Détection d'une nouvelle variante du loader Pikabot,» 26 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1125.
[164] CERT-XMCO, «Détection d'une nouvelle version du loader Pikabot,» 14 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0878.
[165] CERT-XMCO, «Une nouvelle version du Malware-as-a-Service Zloader améliore ses capacités d'évasion,» 03 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2603.
[166] CERT-XMCO, «Connexion des services d'hébergement bulletproof SecureHost et BEARHOST aux AS PROSPERO (AS200593) et Proton66 (AS198953),» 22 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6655.
[167] CERT-XMCO, «Le groupe criminel FIN7 aurait recours au service d'hébergement Stark Industries pour ses campagnes de spearphishin,» 16 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4675.
[168] CERT-XMCO, «Le CERT-UA identifie une campagne de phishing du groupe russe APT29 en Europe via l'usurpation du service légitime Amazon Web Services,» 28 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6183.
[169] CERT-XMCO, «Le groupe russe APT29 distribue à grande échelle des fichiers RDP à des fins de spearphishing en Europe, au Japon et en Australie,» 30 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6220.
[170] CERT-XMCO, «Le groupe russe APT29 cible des partis politiques allemands avec WINELOADER,» 25 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1724.
[171] CERT-XMCO, «Le groupe russe APT28 cible des institutions et partis politiques en Allemagne et en République tchèque,» 06 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2623.
[172] CERT-XMCO, «Une campagne de phishing nommée Diplomatic Orbiter et réalisée par l'APT russe Nobelium cible des entités diplomatiques notamment françaises,» 20 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3549.

[173] CERT-XMCO, «Compromisssion de routeurs Ubiquiti EdgeRouters par le groupe russe APT28 depuis 2022,» 28 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1175.
[174] CERT-XMCO, «Exploitation de l'Intelligence Artificielle par des APTs associées à la Russie, la Corée du Nord, l'Iran et la Chine,» 15 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0912.
[175] CERT-XMCO, «Campagne d'espionnage du groupe russe APT28 ciblant des organisations gouvernementales en Europe de l'Est,» 31 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0558.
[176] CERT-XMCO, «Campagne d'espionnage du groupe russe APT28 ciblant des personnels diplomatiques en Ukraine,» 05 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4455.
[177] CERT-XMCO, «Démantèlement du botnet Moobot, exploité par APT28 dans le cadre de ses opérations d'espionnage,» 16 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0938.
[178] CERT-XMCO, «Les autorités polonaises attribueraient la cyberattaque contre la Polska Agencja Prasowa au groupe russe APT28,» 04 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3836.
[179] CERT-XMCO, «La campagne de désinformation prorusse Matriochka cible les médias et la communauté des fact-checkers,» 10 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3287.
[180] CERT-XMCO, «Campagne de désinformation russe ciblant la Pologne,» 03 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3164.
[181] CERT-XMCO, «La campagne de désinformation russe Operation MiddleFloor cible les élections en Moldavie pour influencer l'opinion et préparer de futures campagnes de distribution de malware,» 10 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watchadvisory/CXN-2024-5787.
[182] CERT-XMCO, «La campagne de désinformation pro-russe Doppelgänger cible activement l'Allemagne à l'approche des échéances politiques,» 28 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1158.
[183] CERT-XMCO, «Intensification des opérations d'influence visant la France en marge des Jeux olympiques de 2024,» 04 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CCXN-2024-3191.
[184] CERT-XMCO, «Étude de la campagne de désinformation pro-russe Doppelgänger en marge des Jeux Olympiques de Paris 2024,» 26 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4297.
[185] CERT-XMCO, «La campagne d'influence pro-russe Doppelgänger s'appuie sur un réseau de fournisseurs de services d'hébergement opérant dans divers pays européens,» 15 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4053.
[186] CERT-XMCO, «Le réseau d'influence pro-russe CopyCop utilise l'Intelligence Artificielle à des fins de désinformation ciblant les pays occidentaux,» 15 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2701.
[187] CERT-XMCO, «Détection d'un réseau de bots opéré par Russia Today et développé à partir de l'outil Meliorator,» 10 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3941.
[188] CERT-XMCO, «Exploitation du wiper AcidPour par le groupe russe APT Sandworm pour cibler l'Ukraine,» 22 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1689.
[189] CERT-XMCO, «Les services de sécurité ukrainiens confirment l'implication du groupe APT russe Sandworm dans l'attaque ayant ciblé Kyïvsta,» 05 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0079.
[190] CERT-XMCO, «Retour sur la compromission de l'opérateur mobile ukrainien Kyïvstar revendiquée par des hacktivistes pro-russes,» 15 12 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-6953.
[191] CERT-XMCO, «Analyse technique du malware FrostyGoop ciblant des systèmes de contrôle industriels en Ukraine et en Roumanie,» 20 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6580.
[192] CERT-XMCO, «Détection du malware FrostyGoop, ciblant des systèmes de contrôle industriel en Ukraine à des fins de sabotage,» 24 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4259.
[193] CERT-XMCO, «Campagne de désinformation pro-chinoise ciblant Taïwan en marge des élections présidentielles de janvier 2024,» 27 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-7174.
[194] CERT-XMCO, «Google bloque 1000 comptes liés à la campagne d'influence chinoise GLASSBRIDGE,» 25 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6677.
[195] CERT-XMCO, «Analyse de la campagne SMUGX opérée par le groupe APT chinois Mustang Panda pour cibler l'Asie,» 22 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1074.
[196] CERT-XMCO, «Campagne d'attaques contre une université taïwanaise distribuant la nouvelle backdoor Msupedge,» 21 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4754.
[197] CERT-XMCO, «La firme de télécommunications taïwanaise Chunghwa Telecom victime d'un vol de données suite à une cyberattaque,» 05 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1272.
[198] CERT-XMCO, «Exploitation de la CVE-2018-0824 affectant Microsoft COM par le groupe APT41 associé à la Chine afin de compromettre un institut de recherche Taiwanais,» 02 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4428.
[199] CERT-XMCO, «Le groupe APT chinois Daggerfly cible des entités taïwanaises et américaines avec les backdoors Macma et Nightdoor,» 24 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4264.
[200] CERT-XMCO, «Le groupe APT chinois TIDRONE a ciblé l'industrie de fabrication de drones à Taïwan,» 09 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5099.
[201] CERT-XMCO, «Exploitation de la CVE-2024-36401 par le groupe chinois APT Earth Baxia à des fins d'espionnage en Asie-Pacifique,» 20 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5388.
[202] CERT-XMCO, «Le groupe chinois APT Earth Preta cible la région Asie-Pacifique à des fins d'espionnage,» 10 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5135.
[203] CERT-XMCO, «Distribution de nouvelles variantes de la backdoor Waterbear par l'APT Earth Hundun en Asie-Pacifique,» 12 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2132.
[204] CERT-XMCO, «L'entreprise I-Soon serait liée à de multiples groupes APT associées à la Chine,» 22 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1661.
[205] Cyberdéfense, Orange, «The hidden network,» 24 11 2024. [En ligne]. Available: https://research.cert.orangecyberdefense.com/hidden-network/report.html.
[206] SEKOIA, «A three beats waltz: The ecosystem behind Chinese state-sponsored cyber threats,» 13 11 2024. [En ligne]. Available: https://blog.sekoia.io/a-three-beats-waltz-the-ecosystem-behind-chinese-state-sponsored-cyber-threats/.

[207] CERT-XMCO, «Le mode opératoire Earth Lusca cible des instances gouvernementales en Asie et dans les Balkans,» 22 09 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-5077.
[208] CERT-XMCO, «Exploitation massive de la CVE-2022-42475 dans Fortigate par un APT chinois à des fins d'espionnage,» 12 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3339.
[209] CERT-XMCO, «La campagne chinoise Salt Typhoon cible les Fournisseurs d'Accès à Internet (FAI) américains à des fins d'espionnage,» 26 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5480.
[210] CERT-XMCO, «La CISA et le FBI dénoncent la compromission d'infrastructures de télécommunications par des acteurs affiliés à la Chine,» 28 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6167.
[211] CERT-XMCO, «Le groupe APT chinois MirrorFace a compromis une organisation diplomatique européenne avec des leurres de phishing sur le thème de l'Exposition universelle 2025,» 04 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6379.
[212] CERT-XMCO, «La Chine intensifie ses campagnes de cyberespionnage visant la Lituanie,» 12 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1410.
[213] CERT-XMCO, «La CISA propose des recommandations pour endiguer les opérations d'espionnage chinoises sur les infrastructures de télécommunications américaines,» 04 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6886.
[214] CERT-XMCO, «Le gouvernement américain envisagerait d'interdire les routeurs TP-Link à partir de 2025 en réponse aux activités d'espionnage parrainées par Pékin,» 19 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7196.
[215] CERT-XMCO, «Détection du nouvel implant Cyclops associé au mode opératoire iranien APT35 (aka Charming Kitten),» 14 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4643.
[216] CERT-XMCO, «Campagne de phishing distribuant AteraAgent par l'APT iranienne MuddyWater,» 25 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1731.
[217] CERT-XMCO, «Le groupe iranien APT Peach Sandstorm (aka APT33) distribue la nouvelle backdoor personnalisée Tickler,» 29 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4919.
[218] CERT-XMCO, «Le groupe APT iranien Charming Kitten cible des chercheurs en politique étrangère au Moyen-Orient,» 15 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0909.
[219] CERT-XMCO, «Le groupe APT associé à l'Iran Mint Sandstorm cible des organismes de recherche et des universités avec de nouvelles TTPs,» 18 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0347.
[220] CERT-XMCO, «Le groupe APT attribué à l'Iran UNC1549 cible les secteurs de l'aéronautique et de la défense au Moyen-Orient,» 28 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1178.
[221] CERT-XMCO, «Détection de la backdoor FalseFont du groupe APT iranien Curious Serpens ciblant les secteurs de la défense et de l'aérospatiale,» 25 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1699.
[222] CERT-XMCO, «Le groupe iranien APT42 cible des environnements Microsoft 365 à des fins d'espionnage,» 02 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2564.
[223] CERT-XMCO, «Campagne de phishing réalisée par APT42 associée à l'Iran ciblant les États-Unis et Israël,» 16 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4676.
[224] CERT-XMCO, «Exploitation de la CVE-2024-30088 par le groupe iranien APT34 pour distribuer la backdoor StealHook au Moyen-Orient,» 14 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5846.
[225] CERT-XMCO, «Avis de sécurité sur les opérations d'espionnage et d'influence associées à l'entreprise iranienne Emennet Pasargad,» 31 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6254.
[226] CERT-XMCO, «Usurpation de TTPs criminelles par des modes opératoires parrainés par l'Iran,» 31 05 2023. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2023-2773.
[227] CERT-XMCO, «Distribution du malware IOCONTROL par le groupe iranien CyberAv3ngers à des fins potentielles de sabotage,» 13 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7081.
[228] CERT-XMCO, «Analyse des opérations de sabotage et d'influence ciblant l'Albanie et Israël réalisées par l'APT iranien Void Manticore,» 21 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2899.
[229] CERT-XMCO, «Des campagnes de phishing exploitent la panne mondiale provoquée par Crowdstrike pour distribuer des malware aux clients impactés,» 22 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4221.
[230] CERT-XMCO, «Campagne d'attaques utilisant le nouveau wiper du groupe Handala,» 09 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5101.
[231] CERT-XMCO, «Opérations d'influence pro-iraniennes en marge du conflit dans la bande de Gaza,» 08 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0717.
[232] CERT-XMCO, «Des campagnes d'influence russe et iranienne ciblent la France en marge des élections législatives,» 01 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3739.
[233] CERT-XMCO, «Des opérations d'influence attribuées à la Russie et à l'Iran ciblent les élections présidentielles aux États-Unis,» 06 11 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6331.
[234] CERT-XMCO, «État de la menace des campagnes d'influence et de fraude ciblant des personnalités politiques à l'appui de deepfakes,» 30 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5543.
[235] CERT-XMCO, «L'APT nord-coréen BlueNoroff exploite le malware TodoSwift ciblant les instances macOS à des fins de vol de cryptomonnaies,» 22 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4783.
[236] CERT-XMCO, «Nouvelle campagne VMConnect réalisée par le groupe nord-coréen APT Lazarus ciblant des développeurs informatique,» 18 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5342.
[237] CERT-XMCO, «Analyse d'une nouvelle variante du malware FASTCash ciblant les systèmes Linux des institutions financières,» 15 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5867.
[238] CERT-XMCO, «Campagne d'attaques du groupe nord-coréen APT Lazarus ciblant des développeurs informatiques spécialisés dans la blockchain,» 05 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5035.
[239] CERT-XMCO, «Vol de 235 millions de dollars en crypto-actifs à l'entreprise WazirX par un groupe nord-coréen,» 22 Juillet 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4225.
[240] CERT-XMCO, «Le groupe APT nord-coréen Moonstone Sleet distribue le ransomware FakePenny,» 29 05 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3056.

[241] CERT-XMCO, «Le cluster APT nord-coréen Jumpy Pisces (aka Andariel) est soupçonné d'agir comme courtier d'accès initial pour le compte du groupe de ransomware Play,» 31 10 2024. [En ligne]. Available: https://bo.leportail.xmco.fr/watch/advisory/CXN-2024-6244.
[242] CERT-XMCO, «Le groupe APT nord-coréen Andariel cible les secteurs de la défense, de l'aérospatial et du nucléaire à des fins d'espionnage,» 26 07 2024. [En ligne]. Available: https://bo.leportail.xmco.fr/watch/advisory/CXN-2024-4309.
[243] CERT-XMCO, «Pyongyang poursuit sa collecte de renseignements d'intérêt militaire en Corée du Sud,» 13 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4581.
[244] CERT-XMCO, «Distribution de Troll Stealer par l'APT nord coréen Kimsuky en Corée du Sud,» 09 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0751.
[245] CERT-XMCO, «Le groupe nord-coréen APT Kimsuky cible des professeurs de sciences politiques sud-coréens à des fins d'espionnage,» 01 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3745.
[246] CERT-XMCO, «La police sud-coréenne dénonce les campagnes d'espionnage des groupes APT nord-coréens contre le secteur de la défense,» 25 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2482.
[247] CERT-XMCO, «Le groupe APT nord-coréen Lazarus a ciblé les personnels d'un centre nucléaire dans le cadre de l'Opération DreamJob,» 20 Décembre 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7226.
[248] CERT-XMCO, «Le groupe nord-coréen UNC2970 cible des professionnels de l'industrie aérospatiale via de fausses offres d'emploI,» 18 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5327.
[249] CERT-XMCO, «Distribution de la backdoor KONNI via un installer usurpant un logiciel exploité par les postes consulaires russes,» 23 02 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1094.
[250] CERT-XMCO, «Des travailleurs nord-coréens cherchent à obtenir des postes dans des entreprises occidentales afin de financer le régime et mener des opérations d'espionnage,» 24 09 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5440.
[251] CERT-XMCO, «Le groupe hacktiviste pro-russe NoName057(16) poursuit ses attaques DDoS contre les participants au Sommet sur la paix pour l'Ukraine,» 20 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3542.
[252] CERT-XMCO, «Plusieurs hacktivistes revendiquent des vols de données et des attaques DDoS contre des entités françaises,» 04 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1245.
[253] CERT-XMCO, «Le collectif hacktiviste pro-russe NoName057(16) revendique des attaques DDoS contre des entités publiques et privées françaises,» 31 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-7319.
[254] CERT-XMCO, «Campagne d'attaques de groupes hackvitistes prorusses contre la France à l'approche des Jeux Olympiques de Paris,» 16 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4068.
[255] CERT-XMCO, «Le groupe hacktiviste SN_BLACKMETA mène des attaques par DDoS en marge des Jeux olympiques de Paris 2024,» 05 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4442.
[256] CERT-XMCO, «Campagne d'opérations hacktivistes contre des entités françaises en réponse à l'arrestation du fondateur de Telegram,» 26 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4849.
[257] CERT-XMCO, «État des lieux des revendications d'attaques DDoS contre la France, en réponse à l'arrestation du fondateur de Telegram,» CERT-XMCO, 30 08 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-4930.
[258] CERT-XMCO, «Les groupes hacktivistes pro-russes, Holy League, NoName057(16), Anonymous Guys, Hunt3rKill3rs et UserSec ciblent des entités publiques et privées françaises,» 09 12 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6949.
[259] CERT-XMCO, «Le groupe hacktiviste pro-russe NoName057(16) revendique des attaques DDoS en soutien aux agriculteurs français,» 26 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0491.
[260] CERT-XMCO, «Des groupes hacktivistes prorusses revendiquent des attaques dans le cadre des élections européennes,» 07 06 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3272.
[261] CERT-XMCO, «Le groupe prorusse NoName057(16) cible la France via des attaques DDoS en amont des élections législatives,» 08 07 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-3861.
[262] CERT-XMCO, «Synthèse des opérations menées par le groupe russe APT44 (aka Sandworm),» 18 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2315.
[263] CERT-XMCO, «La société de télévision et de radiodiffusion d'État russe VGTRK a été ciblée par le groupe pro-ukrainien Sudo rm-RF,» 08 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-5707.
[264] CERT-XMCO, «Le groupe hacktiviste pro-ukrainien Blackjack revendique la compromission de Moscollector,» 16 04 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-2205.
[265] CERT-XMCO, «Le ministère de la Défense ukrainien confirme l'opération de sabotage de Planeta par les hacktivistes de BO Team,» 29 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0536.
[266] CERT-XMCO, «Le groupe hacktiviste pro-iranien Homeland Justice revendique une campagne d'attaques contre l'Albanie,» 02 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0014.
[267] CERT-XMCO, «Analyse de l'attaque du groupe hacktiviste pro-Iran Homeland Justice contre l'Albanie,» 08 01 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-0087.
[268] CERT-XMCO, «Le groupe hacktiviste pro-iranien Lord Nemesis divulgue les données d'établissements supérieurs israéliens,» 13 03 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-1440.
[269] CERT-XMCO, «Compromission d'un fournisseur israélien d'ESET pour réaliser une campagne de phishing afin de distribuer un wiper,» 21 10 2024. [En ligne]. Available: https://leportail.xmco.fr/watch/advisory/CXN-2024-6048.
[270] Tribunal Judiciaire de Paris, «Communiqué de presse - Arrestation Pavel Durov,» 26 08 2024. [En ligne]. Available: https://www.tribunal-de-paris.justice.fr/sites/default/files/2024-08/2024-08-26%20-%20CP%20TELEGRAM%20.pdf.
[271] L'Usine Digitale, «Après l'arrestation de Pavel Durov, Telegram va mieux modérer sa plateforme,» 06 09 2024. [En ligne]. Available: https://www.usine-digitale.fr/article/apres-l-arrestation-de-pavel-durov-telegram-va-mieux-moderer-sa-plateforme.N2218137.
[272] Telegram , «Du Rove's Channel,» 05 09 2024. [En ligne]. Available: https://t.me/durov/342.
[273] Security Affairs, «Russian media outlets Telegram channels blocked in European countries,» 02 01 2025. [En ligne]. Available: https://securityaffairs.com/172565/security/russian-media-outlets-telegram-channels-blocked-in-eu.html.
[274] Twitter, «Twitter account of Noname05716,» 03 01 2025. [En ligne]. Available: https://x.com/Noname05716.
[275] Twitter, «Twitter account sudormRF6,» 03 01 2025. [En ligne]. Available: https://x.com/sudormRF6.
[276] Twitter, «Twitter account Anonymous TV,» 03 01 2025. [En ligne]. Available: https://x.com/YourAnonTV.

À propos du

cert By xmco

Le CERT-XMCO met à votre disposition son équipe d'experts, afin de vous aider à protéger votre entreprise, en maitrisant votre exposition et en facilitant le maintien de votre niveau de sécurité.

Le CERT-XMCO est le CSIRT de la société XMCO. Il est reconnu par le CERT gouvernemental français (le CERT-FR), ainsi que par la TF-CSIRT et le Trusted Introducer, ce qui lui permet d'obtenir les informations et de collaborer avec les autres CERT français et européens.

Le CERT-XMCO protège votre entreprise, en maitrisant votre exposition et en facilitant le maintien de votre niveau de sécurité (veille en vulnérabilités, Cyber Threat-Intelligence, Réponse à Incident, Accompagnement à la remédiation, etc.).

À propos de

xmco

Cabinet de conseil indépendant en cybersécurité, XMCO a à coeur d'accompagner ses clients, de toute taille et de tous secteurs, dans l'anticipation des vulnérabilités, la détection des failles et la réponse à incidents. XMCO est qualifié PASSI sur l'ensemble des portées, ce qui confirme le coeur de métier historique : l'audit et les tests d'intrusion.

Date de création :	2002
Effectif salariés :	+100
Qualifications :	PASSI, QSA et CERT officiel
Clients actifs :	+450
dont clients CERT :	+100
Secteurs :	Banque, Assurance, Industrie, Institutions, Transports, Médias, Luxe, etc.

Renseignement :

info@xmco.fr

01 79 35 29 30

www.xmco.fr