RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

ANSSI

PANORAMA DE LA CYBERMENACE 2024

CERT-FR

MMXXIV

PANORAMA DE LA CYBERMENACE

INTRODUCTION

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité.

Le *Panorama de la cybermenace* est un document publié annuellement, couvrant une période allant du 1er janvier au 31 décembre de l'année précédente, dans lequel l'ANSSI revient sur les grandes tendances de la menace informatique ainsi que sur les éléments et incidents marquants dont elle a eu connaissance sur cette période.

Principalement destiné à la sphère institutionnelle et aux bénéficiaires de l'Agence, le *Panorama de la cybermenace* s'adresse également à la communauté française de la cybersécurité au sens large ainsi qu'aux partenaires internationaux de l'ANSSI.

Écrit du point de vue de l'ANSSI, il ne constitue pas une revue exhaustive de l'actualité de la cybersécurité française en 2024. Au-delà de son objectif de sensibilisation à la menace pesant sur la sécurité des systèmes d'information, le *Panorama* illustre également l'importance de l'application des mesures de sécurité.

Dans la continuité des années précédentes, l'ANSSI estime aujourd'hui que les attaquants liés à l'écosystème cybercriminel ou réputés liés à la Chine et la Russie constituent les trois principales menaces tant pour les systèmes d'information (SI) les plus critiques que pour l'écosystème national de manière systémique.

L'année 2024 a été marquée par l'organisation des Jeux Olympiques et Paralympiques de Paris (JOP 2024), dont l'exposition médiatique et la surface d'attaque ont constitué des opportunités majeures pour les attaquants. Dans ce cadre, l'ANSSI a observé des attaques à des fins d'extorsion et d'espionnage stratégique, et une majorité d'attaques à but de déstabilisation menées par des groupes *hacktivistes* sans qu'aucune de ces attaques ne porte atteinte au déroulement de l'événement.

L'année a également été marquée par le nombre et l'impact des vulnérabilités affectant les équipements de sécurité situés en bordure de SI : plus de la moitié des opérations de cyberdéfense de l'ANSSI, constituant son plus haut niveau d'engagement en réponse à incident, ont ainsi eu pour origine l'exploitation de vulnérabilités sur ces équipements.

Du point de vue des moyens mis en œuvre par les attaquants, l'ANSSI a constaté la poursuite des attaques visant la chaîne d'approvisionnement pour atteindre des cibles finales d'intérêt. Ces attaques, qui sont en constante expansion depuis la fin des années 2010, illustrent combien la maîtrise du SI, de ses interconnexions et de ses dépendances est un enjeu majeur pour les organisations.

En parallèle, l'utilisation des réseaux d'anonymisation par les attaquants se poursuit. Ces réseaux de machines compromises communiquant entre elles permettent à un attaquant de dissimuler ses actions et rendre difficile leur imputation, à toutes les étapes de l'attaque informatique. Ils constituent des infrastructures qui se développent, se complexifient et dont les utilisateurs ne sont pas toujours clairement identifiables. L'essor des entreprises privées de lutte informatique offensive (LIOP) se poursuit quant à lui avec la mise à disposition à un éventail relativement large de clients, de capacités qui étaient jusqu'alors l'apanage des États les plus avancés en matière cyber.

Les attaques par rançongiciel ont largement mobilisé les équipes de l'ANSSI en 2024 avec un nombre d'incidents comparable à l'année passée. Les attaques à but d'espionnage ont quant à elles été caractérisées par le ciblage soutenu d'équipements et d'infrastructures de télécommunications.

Enfin, en plus des attaques à but d'espionnage et d'extorsion, qui restent les plus importantes en termes d'investissement des équipes de l'ANSSI, 2024 a marqué une hausse des attaques à finalité de déstabilisation, notamment opérées par des groupes *hacktivistes*.

Que faire en cas de compromission ?

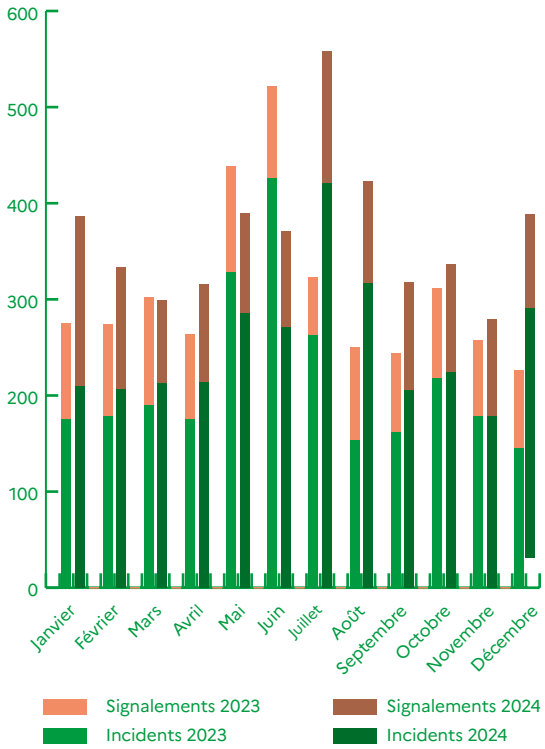
En cas de compromission ou de suspicion de compromission, le CERT-FR vous invite à prendre connaissance de cette page : *https://www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dintrusion-sur-un-systeme-dinformation/*

Le CERT-FR est joignable :
- Par téléphone :
→ depuis la France métropolitaine au 3218 (service gratuit + prix d'un appel) ou 09 70 83 32 18
→ depuis certaines collectivités territoriales situées en outre-mer ou depuis l'étranger au +33 9 70 83 32 18
- Par courriel :
→ à l'adresse *cert-fr@ssi.gouv.fr*

Comparatif du nombre d'incidents et signalements 2023/2024

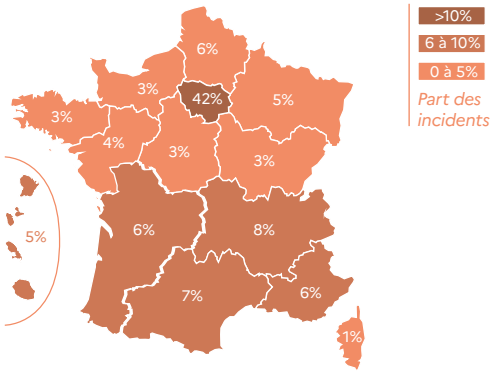
Au cours de l'année 2024, l'ANSSI a traité – avec un degré d'engagement variable – 4386 événements de sécurité[1], soit une augmentation de 15% par rapport à l'année 2023.

Ainsi, 3004 signalements[2] et 1361 incidents[3] ont été portés à la connaissance de l'ANSSI. Cette augmentation peut trouver une explication dans le contexte des JOP 2024, qui s'illustre par une hausse des signalements et des incidents à partir du mois de mai – date de l'arrivée de la flamme olympique en France – jusqu'à la cérémonie de clôture des Jeux Paralympiques en septembre, avec un pic de signalements atteint au mois de juillet.



Répartition par région des incidents traités par l'ANSSI

Une observation de la répartition par région des incidents traités par l'ANSSI au cours de l'année montre que la menace affecte tous les territoires mais reste proportionnelle à l'activité économique et aux usages numériques de chaque région.



Seuls les incidents ayant affecté des bénéficiaires qui sont présents uniquement dans ces territoires sont comptabilisés. À noter qu'un certain nombre de bénéficiaires de l'Agence ont leur siège social en région parisienne.

Capacités de détection de l'ANSSI

L'ANSSI opère un service de supervision au profit des ministères comprenant à la fois des moyens de détection réseau et système. En 2024, l'ANSSI a adressé 162 signalements aux institutions étatiques bénéficiant de ses services de détection. Ces signalements ont couvert majoritairement les domaines suivants[4] :

- Communications suspectes vers des infrastructures d'attaque, détectées à la fois en temps réel et à travers des recherches d'antécédents dans les journaux collectés ;
- Actions d'administration suspectes ou utilisation d'outils légitimes connus comme étant régulièrement détournés par des attaquants ;
- Exploitation ou tentative d'exploitation de vulnérabilités ;
- Campagnes d'hameçonnage ciblant certains ministères.

1 Événements portés à la connaissance de l'ANSSI et qui ont donné lieu à un traitement par les équipes opérationnelles.

2 Les signalements regroupent tous les comportements anormaux ou inattendus pouvant avoir un caractère malveillant ou ouvrir la voie à des usages néfastes à l'encontre d'un SI.

3 Un incident est un événement de sécurité où l'ANSSI est en mesure de confirmer qu'un acteur malveillant a conduit des actions avec succès sur le SI de la victime.

4 Les ministères disposant d'un service de détection traitent en complément les alertes de leurs systèmes d'information.

I

OPPORTUNITÉS POUR LES ATTAQUANTS

Cette année, en complément des traditionnelles faiblesses affectant le niveau de sécurité des SI et des vulnérabilités techniques faisant l'objet d'une attention accrue de la part de nombreux acteurs, les Jeux Olympiques et Paralympiques de Paris 2024 (JOP 2024) ont constitué une opportunité conjoncturelle de premier plan pour des acteurs aux motivations politiques.

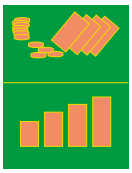
Pour les attaquants, qu'ils soient à la recherche d'une vitrine dans un contexte très médiatisé, ou qu'ils soient soutenus par des États cherchant à espionner ou à déstabiliser, les grands événements offrent des motivations et des opportunités supplémentaires pour agir.

Si en 2024 l'attention et les enjeux ont été principalement tournés vers les JOP 2024, l'année a aussi été marquée par plusieurs processus électoraux, notamment les élections européennes puis législatives en France pendant lesquelles aucune attaque majeure n'a été observée.

A
JEUX OLYMPIQUES ET PARALYMPIQUES DE PARIS 2024

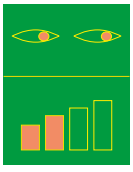
En raison de leur exposition mondiale et des flux financiers importants qu'ils génèrent, les JOP constituent une cible de choix pour des attaquants aux motivations diverses. Ceux-ci peuvent chercher à s'enrichir au travers d'activités cybercriminelles, perturber le déroulement de l'événement ou nuire à la réputation du pays hôte sur la scène internationale. En amont des JOP 2024, le Comité d'organisation des Jeux Olympiques (COJO) avait ainsi indiqué s'attendre à huit à dix fois plus de cyberattaques qu'aux Jeux de Tokyo et estimé que le niveau de la menace allait être multiplié par dix. Dans ce contexte tendu, l'ANSSI et l'ensemble des entités impliquées dans l'organisation des JOP 2024 ont mis en œuvre d'importants travaux de préparation [01].

Dans son évaluation de la menace ciblant les JOP 2024 [02], l'ANSSI avait anticipé :



• Un niveau **élevé** de menace à motivation lucrative : escroqueries « classiques », tentatives d'extorsion, vols de données ou attaques opportunistes tirant profit du besoin important de disponibilité des services informatiques ;

• Un niveau **important** de menace à visée de déstabilisation : attaques visant à perturber l'organisation des Jeux et attenter au bon déroulement des épreuves sportives, parmi lesquelles le sabotage informatique, mais aussi les attaques par déni de service distribué (DDoS), les défigurations de sites Web ou les divulgations de données ;



• Un niveau **moyen** de menace à but d'espionnage : attaques conduites par un acteur potentiellement soutenu par un État, ciblant par exemple une délégation étrangère ou un sous-traitant détenant des données sensibles.

Malgré une intensité élevée, aucune attaque informatique n'a perturbé le bon déroulement des JOP 2024. Comme attendu, des tentatives de déstabilisation, de l'espionnage et des attaques à but lucratif ont été observés.

• L'ANSSI n'a pas constaté de ciblage spécifique ou massif des JOP par des acteurs cybercriminels. Compte tenu du nombre d'entités liées aux JOP 2024, l'activité cybercriminelle a été habituelle et les attaques par rançongiciel observées pendant la période des Jeux n'ont pas eu d'incidence sur la tenue des épreuves.

Deux attaques majeures par rançongiciel ont été observées pendant cette période :

→ Début août 2024, le réseau du Grand Palais — Réunion des Musées Nationaux (RMN) a été compromis au moyen du rançongiciel *BrainCipher*. Un logiciel commun à plusieurs musées a été rendu indisponible, mais la compromission n'a pas eu d'incidence sur la tenue des épreuves se déroulant dans l'enceinte du site d'épreuves du Grand Palais, entité distincte du Grand Palais RMN. Le réseau affecté ne possédait pas d'interconnexion avec les SI permettant la tenue des épreuves.

→ Le 11 août, l'Université Paris-Saclay a contacté l'ANSSI pour signaler sa compromission par le rançongiciel *WhiteRabbit*. Le laboratoire antidopage français (LADF), hébergé au sein de l'université a, à cette occasion, fait l'objet d'une attention particulière par l'ensemble des parties prenantes. Toutefois, le cloisonnement des SI et la mise en œuvre rapide de mesures de secours ont permis de préserver l'intégrité des analyses et d'assurer la poursuite des activités du laboratoire pendant les Jeux Paralympiques.

• Des opérations de déstabilisation ont été observées par l'ANSSI pendant toute la période des JOP 2024. Ces actions ont été principalement menées par des groupes *hacktivistes* pro-russes et pro-palestiniens, dont certains pouvant être affiliés à des États, avec un recours constant à des attaques par DDoS et des revendications d'exfiltration de données.

Les attaquants ont exploité le contexte des JOP 2024 pour amplifier la portée médiatique de leurs actions, dans un contexte géopolitique dense : guerre en Ukraine, guerre au Proche-Orient et arrestation par la justice française de Pavel Durov, PDG et fondateur de la messagerie Telegram. Certaines revendications d'exfiltration de données ont concerné des entités liées à l'organisation des JOP 2024, sans que cela ne corresponde à des incidents significatifs. Le 31 juillet 2024, LulzSec Muslims a notamment revendiqué une exfiltration de données appartenant au Comité national olympique et sportif français (CNOSF). Le groupe justifiait son attaque en réaction à la cérémonie d'ouverture des JOP 2024.

À l'étranger, l'attaque à but de déstabilisation la plus remarquée fut l'exfiltration, en juillet 2024, de données de l'Agence antidopage polonaise POLADA (*Polish Anti-Doping Agency*) par les opérateurs du MOA réputé russe UNC1151. Le 6 août 2024, les données exfiltrées des SI de POLADA ont été divulguées par le groupe *hacktiviste* pro-russe Beregini, en coopération avec le groupe *hacktiviste* Zarya. Cette revendication visait à dénoncer la lutte contre le dopage comme un chantage à l'encontre des pays qui mènent une politique opposée à celle des États-Unis. Les données divulguées incluaient notamment des données personnelles et médicales d'athlètes, des contrôles antidopage échoués, des éléments d'enquête liés à des laboratoires chimiques illégaux, et des mots de passe. Le même mois, POLADA a déclaré que des informations relatives à des tests d'athlètes polonais divulgués avaient été manipulées, vraisemblablement à des fins de désinformation [03].

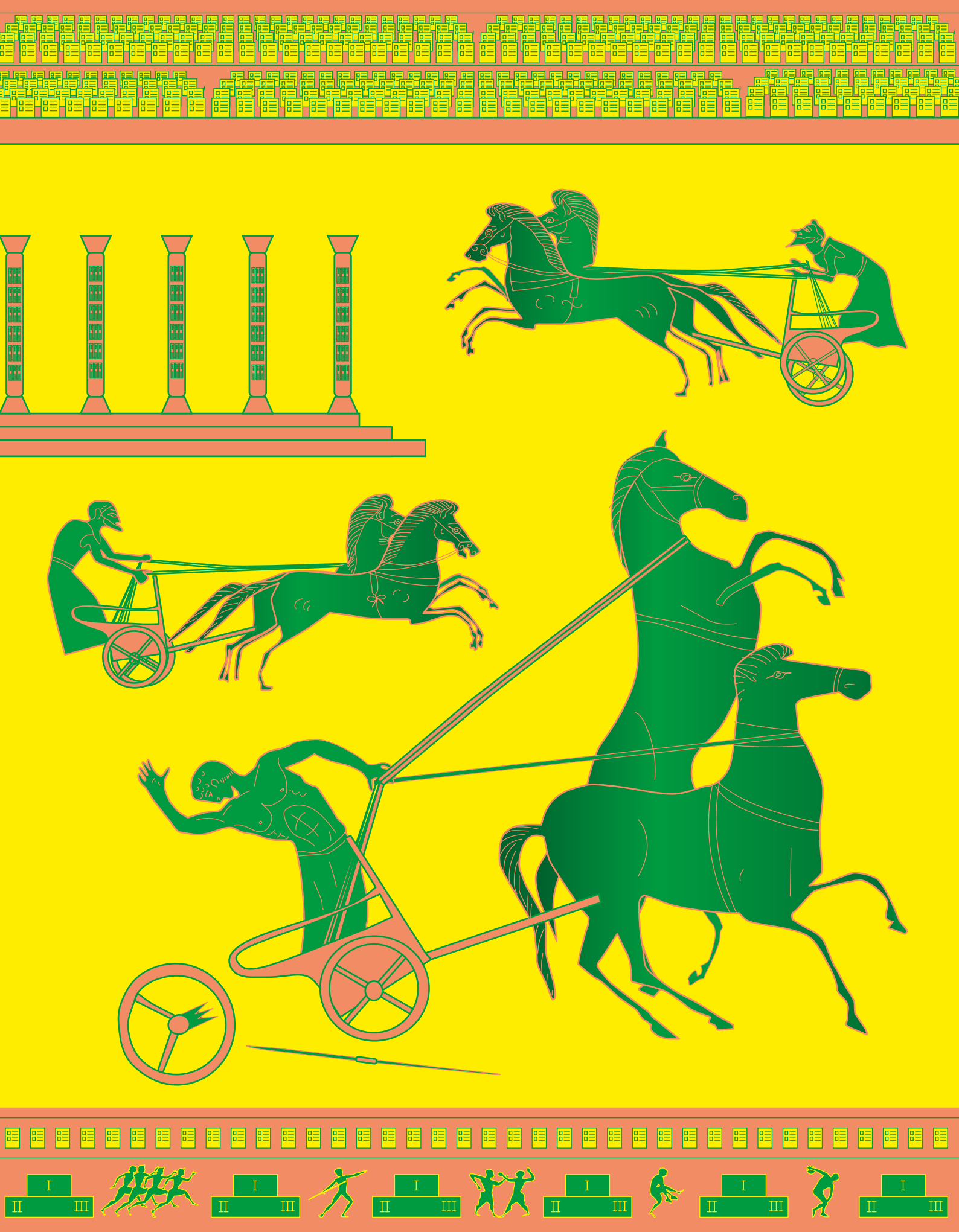
Tentative de déstabilisation dans le cadre des JOP 2024

Fin juillet, Viginum a identifié une opération d'influence et de déstabilisation à l'encontre des JOP 2024 et de la délégation israélienne à l'aide de profils *hacktivistes* réputés iraniens [04].

Dans ce cadre, une tentative notable de compromission à des fins de déstabilisation a été recensée : le 25 juillet 2024, la veille de la cérémonie d'ouverture des JOP 2024, l'ANSSI a été informée de la compromission d'une entreprise opérant la gestion de bornes d'affichage publicitaire. Le mode opératoire d'attaque (MOA) Haywire Kitten, opéré selon le FBI par l'entreprise iranienne Emennet Pasargad au profit du Corps des gardiens de la révolution islamique [05], aurait tenté, infructueusement, de détourner les bornes gérées par l'entreprise dans le but d'afficher des photomontages dénonçant la participation des athlètes israéliens aux JOP 2024. Une fois découverte, l'attaque a pu être rapidement enrayée grâce au travail de l'ensemble de l'écosystème français impliqué dans la cybersécurité des JOP 2024 [06].

- Même si l'ANSSI avait estimé possible la conduite d'opérations d'espionnage à l'encontre des JOP 2024, celles-ci ne représentaient pas de menace pour la bonne tenue des épreuves sportives dans la mesure où elles ne portaient atteinte ni à la disponibilité ni à l'intégrité des systèmes et des données.

L'ANSSI a traité la compromission d'une entité impliquée dans la tenue des JOP 2024 ciblée par une attaque à visée d'espionnage, probablement menée par un MOA réputé chinois. Les analyses de l'ANSSI ont mis en évidence des activités malveillantes datant d'au moins 2022, révélant un pré-positionnement de l'attaquant très en amont sur le SI de l'entité. Détectée avant le début des Jeux, cette intrusion n'a pas provoqué de perturbation sur leur déroulé.


I
II
III

B
FAIBLESSES TECHNIQUES

Si l'actualité et les grands événements offrent aux attaquants des moments propices pour agir, les faiblesses techniques exposées par les SI leur fournissent quant à elles des opportunités constantes. Comme les années précédentes, l'ANSSI observe ainsi que des attaquants aux compétences variables sont en mesure d'exploiter les vulnérabilités de SI dont le niveau de sécurité est insuffisant. Le durcissement des SI et leur maintien en condition de sécurité permettent de réduire la surface d'attaque et les opportunités de latéralisation suivant le principe de défense en profondeur[5].

1/ RAPPEL DU TRIPTYQUE DES BONNES PRATIQUES DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (SSI)

L'ANSSI rappelle que les bonnes pratiques pour protéger les SI et les maintenir en condition de sécurité se déclinent au travers des actions suivantes :

1. La sécurisation constitue la première ligne de défense. Elle vise à prévenir les attaques en réduisant l'exposition du SI et les possibilités de latéralisation, notamment au travers d'actions de durcissement, et à contraindre un attaquant à faire usage de techniques ou d'outils susceptibles de générer des événements journalisés ;
2. La supervision permet de détecter une activité malveillante au travers de l'analyse des journaux système, applicatifs ou réseau et de lever les alertes le plus tôt possible dans la progression d'un attaquant ;
3. La réponse à incident intervient en dernier lieu et comprend la gestion de crise, les investigations numériques et la remédiation. L'ANSSI a publié en 2024 trois guides dédiés aux volets stratégique, organisationnel et technique de la remédiation [07].

Les coûts de sécurisation du SI et de mise en place d'une supervision, qui permettent de limiter significativement le risque de survenue d'un incident de sécurité et de limiter sa gravité et son impact, sont souvent largement inférieurs à ceux de la remédiation.

2/ DURCISSEMENT DU SYSTÈME D'INFORMATION

L'ANSSI constate qu'un nombre important de ses bénéficiaires a recours à des produits ou services de détection d'incidents de sécurité. Toutefois, ces dispositifs n'atteignent leur plein potentiel que lorsque le SI a fait l'objet d'une sécurisation, avec en particulier l'application de mesures de défense en profondeur. D'une part, ces mesures permettent de ralentir la progression de l'attaquant et de réagir avant qu'il n'ait obtenu des privilèges élevés sur le SI, facilitant donc son éviction. D'autre part, elles rendent les tentatives de latéralisation plus complexes, générant ainsi de meilleures opportunités de détection. Enfin, elles permettent de limiter drastiquement les conséquences de la compromission du poste utilisateur, qui est par nature un élément très exposé du SI.

Selon ce principe, la priorité doit donc être donnée à la sécurisation de l'actif le plus critique du SI : l'annuaire d'authentification (ou le tenant dans le cas de l'utilisation de services nuagiques), le plus souvent un annuaire *Active Directory*[6].

S'il est essentiel, le durcissement de l'annuaire *Active Directory* ne permet pas de se prémunir de l'ensemble des attaques. Des incidents aboutissant au déploiement d'un rançongiciel ont notamment pu être observés dans les cas suivants :

- L'exploitation de la vulnérabilité *Zerologon* sur les contrôleurs de domaine *Active Directory* dont la version n'est pas à jour, permettant la compromission de l'ensemble du SI [08] ;
- L'absence de gestion du mot de passe du compte administrateur local des serveurs et postes de travail Windows, permettant également une latéralisation. Certaines solutions (comme le service LAPS de Microsoft) permettent de se prémunir de ce risque ;
- Le détournement de l'usage légitime d'applicatifs métier ou de gestion de parc mal configurés ou vulnérables (outils de sauvegarde, de déploiement de mises à jour ou de prise en main à distance,

5 Ces mesures peuvent inclure le durcissement des configurations, la mise en place de bonnes pratiques d'administration ou encore la mise en place de segmentation réseau.

6 L'annuaire *Active Directory*, centre névralgique de la sécurité des systèmes d'information Microsoft, est un élément critique permettant la gestion centralisée de comptes, de ressources et de permissions. L'obtention de privilèges élevés sur cet annuaire entraîne une prise de contrôle instantanée et complète de toutes les ressources ainsi administrées.

consoles antivirales ou EDR, etc.), permettant de compromettre une proportion significative d'un SI.

Le premier exemple illustre la nécessité de maintien en condition de sécurité des éléments critiques du SI. L'ANSSI constate qu'une part importante de ses bénéficiaires ayant un SI en environnement Microsoft dispose de serveurs et de postes de travail dans une version obsolète ou prochainement en fin de support :

- 82% des postes de travail[7] des organismes utilisateurs du service ADS de l'Agence utilisent le système d'exploitation Windows 10, dont la fin de support est prévue le 14 octobre 2025 (hors version LTSC et support étendu). L'ANSSI recommande d'initier les travaux de migration vers Windows 11 au plus tôt.
- 36% des serveurs Windows des organismes utilisateurs du service ADS se trouvent dans une version obsolète (Windows Server 2012R2 ou inférieur). L'ANSSI recommande de mettre à jour vers la version la plus récente du système d'exploitation afin de bénéficier de la plus grande période de support possible.

Parmi les mesures de défense en profondeur, la segmentation réseau interne est un moyen efficace pour réduire les possibilités de latéralisation de l'attaquant et faciliter la détection d'actions malveillantes. Elle peut notamment être mise en œuvre par l'utilisation de mécanismes réseau tel que le VLAN privé[8], associé à des règles de filtrage.

Les moyens d'authentification constituent également un élément central de la sécurisation du SI. L'ANSSI constate que certains moyens d'authentification comme le TOTP[9] ou l'utilisation d'une application tierce sont désormais contournés par les attaquants au moyen de nouvelles techniques (voir par exemple [09]). Il convient de préférer une authentification forte utilisant l'emploi de certificats ou de clés de sécurité.

Enfin, l'ANSSI rappelle l'importance de disposer de sauvegardes, y compris hors ligne. ←

Mauvaises pratiques systémiques de configuration des annuaires *Active Directory*

Les mauvaises pratiques de configuration des annuaires *Active Directory* décrites ci-dessous sont un point commun à de nombreux SI ayant été victimes d'attaques informatiques, en particulier de chiffrement par un rançongiciel. En effet, des outils largement disponibles permettent de faciliter leur exploitation.

- **Comptes privilégiés ayant l'attribut ServicePrincipalName (SPN) positionné :** L'attribut SPN permet d'associer des noms de service Kerberos[10] à des comptes *Active Directory*. Lorsqu'un compte possède un nom de service Kerberos, n'importe quel utilisateur authentifié peut demander un ticket Kerberos pour ce service, et ainsi réaliser une attaque par force brute pour obtenir le mot de passe du compte (attaque couramment appelée *Kerberoasting*). Compte tenu de ces risques, l'attribut SPN ne devrait être positionné que sur des comptes de service non privilégiés.
- **Comptes à hauts privilèges dont le mot de passe est inchangé depuis plus de 3 ans :** Les mots de passe des comptes à hauts privilèges doivent être changés à une fréquence régulière de maximum 3 ans pour que ces secrets soient connus uniquement par les administrateurs actuels. L'ANSSI constate régulièrement des mots de passe de comptes à hauts privilèges inchangés depuis 15, 20 voire 25 ans et dont la complexité ne répond pas aux exigences actuelles.
- **Permissions d'enrôlement sur les modèles ou conteneurs de certificats :** Ce type de vulnérabilité est lié à une mauvaise configuration de l'infrastructure de gestion de clé Microsoft AD-CS permettant de générer des certificats de sécurité. Ainsi, un demandeur peut générer un certificat valable pour l'authentification Windows pour n'importe quel compte de l'annuaire, y compris les comptes à hauts privilèges.
- **Permissions dangereuses :** Les permissions d'un compte non privilégié vers des membres de groupes privilégiés, vers les contrôleurs de domaine, vers la racine des *naming contexts* ou vers les objets de GPO s'appliquant aux membres des groupes privilégiés permettent à un attaquant qui compromettrait ce compte de prendre le contrôle d'un élément critique de l'annuaire, et ainsi compromettre l'ensemble du SI.

L'ensemble de ces vulnérabilités est vérifié par le service ADS (*https://club.ssi.gouv.fr*) proposé par l'ANSSI à ses bénéficiaires [10].

7 Disposant d'un support Microsoft.

8 *Private VLAN* ou PVLAN, technique de segmentation réseau qui permet de limiter les communications entre équipements reliés à un même commutateur.

9 TOTP : « *Time-based One-time Password* », mot de passe à usage unique basé sur le temps.

10 Kerberos est un protocole d'authentification reposant sur l'utilisation de tickets pour accéder à des services, couramment utilisé en environnement Microsoft.

C
VULNÉRABILITÉS EXPLOITÉES

L'exploitation de vulnérabilités, en particulier sur les équipements exposés sur Internet, est un des principaux vecteurs d'intrusion utilisés par les attaquants. L'année 2024 a ainsi été marquée par des campagnes d'exploitation massive de vulnérabilités affectant des équipements de sécurité situés en bordure de SI.

Le cadre légal a également évolué, avec la promulgation de la loi de programmation militaire 2024-2030, qui oblige notamment les éditeurs à signaler à l'ANSSI les vulnérabilités significatives découvertes dans leurs logiciels.

1 ÉQUIPEMENTS DE BORDURE ET DE SÉCURITÉ : DES CIBLES DE CHOIX

Dans la continuité de l'année 2023 [01], l'ANSSI a constaté en 2024 une intensification de l'exploitation de vulnérabilités affectant des équipements exposés sur Internet, parmi lesquels figurent des équipements de sécurité mis en place par de nombreuses entités pour sécuriser l'accès distant à leur SI (par exemple des pare-feux ou des passerelles VPN). Durant l'année 2024, l'ANSSI a eu connaissance de la compromission en France de plusieurs milliers d'équipements de bordure, et traité plusieurs dizaines d'incidents de sécurité liés à l'exploitation de vulnérabilités logicielles sur ces équipements qui constituent des cibles attractives pour les attaquants (voir focus page 14).

L'ANSSI observe que de nombreux acteurs réalisent des opérations de balayage réseau sur ces équipements à la recherche de vulnérabilités à exploiter. Ces scans, très réguliers et étendus, permettent de rechercher de manière systématique les équipements exposés qui n'ont pas été mis à jour et peuvent amener à des exploitations opportunistes de vulnérabilités. Afin de se protéger de leur exploitation, il importe donc d'appliquer les correctifs le plus rapidement possible.

En effet, les vulnérabilités affectant les équipements de sécurité en bordure de SI sont souvent exploitées dans un délai très court après leur publication, en raison de l'apparition de plus en plus rapide de preuves de concept ou de codes d'exploitation publics[11]. Or, l'ANSSI constate que des vulnérabilités sont encore exploitées par des attaquants plusieurs mois après la mise à disposition de correctifs.

Par exemple, l'ANSSI a traité en 2024 la compromission et le chiffrement par le biais d'un rançongiciel d'une entité du secteur des télécommunications. Un équipement de bordure – un pare-feu Palo Alto vulnérable à la CVE-2024-3400 (voir focus page 14) – a été la cible de multiples tentatives de connexions par les attaquants pendant plusieurs mois. Une fois l'équipement compromis, ceux-ci ont exploité cet accès pour se latéraliser sur le SI. L'incident a affecté le fonctionnement nominal de l'entité victime pendant plusieurs semaines et a nécessité de lourds travaux de reconstruction. Dans ce cas, il est à noter que l'exploitation de la vulnérabilité a eu lieu plus de deux mois après la publication d'un correctif par l'éditeur ainsi que d'une alerte par le CERT-FR.

Enfin, l'ANSSI a également traité plusieurs cas de compromissions faisant suite à l'exploitation de vulnérabilités de type jour-zéro, comme la vulnérabilité CVE-2024-47575 affectant le produit Fortinet FortiManager.

Lorsque la publication d'un code d'exploitation pour une vulnérabilité est antérieure à l'application du correctif sur le système, ou que la vulnérabilité est de type jour-zéro, il est indispensable de réaliser des investigations sur l'équipement pour s'assurer que la vulnérabilité n'a pas déjà été exploitée. À titre d'exemple, en 2024, l'ANSSI a réalisé une campagne de signalement relative à une vulnérabilité affectant le produit FortiEMS de Fortinet (CVE-2023-48788). La réaction rapide d'un bénéficiaire dont l'équipement était vulnérable a permis de découvrir la compromission de ce dernier, et d'empêcher la latéralisation de l'attaquant. Ce cas fréquent illustre l'utilité des investigations lorsqu'un équipement vulnérable a été exposé sur Internet.

11 La description détaillée de l'exploitation de la vulnérabilité CVE-2024-22024 affectant plusieurs produits de sécurité Ivanti a ainsi été publiée deux jours seulement après publication de l'avis de vulnérabilité de l'éditeur. De même pour les vulnérabilités CVE-2024-24919 et CVE-2024-3400, affectant respectivement plusieurs produits *CheckPoint* et Palo Alto, dont la méthode d'exploitation a été publiée quatre jours seulement après l'avis de l'éditeur.

Incidents issus de l'exploitation de vulnérabilités sur des équipements de bordure et de sécurité.

Les vulnérabilités les plus exploitées dans les incidents traités par l'ANSSI se trouvent dans le tableau ci-contre, par ordre décroissant.

Il est particulièrement notable que les neuf vulnérabilités les plus exploitées en 2024 affectent des équipements de sécurité en bordure de SI. L'ANSSI a publié un retour d'expérience sur ces campagnes ciblant les principales solutions de pare-feux, passerelles VPN ou passerelles de filtrage en juin 2024 [11], incluant des mesures de prévention et de durcissement. Il met en évidence l'importance de la maîtrise de ces équipements par les organisations, que ces dernières les mettent en œuvre pour leur propre compte, pour le compte de clients ou qu'elles en délèguent la mise en œuvre à des prestataires ou sous-traitants. La responsabilité de la supervision et du maintien en condition de sécurité de ces équipements doit être clairement établie et connue de tous.

Cette tendance peut s'expliquer par plusieurs caractéristiques qui font de ces équipements des cibles de choix :

- une surface d'attaque rendue importante par l'accumulation au cours du temps de nombreuses fonctionnalités, dont certaines reposent sur des briques logicielles obsolètes ;
- une exploitation de vulnérabilité généralement assez simple, fiable et reproductible ;
- un potentiel de compromission du SI en profondeur en raison de leur position privilégiée et de leur adhérence à d'autres briques logicielles (*Active Directory* par exemple) ;
- une exposition permettant une identification de leurs vulnérabilités potentielles par des scans.

Ce phénomène se trouve en outre aggravé par la confiance accordée à ces équipements, susceptible de diminuer chez leurs utilisateurs le respect des bonnes pratiques habituelles, et l'exposition trop fréquente d'interfaces d'administration sur Internet.

Il convient donc de rappeler que ces équipements ne sont pas forcément bien sécurisés par défaut et que, du fait du potentiel qu'ils ont pour les attaquants, ils doivent impérativement faire l'objet d'un effort particulier d'administration et de supervision. Par ailleurs, certains de ces équipements de sécurité ne proposent pas nativement des fonctionnalités d'audit, de supervision et de réponse suffisantes.

CVE	SCORE CVSS3.x	ÉDITEUR	RISQUE	RÉFÉRENCE CERT-FR
CVE-2024-21887	9,1	IVANTI	Exécution de code arbitraire à distance, contournement d'authentification et de politique de sécurité, accès à des ressources restreintes sur différentes passerelles de sécurité et de VPN	CERTFR-2024-ALE-001 CERTFR-2024-AVI-0109 CERTFR-2024-AVI-0085
CVE-2023-46805	8,2			
CVE-2024-21893	8,2			
CVE-2024-3400	10,0	PALO ALTO NETWORKS	Exécution de code arbitraire à distance sur différents équipements de sécurité	CERTFR-2024-ALE-006 CERTFR-2024-AVI-0307
CVE-2022-42475	9,8	FORTINET	Exécution de code arbitraire à distance sur différentes passerelles VPN SSL	CERTFR-2022-ALE-012 CERTFR-2022-AVI-1090
CVE-2024-8963	9,4	IVANTI	Exécution de code arbitraire à distance et contournement de la politique de sécurité sur différentes passerelles de sécurité et de VPN	CERTFR-2024-ALE-013 CERTFR-2024-AVI-0796 CERTFR-2024-AVI-0917
CVE-2024-8190	7,2			
CVE-2024-47575	9,8	FORTINET	Exécution de code arbitraire à distance sur différents équipements de sécurité	CERTFR-2024-ALE-014 CERTFR-2024-AVI-0917
CVE-2024-21762	9,8	FORTINET	Exécution de code arbitraire à distance sur différents équipements de sécurité	CERTFR-2024-ALE-004 CERTFR-2024-AVI-0108
CVE-2021-44228	10,0	APACHE	Exécution de code arbitraire à distance	CERTFR-2021-ALE-022
CVE-2024-24919	8,6	CHECK POINT	Atteinte à la confidentialité des données	CERTFR-2024-ALE-008 CERTFR-2024-AVI-0449

Avertissement :
ce classement ne comptabilise que les événements pour lesquels l'ANSSI ou un prestataire d'investigations numériques a pu confirmer avec un haut degré de certitude l'exploitation d'une vulnérabilité. Les vulnérabilités appartenant à la même chaîne d'exploitation apparaissent groupées.

2 ACTEURS EXPLOITANT LES VULNÉRABILITÉS DANS DES ÉQUIPEMENTS DE SÉCURITÉ EN BORDURE

Les vulnérabilités affectant les équipements de sécurité en bordure de SI sont utilisées par une large gamme d'acteurs. Les attaquants soutenus par des États et disposant de capacités de recherche ou d'achat de vulnérabilités les exploitent traditionnellement de manière ciblée. Toutefois, ces dernières années, l'ANSSI a observé la multiplication de campagnes d'espionnage à large échelle reposant sur l'exploitation massive de vulnérabilités dans des équipements de bordure, suivies de phases de post-exploitation sélectives selon la victime. Certains acteurs cybercriminels avancés disposent également de capacités d'acquisition de vulnérabilités, et réalisent des campagnes d'exploitation massive à des fins d'extorsion. Enfin, lorsque des codes d'exploitation sont rendus publics, les vulnérabilités sont exploitées de manière large et opportuniste par de nombreux acteurs, majoritairement cybercriminels.

Ainsi, certaines vulnérabilités peuvent être exploitées d'abord par un acteur étatique de manière ciblée (par exemple en tant que vulnérabilité jour-zéro), puis massivement par ce même acteur lorsque l'exploitation de la vulnérabilité est détectée, et enfin par l'ensemble de l'écosystème lorsque la vulnérabilité et un code d'exploitation sont rendus publics.

Exploitation des vulnérabilités dans les équipements Ivanti CSA

En 2024, l'ANSSI a observé un attaquant employant des tactiques, techniques et procédures (TTP) similaires à UNC5174[12], exploiter des vulnérabilités dans le produit Cloud Service Appliance (CSA) commercialisé par Ivanti. En particulier, l'exploitation successive des vulnérabilités CVE-2024-8963, CVE-2024-9380 et CVE-2024-8190 a permis à cet attaquant d'exécuter du code arbitraire à distance sur les équipements Ivanti CSA.
La vulnérabilité jour-zéro CVE-2024-8190 a été exploitée plusieurs jours avant la publication de l'avis de sécurité par Ivanti.

Les investigations effectuées par l'ANSSI sur les SI de plusieurs entités victimes indiquent l'utilisation – pour la compromission initiale – d'un même mode opératoire des attaquants (MOA). Ce dernier, dont les techniques présentent un niveau de sophistication et de discrétion modéré, se caractérise par l'usage d'un arsenal d'outils d'intrusion majoritairement disponibles en sources ouvertes, ainsi que par l'usage d'un code de type *rootkit*[13] dont l'utilisation a déjà été rapportée publiquement [12].

Toutefois, les activités de post-exploitation divergent selon les incidents traités, ce qui crédibilise l'hypothèse d'un MOA employé dans l'objectif d'obtenir des accès initiaux, qui seraient ensuite vendus ou confiés à d'autres opérateurs.

3 ÉVOLUTIONS RÉGLEMENTAIRES ET COORDINATION DU TRAITEMENT DES VULNÉRABILITÉS PRODUIT

Plusieurs évolutions réglementaires en cours visent à améliorer la sécurité des produits et la prise en compte des vulnérabilités. L'adoption du *Cyber Resilience Act*[14] (CRA) par l'Union européenne en octobre 2024 a pour objectif de définir des exigences minimales de cybersécurité pour l'ensemble

12 Mode opératoire nommé par l'éditeur américain Mandiant, qui agirait selon ce dernier comme sous-traitant au profit du gouvernement chinois [83].

13 Ensemble de programmes malveillants permettant de maintenir un accès illégitime à hauts privilèges sur un système, et ayant fréquemment une fonctionnalité de dissimulation.

14 Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques.

des produits comportant des éléments numériques, incluant les logiciels. Parmi celles-ci, on trouve la prise en compte de la sécurité dès la conception des produits, la mise en place de configurations sécurisées par défaut, la gestion automatisée des mises à jour ou encore une obligation de signalement sur les vulnérabilités [13].

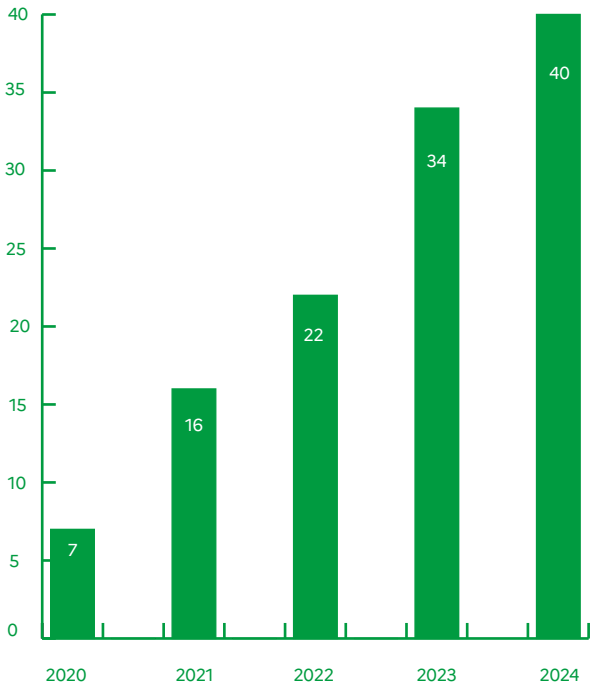
La France dispose également d'un dispositif légal national encadrant les signalements de vulnérabilités et d'incidents affectant la sécurité des systèmes d'information des éditeurs et leur traitement par l'ANSSI. Partageant certains objectifs du CRA, ces dispositions seront confortées par l'entrée en vigueur de ce dernier à partir de 2026.

Le CERT-FR, opéré par l'ANSSI, est chargé du traitement coordonné des vulnérabilités avec les parties intéressées (découvreur et éditeur du produit) jusqu'à leur correction. Cette activité est grandissante au sein du CERT-FR, qui a traité 40 dossiers de coordination en 2024.

Les vulnérabilités faisant l'objet d'un travail de coordination peuvent être découvertes par l'ANSSI dans le cadre de ses activités, rapportées par des partenaires institutionnels, ou être issues de signalements adressés au CERT-FR.

Les signalants de vulnérabilités bénéficient d'une protection prévue à l'article L. 2321-4 du Code de la défense (CD) [14] lorsqu'ils agissent de bonne foi et signalent à la seule ANSSI leur découverte. Le CERT-FR a reçu au total 236 signalements de vulnérabilités en 2024. Ces signalements sont transmis par le CERT-FR au propriétaire du service vulnérable (dans le cadre d'une vulnérabilité affectant un service en production, comme un site Web) ou à l'éditeur lorsque la vulnérabilité concerne un produit, en protégeant l'identité du signalant et les circonstances de sa découverte. Pour les vulnérabilités produit, le CERT-FR peut proposer son service de coordination du traitement de la vulnérabilité.

Nombre de dossiers de coordination de vulnérabilités traités par le CERT-FR



Ce dispositif légal a été renforcé en 2024 par l'introduction à l'article L2321-4-1 CD [15] d'une nouvelle obligation pour les éditeurs fournissant leurs produits en France, de notifier à l'ANSSI les vulnérabilités significatives et les incidents affectant significativement la sécurité de leurs produits[15]. L'ANSSI dispose de plusieurs moyens d'action en cas de non-respect de leurs obligations par les éditeurs : émission puis publication d'une injonction, communication aux utilisateurs ou encore publication de la vulnérabilité. ←

15
Pour signaler une vulnérabilité ou un incident :
ClubSSI – Faire une déclaration au CERT-FR
https://club.ssi.gouv.fr/#/declarations

II

MOYENS MIS EN ŒUVRE PAR LES ATTAQUANTS

Afin de tirer profit des nombreuses opportunités qui s'offrent à eux, les attaquants disposent de moyens et d'outils variés, allant de l'exploitation de vulnérabilités aux codes malveillants, en passant par les moyens d'anonymisation. L'arsenal offensif des attaquants peut également être renforcé par l'acquisition d'outils conçus et développés par des entreprises de lutte informatique offensive privée (LIOP).

A
CIBLAGE DE LA CHAÎNE D'APPROVISIONNEMENT

La chaîne d'approvisionnement (*supply-chain*) d'un SI prend différentes formes (équipements, logiciels, prestataires de service) qui offrent des possibilités d'attaque variées. Les attaques par la chaîne d'approvisionnement permettent de compromettre par rebond les organisations clientes d'un prestataire commun ou utilisant un même logiciel ou équipement. Au-delà de leur diversité, leur furtivité les rend particulièrement efficaces et elles peuvent faire l'objet d'un investissement ayant des retombées significatives pour les attaquants.

Attaques par la chaîne d'approvisionnement logiciel

Ce type d'attaque consiste à piéger un logiciel dans l'objectif d'atteindre l'ensemble de ses utilisateurs. Plusieurs exemples aux conséquences importantes ont marqué l'actualité des dernières années, comme la compromission de MeDoc en 2017 dans le cadre de l'attaque NotPetya, celle du logiciel Orion de Solarwinds en 2020 ou encore de l'application 3CX Desktop App en 2023, elle-même précédée de la compromission du logiciel financier X_TRADER.

La majeure partie des attaques par la chaîne d'approvisionnement logiciel est réalisée en compromettant le SI d'un éditeur de logiciel. Toutefois, il est également possible de réaliser une telle attaque en ajoutant du code malveillant dans un projet *open source*. L'attaque ciblant le projet XZ Utils, utilisé dans de nombreuses distributions Linux, en a été un exemple particulièrement marquant en 2024[16]. L'attaque s'est déroulée sur environ trois ans, permettant à son auteur d'obtenir la position de co-mainteneur du projet et d'y introduire des modifications malveillantes. Elle illustre la complexité de la sécurisation de la chaîne d'approvisionnement logiciel.

En janvier 2024, l'ANSSI a également été alertée d'une fuite de données visant l'éditeur *AnyDesk Software*, spécialisé dans le développement de solutions logicielles de bureau à distance. Le code source des applications développées par l'éditeur ainsi que des certificats et clés privées pourraient avoir été dérobés, et deux serveurs relais situés en Europe auraient également été affectés par l'incident. Si aucune preuve de l'altération des logiciels distribués par *AnyDesk* n'a été établie, cette attaque aurait pu avoir des conséquences importantes compte tenu du type de logiciel concerné et de sa large distribution. [16]

16
La version modifiée à des fins malveillantes de XZ Utils permet d'altérer le comportement de OpenSSH, et offre une possibilité d'exécution de code à distance sous certaines conditions.

Attaques par la chaîne d'approvisionnement via les prestataires de services informatiques

Le principe d'une attaque par la chaîne d'approvisionnement peut être aussi, cette fois-ci via les prestataires de service, de compromettre des ressources d'un prestataire de service disposant d'accès sur le SI de la cible finale. Une fois le prestataire compromis, l'attaquant peut profiter des privilèges et ressources dont le prestataire dispose sur le SI de cette dernière. L'attaquant aura tiré profit du niveau de sécurité plus faible du prestataire pour atteindre la cible finale de manière discrète, souvent difficile à détecter.

L'ANSSI a traité plusieurs compromissions d'entités importantes par ce moyen en 2024.

Par exemple, un sous-traitant informatique étranger intervenant au profit de plusieurs grandes entreprises françaises a été compromis en profondeur, permettant ainsi à des attaquants de pénétrer les SI de ces dernières. Au moyen d'accès légitimes – donc difficilement détectables – les attaquants ont pu consulter et exfiltrer des données d'intérêt.

L'ANSSI a également traité en 2024 une tentative de compromission par chaîne d'approvisionnement touchant un industriel français de pointe et faisant suite à la compromission de ressources métier fournies par des prestataires. Si aucune latéralisation sur le SI de la société française n'a été détectée, l'ANSSI constate une forme de récurrence dans les méthodes utilisées pour tenter d'atteindre des entités stratégiques françaises. En effet, en 2015, cette même entité avait déjà été victime d'un incident similaire après que les attaquants se furent introduits sur les SI de filiales récemment acquises. Ces exemples témoignent de l'exploitation active par certains acteurs malveillants des liens de confiance et des potentielles interconnexions informatiques entre une cible finale et son environnement (prestataires, filiales, etc.) afin d'atteindre leurs objectifs.

Les groupes cybercriminels exploitent également le manque de maturité de certains prestataires de services dans leurs pratiques de sécurité. En 2024, de nombreuses entités françaises victimes de fuites de données ont été compromises au travers d'un prestataire informatique [17]. Par ailleurs, en octobre 2024, un affilié du *Ransomware as a Service* (*Raas*)[17] Qilin a compromis une entreprise d'infogérance menant au chiffrement ou à l'exfiltration de données d'une trentaine de ses clients. L'attaquant aurait notamment tiré profit du déploiement de solutions d'accès à distance par l'infogérant chez ses clients pour accéder et chiffrer des postes de travail de ces derniers. Pour au moins l'un d'entre eux, l'attaquant serait parvenu à se latéraliser sur le SI, à y déposer des outils malveillants et à en exfiltrer des données sensibles.

Ces événements (tentatives de compromission comme incidents) illustrent une tendance forte observée par l'ANSSI : le gain d'expérience et de maturité de certaines organisations pousse les attaquants à cibler les fournisseurs de services numériques (FSN) pour atteindre leurs cibles finales de manière plus discrète.

17
Modèle économique dans lequel un service et des ressources sont fournis par un individu ou un groupe dit « opérateur » à des attaquants dits « affiliés » afin d'être utilisés dans leurs propres attaques en échange d'un pourcentage des rançons récupérées.

B
ÉVOLUTIONS DE L'OUTILLAGE ET DES INFRASTRUCTURES D'ATTAQUE

1 RÉSEAUX ET INFRASTRUCTURES D'ANONYMISATION

Ces dernières années ont été particulièrement marquées par le développement et l'utilisation des réseaux d'anonymisation.

S'ils sont particulièrement prisés par les acteurs réputés liés à la Chine, des acteurs étatiques réputés russes (notamment des MOA tels qu'APT28 ou Nobelium) ont utilisé ou utilisent aussi des réseaux de machines compromises à des fins d'anonymisation. Ces réseaux peuvent être constitués de routeurs compromis, de *proxies* ou de services VPN commerciaux. Les groupes d'attaquants réputés russes restent très actifs dans le ciblage de messageries électroniques, pour lequel ils ont développé des infrastructures d'attaques par force brute ou pulvérisation de mots de passe[18] et de nouvelles techniques d'hameçonnage. De la phase de reconnaissance s'appuyant sur des services VPN ou de *proxy* commercial, à l'utilisation de services d'hébergement gratuits pour l'exposition de pages d'hameçonnage, les opérateurs de ces MOA bénéficient d'infrastructures infogérées à moindre coût et prêtes à l'emploi. Par ailleurs, ces services offrent une grande flexibilité dans la création et l'administration de nouvelles ressources, et peuvent partiellement reposer sur des infrastructures aussi utilisées à des fins légitimes par des particuliers et des entreprises, rendant complexes la distinction entre un usage légitime ou pas et donc la détection et le suivi par les équipes de sécurité. Des groupes cybercriminels emploient également de telles infrastructures d'anonymisation.

L'ampleur de l'utilisation des réseaux d'anonymisation par des attaquants réputés liés à la Chine rend l'étude de ceux-ci particulièrement nécessaire.

2 ATTAQUES AYANT UN OBJECTIF CAPACITAIRE

En 2023 et 2024, des attaquants liés à des intérêts stratégiques étatiques ont compromis des entreprises du secteur du numérique et de la cybersécurité, en particulier au moyen du MOA réputé russe Nobelium. L'objectif probable de ces attaques est d'obtenir des accès ou des informations permettant de réaliser des attaques ultérieures, par exemple par la recherche de vulnérabilités, la réutilisation d'authentifiants voire la préparation d'une attaque par la chaîne d'approvisionnement logiciel. Néanmoins, il semble que dans certains cas les opérateurs aient également cherché à se renseigner sur l'état de la connaissance à leur sujet.

Le mode opératoire Nobelium, actif depuis au moins octobre 2020 et réputé lié au service de renseignement extérieur russe (SVR) [21], est associé à des campagnes d'attaques informatiques par hameçonnage ciblé, visant à collecter des renseignements stratégiques. Les victimes habituellement associées à ces campagnes appartiennent aux secteurs gouvernementaux, notamment diplomatiques, en Europe dont en France, en Afrique, en Amérique du Nord et en Asie. Ce mode opératoire a ainsi été employé contre des entités diplomatiques françaises à plusieurs reprises entre 2021 et 2023.

D'après l'entreprise américaine Microsoft, une partie des attaques associées à Nobelium a ciblé des entités du secteur du numérique dans le monde entier et notamment en Amérique du Nord et en Europe de l'Ouest. En novembre 2023, Microsoft a fait part d'un incident de sécurité lors duquel les opérateurs de Nobelium ont exfiltré des courriers électroniques appartenant à ses équipes juridiques et de cybersécurité, ainsi qu'à des membres de son comité exécutif. En tant qu'éditeur de sécurité informatique, Microsoft est un important contributeur à la connaissance en sources ouvertes sur le mode opératoire Nobelium, ainsi que sur les moyens d'entraver les attaques qui lui sont associées. D'après Microsoft, les opérateurs de Nobelium ont notamment cherché lors de la compromission de l'entreprise, des informations liées au mode opératoire lui-même [22].

18 *Ou password spraying*

Utilisation de réseaux d'anonymisation par des attaquants réputés liés à la Chine

Depuis 2022, l'utilisation de réseaux d'anonymisation par des MOA réputés chinois a été observée dans le cadre de quatre opérations de cyberdéfense traitées par l'ANSSI.

De leur côté, des éditeurs de sécurité ont également documenté certains de ces réseaux comme ORBWEAVER, SPACEHOP [18] ou KV Botnet [19].

La particularité de ces réseaux d'anonymisation réside dans le grand nombre de machines impliquées et l'industrialisation de leur infection. Composés de plusieurs centaines, voire milliers, d'équipements compromis ou loués, ils augmentent le coût de la défense contre les attaques informatiques en faisant évoluer les infrastructures attaquantes et les TTP. L'utilisation d'équipements réseau légitimes dans ces infrastructures complique également la détection et le blocage, puisqu'il est difficile de discriminer le trafic malveillant.

Ces réseaux d'anonymisation révèlent de nouveaux paradigmes pour appréhender la menace. Ils font évoluer l'idée que les attaquants contrôlent l'intégralité des infrastructures d'attaques. En effet, dans le cas des réseaux d'anonymisation réputés chinois, les infrastructures seraient administrées par des entités indépendantes, des prestataires ou des administrateurs localisés en République Populaire de Chine (RPC). Elles ne sont pas contrôlées par un groupe d'attaquants donné et semblent être utilisées conjointement par des groupes distincts. Cette évolution est à mettre en parallèle du partage de codes, d'infrastructures et de prestataires (de manière institutionnalisée, commerciale ou informelle) entre les différents MOA réputés chinois, qui réduit également les possibilités d'imputation à un MOA spécifique.

Les campagnes d'attaques du MOA Volt Typhoon, utilisé potentiellement à des fins de pré-positionnement en vue de déstabilisation et attribué par les *Five Eyes*[19] à la Chine, se caractérisent également par leur discrétion. Au-delà du recours au réseau d'anonymisation KV Botnet, l'utilisation de TTP particulièrement discrets, incluant l'usage de techniques de *Living off the Land*[20] et la mise en œuvre de précautions de sécurité opérationnelle, illustrent cette volonté d'anonymisation. Les opérateurs du MOA auraient, par exemple, évité d'utiliser des identifiants de connexion en dehors des heures de travail considérées comme « standards » chez leurs cibles afin d'éviter de générer des alertes de sécurité [20].

19 Le terme désigne l'alliance des services de renseignement des États-Unis, de l'Australie, de la Nouvelle-Zélande, du Royaume-Uni et du Canada.

20 Où il s'agit pour un attaquant d'utiliser les outils déjà présents sur le système d'information ciblé. La détection et l'investigation numérique ne peuvent alors plus se faire en se fondant sur la recherche d'outils spécifiques à l'attaquant.

Les attaquants auraient donc eu pour intention de conduire une opération de contre-espionnage, vraisemblablement afin de renforcer leur sécurité opérationnelle.

En janvier 2024, l'entreprise américaine Hewlett Packard Enterprise a fait part d'une attaque vraisemblablement associée à Nobelium, contre son environnement de messagerie basé sur le *cloud*. Si les motivations des attaquants demeurent inconnues, ceux-ci auraient pu chercher à obtenir des informations relatives à ces produits [23].

Enfin, d'après un rapport conjoint des autorités polonaises, britanniques et américaines publié en décembre 2023 [24], les opérateurs de Nobelium ont mené une campagne d'exploitation à grande échelle de la vulnérabilité CVE-2023-42793 affectant les serveurs hébergeant le logiciel JetBrains, développé par l'entreprise TeamCity. Ce produit étant largement utilisé par les développeurs de logiciels, cette campagne aurait pu permettre de réaliser ensuite une attaque par la chaîne d'approvisionnement logiciel.

3 UTILISATION DES MÊMES RESSOURCES OU CAPACITÉS PAR DES ACTEURS ÉTATIQUES ET DES ACTEURS CYBERCRIMINELS

En 2024, l'ANSSI continue d'observer une porosité grandissante entre les différents profils d'attaquants. Premièrement, la recherche de furtivité et d'efficacité à moindre coût pousse l'ensemble des acteurs malveillants à privilégier des outils commerciaux disponibles en sources ouvertes ou des techniques de *Living off the Land* (LoTL). Des MOA réputés chinois utiliseraient notamment les outils légitimes de proxy SOCKS5, ou encore le VPN SoftEther.

Des codes et des services malveillants d'origine cybercriminelle sont également utilisés par des MOA réputés étatiques. Les *Remote Access Trojan* (RAT) Remcos et DarkCrystal seraient ou auraient été déployés à la fois par des groupes cybercriminels et des acteurs réputés liés à la Russie [25] [26] [27]. Les opérateurs du MOA réputé russe UNC5812 auraient aussi utilisé le code malveillant pour Android CraxsRAT, d'origine cybercriminelle, pour cibler des entités militaires ukrainiennes dans le contexte de l'offensive russe en Ukraine [28].

Certains acteurs liés à des États déploieraient également des rançongiciels soit pour rendre indisponibles des données sensibles [29], soit comme couverture d'opérations d'espionnage plus ciblées. Depuis 2021, les éditeurs SentinelOne et Recorded Future auraient observé plusieurs campagnes d'espionnage menées par le groupe réputé chinois ChamelGang menant au déploiement du rançongiciel CatB [30]. À deux reprises en 2024, l'ANSSI a observé l'utilisation d'outils d'intrusion tels que PlugX ou Shadowpad, généralement associés à des modes opératoires réputés chinois, dans des attaques ayant abouti au chiffrement du SI victime. Enfin, les groupes cybercriminels se sont professionnalisés et sont aujourd'hui capables d'employer des techniques d'attaque sophistiquées et d'exploiter des vulnérabilités jour-zéro [31] [29].

Certains attaquants peuvent également cibler et compromettre les capacités offensives d'autres acteurs malveillants, potentiellement pour dissimuler leur propre activité. Les opérateurs du MOA Turla, attribué en sources ouvertes au FSB russe, auraient ainsi déjà exploité l'outillage et l'infrastructure d'au moins six MOA différents dans le cadre de leurs attaques [32].

Cette porosité dans les activités entre différents acteurs malveillants est accentuée par certains groupes qui agissent à la frontière entre différents milieux. Le groupe mettant en œuvre le code malveillant RomCom aurait cette année encore mené plusieurs campagnes à des fins tantôt d'espionnage stratégique, tantôt lucratives. Ces hypothèses découlent de l'étude de la victimologie du groupe qui oscille entre un ciblage spécifique à l'encontre d'entités gouvernementales et sensibles en Ukraine ou dans les pays de l'OTAN, et un ciblage plus opportuniste à l'encontre d'entreprises privées de secteurs variés [33]. ←

C
MERCENARIAT ET PRESTATAIRES DE SERVICE

1 ENTRE COMMERCE RENTABLE ET ÉCOSYSTÈME AU SERVICE D'UN ÉTAT

Tandis que le secteur de la LIOP continue sa croissance, l'ANSSI constate en parallèle le développement d'un écosystème privé au sein des États, notamment en Chine. De nouveaux acteurs apparaissent également, en raison de la variété et de la démocratisation des moyens d'attaque.

Un exemple de la variété de ces moyens est constitué par l'ADINT[21], au travers duquel les failles du marché de la publicité sont exploitées. Afin de récupérer les critères identifiants[22] faisant l'objet de la mise en relation entre l'offre et la demande sur le marché publicitaire et permettant d'associer un équipement à son utilisateur, les entreprises d'ADINT internalisent des capacités d'annonceurs ou collaborent avec eux. Il leur est ainsi possible de récolter légalement des données sur un large ensemble d'individus puis de les réutiliser dans le cadre d'opérations de surveillance ou d'espionnage [34] [35] [36]. De plus, ces outils de géo-surveillance n'impliquant pas la compromission de l'appareil ciblé, ils ne sont pas considérés comme des biens à double usage[23]. À ce titre, les services ADINT peuvent être commercialisés plus facilement que les logiciels espions conventionnels. Au-delà de ces objectifs de surveillance géographique, de récentes publications ont mis en évidence l'existence d'un nouveau type de technologie basé sur l'ADINT, capable de compromettre des appareils mobiles et des ordinateurs par la combinaison de l'envoi de publicités et de l'exploitation de vulnérabilités. Le simple affichage d'une publicité sur un téléphone ciblé aboutirait à sa compromission[24] [37].

Aujourd'hui, l'écosystème privé est diversifié et rassemble des acteurs aussi variés que des entreprises privées, des mercenaires ou des attaquants louant leurs services au plus offrant (*hackers for hire*) et des prestataires travaillant au profit d'États. Si ces activités ont été mises en lumière auprès du grand public au travers des espiogiciels et des attaques sur les appareils mobiles, elles ne s'y limitent pas mais couvrent au contraire un éventail de prestations allant de la fourniture de services (voir focus page 28) à la mise à disposition de moyens d'attaque. La fuite de données concernant l'entreprise chinoise I-SOON donne un aperçu de l'organisation que peuvent avoir de tels acteurs (voir focus page 27).

2 CIBLAGE DES APPAREILS MOBILES

Par leur omniprésence et leur usage systématique, les appareils mobiles sont des équipements d'intérêt pour l'acquisition de renseignement d'origine cyber. Les logiciels espions fournis par les entreprises de LIOP constituent une des menaces majeures pour leurs utilisateurs. Ces outils, officiellement conçus pour lutter contre le terrorisme et la criminalité organisée, sont utilisés par certains États ou par leurs services de renseignement dans l'objectif de surveiller des opposants politiques, des journalistes et des ONG. L'utilisation de ces logiciels n'est par ailleurs pas limitée à de la surveillance interne puisque des cas d'espionnage de personnalités politiques et de gouvernements ont également été rapportés. La compromission des téléphones mobiles de deux députés française et bulgare siégeant au Parlement européen et appartenant à la sous-commission sécurité et défense fin 2023, témoigne de l'emploi de ces outils à des fins d'espionnage stratégique [44].

Ce commerce d'outils de surveillance sophistiqués profite principalement à des États. D'une part, ces outils permettent aux États qui ne disposent pas en propre de ces technologies ou des capacités techniques pour les développer de mener des actions de surveillance ciblée. D'autre part, ils fournissent aux États disposant des ressources nécessaires un moyen pratique pour rendre beaucoup plus complexes les processus d'imputation en facilitant la dissimulation de leurs attaques [45]. Cet anonymat est par ailleurs renforcé par la sophistication des chaînes d'infection. Les délais entre compromission et identification de l'attaque ainsi que l'absence de persistance sur les

21 Contraction de *advertising* et *intelligence* (ou renseignement issu de la publicité). Il peut se définir comme la distribution massive ou spécifique de contenus publicitaires vers une ou plusieurs cibles à des fins de profilage et de géolocalisation.

22 Tels que les habitudes, les centres d'intérêt ou bien encore le matériel utilisé.

23 Les biens à double usage sont des biens sensibles, souvent destinés à des applications civiles, mais qui peuvent être utilisés à des fins militaires. À ce titre, leur exportation est soumise à autorisation.

24 Différents produits, tels que Sherlock, Patternz ou Alladin, développés respectivement par les sociétés INSANET, ISA SECURITY et INTELLEXA, disposeraient de telles capacités [84].

appareils ciblés entravent significativement les analyses forensiques et les moyens de détecter ce type d'outil et leur emploi.

De ce fait, il convient de porter une attention particulière aux notifications des éditeurs, qu'il s'agisse d'une notification du constructeur du téléphone[27] ou de l'éditeur d'une application (de messagerie notamment).

Une séparation stricte entre les usages professionnels et personnels, ou l'emploi de moyens spécifiques à certains usages, reste déterminante pour espérer réduire l'exposition à ces menaces. Par ailleurs, un redémarrage régulier du support peut permettre de limiter les impacts d'une compromission non persistante, en forçant l'attaquant à réinfecter le support.

Enfin, l'activation de mécanismes de durcissement du système d'exploitation[28] est à privilégier, notamment pour les populations à risque.

3 UN MARCHÉ EN CONSTANTE ÉVOLUTION FACE AUX LIMITES TECHNIQUES ET AUX EXPOSITIONS MÉDIATIQUES

Le ciblage d'appareils mobiles requiert un niveau de sophistication élevé, notamment par l'emploi de techniques d'infection furtives (chaînes d'attaque ne nécessitant pas d'action de la cible, dites « *0-click* ») et d'exploitation de vulnérabilités jour-zéro. Cependant, le temps de développement de ces vulnérabilités, leur durée de vie et les contre-mesures prises par les gouvernements et les industriels à l'encontre des logiciels espions constituent aujourd'hui autant de limites pour ces chaînes d'infection. En février 2024, le Royaume-Uni et la France ont lancé le processus de Pall Mall, dialogue consacré à la lutte contre la prolifération et l'utilisation irresponsable des outils commerciaux d'intrusion cyber. L'initiative rassemble une coalition d'États, d'entreprises et de représentants de la société civile. Elle a donné lieu à une déclaration multipartite et vise notamment à l'élaboration d'un code de bonnes pratiques pour l'utilisation de ce type d'outils. [46]

En parallèle, les publications relatives à ces entreprises et leurs activités se poursuivent. Plusieurs éditeurs de sécurité et organisations internationales ont développé des capacités de suivi des infrastructures de certains logiciels espions qu'ils exposent en sources ouvertes, diminuant par là même leurs capacités. Ces rapports obligent les entreprises de LIOP à faire évoluer leurs infrastructures comme ce fut le cas pour l'entreprise Cytrox après les publications par l'éditeur Sekoia d'un document traitant du logiciel espion Predator [47]. L'entreprise espagnole Variston aurait par ailleurs perdu une grande partie de son activité puis de ses salariés à la suite de l'exposition par Google de la chaîne d'infection menant au déploiement de son logiciel espion [48] [49].

L'année 2024 a également été marquée par un nombre croissant d'actions en justice intentées par des victimes de logiciels espions. Le procès opposant NSO Group à Meta pour sa plainte en 2019 démontre la volonté des industriels de se protéger des capacités des entreprises de LIOP. Des plaintes ont également été déposées par des personnalités civiles : l'avocat catalan Andreu Van den Eynde Adroer, dont le smartphone avait été infecté par Pegasus en mai 2020, a porté plainte contre NSO Group en visant directement ses fondateurs ainsi que son directeur [50].

Malgré tout, le secteur de la lutte informatique privée reste attractif et ses entreprises s'adaptent et se réorganisent rapidement. Elles ont ainsi recours à des sociétés écrans ou des intermédiaires qui profitent de l'absence de régulation sur l'utilisation des biens à double usage pour s'implanter dans certains pays disposant de législations favorables comme l'Indonésie et les Émirats arabes unis [51]. ←

27 À titre d'exemple, Apple envoie des notifications depuis l'adresse *threat-notifications @apple.com*

28 Le mode Isolement (*Lockdown Mode*) en environnement iOS en est un exemple [82]

La divulgation des données de l'entreprise I-SOON, une plongée dans l'écosystème offensif chinois

Le 16 février 2024, un acteur inconnu, @iSOON sur X (anciennement Twitter), a publié sur la plateforme d'hébergement de projets et de gestion de développement logiciel GitHub, des données appartenant à l'entreprise chinoise Sichuan I-SOON (ou I-SOON) Information Technology Co., Ltd. Si l'authenticité de ces documents paraît probable, il n'est pas possible en l'état pour l'ANSSI de confirmer ou d'infirmer leur provenance. Selon des informations disponibles en sources ouvertes, l'entreprise est un prestataire du ministère de la Sécurité Publique (MSP), du ministère de la Sécurité de l'État (MSE) chinois, ainsi que de l'Armée populaire de libération (APL). Sur son site Internet ou dans ses brevets enregistrés, l'entreprise indique fournir notamment des logiciels de surveillance conçus pour collecter des informations sensibles. Son PDG, Wu Haibo (également connu sous l'alias shutd0wn) faisait partie du groupe *hacktiviste* Honker Union fondé en 1999 qui a constitué la première génération « d'attaquants patriotiques » chinois.

L'entreprise I-SOON est un acteur pleinement intégré à l'écosystème de lutte informatique offensive (LIO) chinoise. Les documents et les conversations divulguées révèlent des liens contractuels, d'infrastructures et de codes entre l'entreprise et plusieurs MOA réputés chinois. Les objectifs de ciblage de ces MOA sont concordants avec les intérêts de l'État chinois en matière d'espionnage et de lutte contre les « Cinq Poisons » [25]. Cette divulgation de données met en exergue un cas représentatif des liens de prestation de services avec différentes entités gouvernementales, que ce soit l'APL, le MSE ou le MSP, ainsi que le partage d'outils offensifs entre plusieurs acteurs, visibles sur les tableaux de contrats d'achats et de prestations divulgués.

De ce mode de fonctionnement contractuel résulte une difficulté à relier les campagnes d'attaques chinoises à leur donneur d'ordre.

Par ailleurs, cette divulgation illustre le niveau actuel de concurrence entre les entreprises de lutte informatique offensive chinoises et leurs difficultés à émerger parmi les acteurs majeurs du secteur à l'échelle nationale. Selon les extraits de conversations internes divulgués, l'entreprise I-SOON est contrainte de s'allier avec des entreprises plus importantes dans le but de remporter des appels d'offres. Cela se traduit par une activité offensive opportuniste et autonome, alignée sur les intérêts des autorités chinoises, dans le but de vendre ces accès *a posteriori* et ainsi remporter des contrats. En cela, la divulgation de données de l'entreprise I-SOON est révélatrice d'un fonctionnement peu documenté en sources ouvertes : il ne s'agirait plus exclusivement de victimes ciblées sur la base d'un contrat étatique, mais bien d'un ciblage en vue d'un contrat et d'une rémunération par un ou plusieurs acteurs gouvernementaux potentiellement intéressés.

C'est au travers de cette nouvelle grille d'analyse de la menace que les éléments divulgués d'un ciblage extensif par l'entreprise I-SOON d'au moins 45 pays, dont la France, peuvent être interprétés. À ce jour, le ciblage par les MOA réputés chinois tel que constaté par l'ANSSI est cohérent avec cette analyse. L'ANSSI estime que cette capacité de prolifération est amenée à croître avec la maturation de l'écosystème informatique chinois : un écosystème qui tend à intégrer la sphère publique, privée et universitaire dans un même effort de participation à la « sécurité nationale » impliquant tant la lutte informatique défensive qu'offensive.

25
Les militants pour l'indépendance de Taïwan, les Ouïgours, les Tibétains, le Falun Gong et les partisans de la démocratie sont les « Cinq Poisons » que le Parti communiste chinois (PCC) juge menaçants pour la stabilité de son régime politique. De fait, ces cinq entités apparaissent de manière récurrente dans la victimologie des modes opératoires d'attaque réputés chinois, car elles sont considérées par le gouvernement comme des cibles prioritaires.

Les Bullet Proof Hosters

Déjà mentionnés dans le *Panorama de la cybermenace* 2021, les *Bullet Proof Hosters* (BPH) occupent toujours une place importante au cœur de l'écosystème cybercriminel. Ces hébergeurs, généralement situés dans des pays hors d'atteinte des accords d'entraide judiciaire, fondent leur modèle économique sur l'immunité de fait qu'ils proposent à leurs clients : inertie ou inaction face aux injonctions judiciaires, acceptation de paiements en cryptomonnaies, peu ou pas de contrôle quant à l'identité de leurs clients, absence de supervision des activités hébergées, etc.

Une analyse des incidents connus de l'ANSSI en 2024 montre que les infrastructures fournies par ces hébergeurs sont utilisées par des acteurs malveillants aux profils hétérogènes. Outre des cybercriminels, des acteurs *hacktivistes* comme étatiques ont également recours à des BPH. Ainsi, le groupe *hacktiviste* pro-russe NoName057 est connu pour avoir utilisé les infrastructures des hébergeurs Stark Industries [38] et Global Internet Solutions LLC (GIR) [39]. Stark Industries apparaît également dans des incidents liés au groupe cybercriminel FIN7 [40] et des attaques menées par l'acteur réputé Iranien Haywire Kitten [41].

Certains opérateurs de réseaux d'anonymisation réputés chinois sont également connus pour appuyer une partie de leur infrastructure d'anonymisation sur des BPH [18].

L'hébergeur GIR est quant à lui utilisé par le MOA réputé lié à la Russie Gamaredon [42], mais également par des cybercriminels déployant le loader Emmenhtal [43].

Enfin, si les BPH font régulièrement la publicité de leurs services sur des forums spécialisés en mettant en avant l'absence de contrôle sur les activités de leurs clients, l'ANSSI a depuis observé plusieurs événements de sécurité impliquant des hébergeurs ne se revendiquant pas comme des BPH. Ces hébergeurs sont enregistrés auprès de registres nationaux et ne promeuvent pas l'utilisation de leurs infrastructures à des fins malveillantes. Toutefois, un faisceau d'indices concordants suggère des activités de ce type – comme l'utilisation de leurs services dans des incidents de sécurité, leur manque de réactivité dans la mise hors ligne de machines impliquées dans des attaques, l'utilisation de moyens de paiement en cryptomonnaie, l'absence de politique de KYC[26] et une certaine opacité entourant l'enregistrement légal des entreprises associées – tout à fait comparables à celles pratiquées à partir de BPH.

26 *Know your customer* (KYC), ou connaissance du client.

III

FINALITÉ DES ATTAQUES OBSERVÉES

À l'image des années précédentes, les attaques à but d'espionnage et à but lucratif restent les plus importantes en termes d'investissement des équipes de l'ANSSI. Par ailleurs, 2024 a été marquée par une hausse des attaques à finalité de déstabilisation, notamment opérées par des groupes *hacktivistes*. L'ANSSI observe que les infrastructures ultramarines sont particulièrement exposées lors des attaques à but de déstabilisation ou par rançongiciel, en raison notamment de la résilience moindre des accès à Internet et des services publics ou encore des délais d'intervention accrus pour des entités basées en métropole, que ce soit l'ANSSI ou des prestataires spécialisés.

A
ATTAQUES À BUT LUCRATIF

→ Les attaques à but lucratif reposent essentiellement sur le principe de l'extorsion financière, et se manifestent en général par le vol ou le chiffrement de données. Les deux approches peuvent être cumulées dans les attaques dites par « double extorsion ». Ces attaques se veulent toujours très opportunistes et les attaquants n'hésitent pas à les médiatiser pour accentuer la pression sur leurs victimes.

1 UNE ACTIVITÉ CYBERCRIMINELLE QUI SE MAINTIENT À UN NIVEAU ÉLEVÉ

L'activité des groupes de rançongiciel, qui représentent une part significative de l'activité cybercriminelle, s'est poursuivie avec une intensité importante en 2024. Si ces attaques à finalité lucrative sont conduites par des groupes ciblant indistinctement la plupart des secteurs et des zones géographiques, les cybercriminels concentrent toutefois leurs activités à l'encontre de pays riches afin d'augmenter la probabilité d'obtenir le paiement d'une rançon.

Afin d'accentuer la pression sur les victimes, les opérateurs de rançongiciels ciblent les éléments du SI susceptibles de contenir des données, comme les serveurs de stockage nuagique. Depuis 2023, l'ANSSI observe également le ciblage continu d'hyperviseurs (notamment les équipements ESXi de VMware), qui hébergent de nombreux services et données. Des groupes tels que Mallox, RansomHub ou Qilin ont développé de nouveaux variants de leur rançongiciel ciblant spécifiquement ces équipements. La capacité à chiffrer plusieurs types d'équipements est par ailleurs un argument d'attractivité utilisé par les groupes de *RaaS* pour recruter leurs affiliés [53].

Les attaques ayant pour finalité l'extorsion financière, qu'elles prennent la forme d'attaques par rançongiciel ou d'exfiltration de données, ont des conséquences parfois très lourdes pour l'entité victime, que ce soit en termes de réputation ou de continuité d'activité. Les dommages financiers engendrés par ces attaques peuvent également être importants et aggraver la situation des victimes les plus précaires.

L'attaque par rançongiciel contre l'université Paris-Saclay, déjà mentionnée dans le retour d'expérience JOP 2024, a entraîné de forts impacts opérationnels tels que l'indisponibilité de nombreuses applications métier durant la période d'inscription étudiante et au cours des mois suivant la rentrée. Ces perturbations ont également affecté les écoles, les universités membres-associées et les organismes de recherche dont les infrastructures sont mutualisées avec celle de l'université. Si des mesures de remédiation ont progressivement été mises en place, cet incident souligne l'importance des plans de continuité (PCA) et de reprise d'activité (PRA) pour la priorisation des actions de reconstruction du SI.

2 DÉSORGANISATION DE L'ÉCOSYSTÈME CYBERCRIMINEL

L'année 2024 a également été marquée par la perturbation de l'écosystème cybercriminel, du fait de l'éclatement successif de plusieurs groupes majeurs et d'opérations de démantèlement.

À partir de la mi-année, l'ANSSI a observé l'augmentation de l'utilisation d'*infostealers*[29] dans les chaînes d'infection menant au déploiement de rançongiciels. Généralement peu sophistiqués mais déployés massivement, ces programmes malveillants permettent d'obtenir des authentifiants sur le poste de travail de la victime. Ces derniers sont ensuite revendus sur des forums ou par le biais de canaux Telegram privés, puis réutilisés par d'autres attaquants. À l'instar de l'ensemble de l'écosystème cybercriminel, certains opérateurs d'*infostealers* s'organisent autour d'offres de service et travaillent avec des courtiers en accès initiaux[30] ou directement avec des affiliés de rançongiciels.

29 Un *infostealer* est un code malveillant utilisé pour collecter des informations sur le poste de travail de la victime, notamment des authentifiants enregistrés dans les navigateurs Web.

30 Acteur cybercriminel spécialisé dans l'obtention et la revente d'accès non autorisés à un système d'information.

Évolution des attaques par rançongiciel suivies par l'ANSSI

En 2024, 144 compromissions par rançongiciel ont été portées à la connaissance de l'ANSSI. Le nombre d'attaques se maintient à un niveau équivalent à 2023, et la menace associée demeure particulièrement importante pour la France.

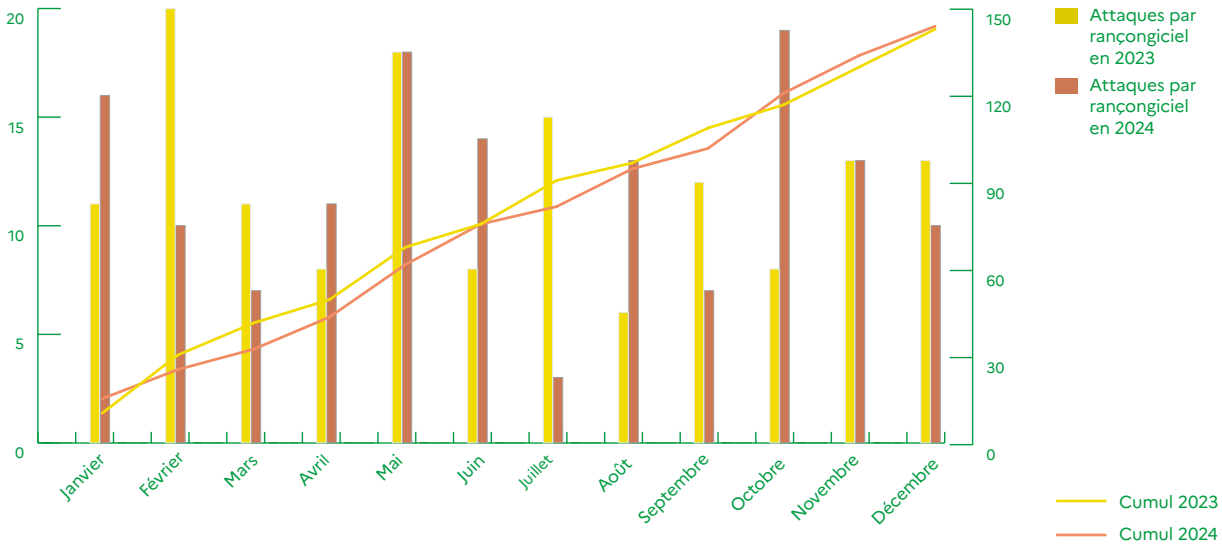
Il est à noter que si l'on observe globalement un nombre d'attaques comparable aux années précédentes, l'écosystème s'est renforcé afin d'assurer la réponse à ce type d'attaques, ce qui permet à l'Agence de concentrer son implication sur celles ayant les impacts les plus importants ou présentant des risques politiques.

Si les PME/TPE/ETI constituent la catégorie d'entités la plus affectée par les compromissions par rançongiciel, la proportion de collectivités territoriales (17%) et d'établissements de santé (4%) victimes de ce type d'attaque a diminué. En revanche, l'ANSSI note une augmentation de la part de compromissions par rançongiciel des établissements d'enseignement supérieur, atteignant 12% de l'ensemble des attaques de ce type en 2024, à égalité avec les entreprises stratégiques.

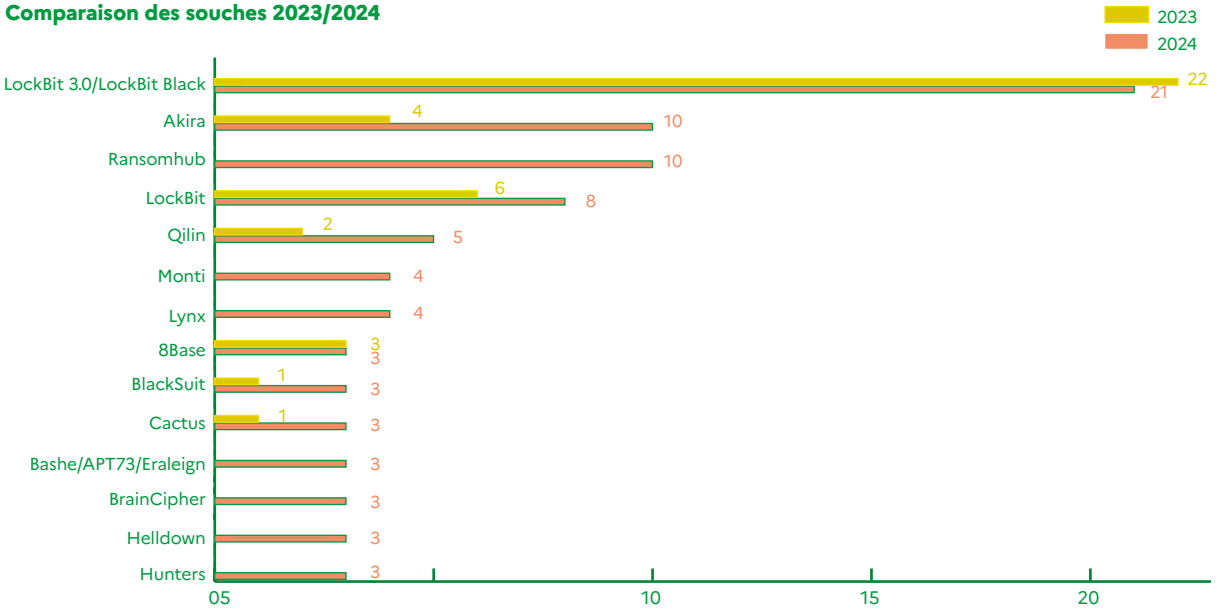
Au cours de la période étudiée, l'ANSSI a observé 39 souches différentes de rançongiciels. Les souches les plus représentées sont LockBit 3.0 (15%), Ransomhub (7%) et Akira (7%). Si LockBit et Akira étaient déjà à l'origine de nombreuses compromissions d'entités françaises en 2023, la souche Ransomhub n'avait pas été observée par l'ANSSI, de même que les souches Monti et Lynx. La souche de rançongiciel Bashe, anciennement Eraleign, n'avait quant à elle plus été observée depuis 2021.

Les souches les plus utilisées évoluent également au fil des années. Si Ryuk et Hive étaient respectivement les rançongiciels les plus observés en 2021 et 2022, ils ont été remplacés par les souches LockBit depuis 2023.

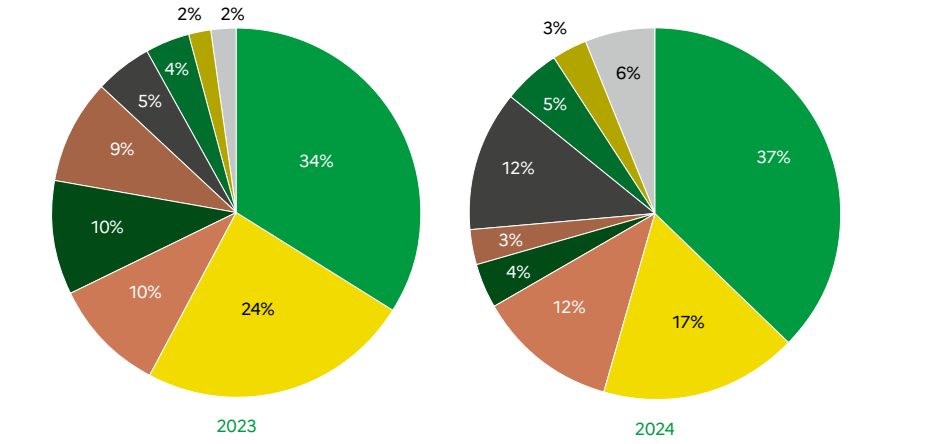
Comparaison annuelle du nombre d'incidents et de signalements



Comparaison des souches 2023/2024



Répartition des victimes d'attaques par le biais de rançongiciels



NB :
ces proportions correspondent aux compromissions portées à la connaissance de l'ANSSI et peuvent varier avec la visibilité dont dispose l'Agence sur ces attaques.

La section de lutte contre la cybercriminalité de la Juridiction nationale de lutte contre la criminalité organisée (JUNALCO) du parquet de Paris a observé en 2024 une baisse du nombre d'attaques [52].

En février et mars 2024, le démantèlement partiel du groupe LockBit (voir focus page 34) puis l'*exit scam*[32] du groupe BlackCat ont participé à désorganiser temporairement l'écosystème des groupes de rançongiciels. Ces deux *RaaS* figuraient depuis 2022 parmi les franchises les plus populaires de l'écosystème, comptant plusieurs centaines d'affiliés. Une partie d'entre eux se serait réorientée vers d'autres franchises telles que RansomHub et Hunters International pour lesquelles l'ANSSI a observé une hausse conséquente des attaques avec près de 200 revendications chacune, dont plusieurs en France [54] [55]. Une seconde partie des affiliés se serait désolidarisée des grands groupes de *RaaS* en créant ou rejoignant de petits groupes privés. À compter du deuxième semestre 2024, l'ANSSI a ainsi observé une hausse des attaques par de nouveaux groupes peu sophistiqués déployant généralement des versions modifiées de rançongiciels dont les codes sources ont été partagés publiquement. Cette tendance, déjà identifiée en 2023, s'est confirmée en 2024 suite aux multiples opérations de démantèlement qui ont favorisé l'éclatement de groupes cybercriminels majeurs et la réorganisation de l'écosystème. Ces nouveaux acteurs ont jusqu'à présent mené des attaques peu régulières, comme le groupe Brain Cipher responsable de plusieurs attaques en France entre juin et août 2024 et dont l'activité semble avoir depuis drastiquement diminué. L'apparition régulière de nouvelles souches de rançongiciels s'appuyant sur des codes sources précédemment divulgués témoigne du fort potentiel de prolifération de ces programmes malveillants cybercriminels.

3 VOLS ET FUITES DE DONNÉES À L'ENCONTRE D'ENTITÉS FRANÇAISES

En 2024, de nombreuses entités françaises publiques et privées ont été victimes de fuites de données, diffusées sur des forums, des sites de divulgation de données ou des canaux Telegram [17].

Des entités du secteur social, naturellement amenées à gérer des données à caractère personnel, ont fait l'objet de nombreux incidents au début de l'année. Parmi les incidents les plus marquants, sont notables ceux ayant affecté les prestataires de tiers-payant Viamedis et Almerys, ou bien encore celui ayant touché France Travail, avec pour conséquence l'exfiltration de quantités importantes de données personnelles appartenant à de nombreux Français [63]. Ces incidents ont mis en exergue des insuffisances de protection dans la façon dont ces données sont traitées et les moyens d'y accéder, et ce dès la conception des projets. Le CERT-FR a publié en 2024 un retour d'expérience sur ces incidents [64].

L'ANSSI constate que ces fuites de données, avérées ou non, peuvent être revendiquées et republiées parfois plusieurs mois après l'incident et par plusieurs acteurs cybercriminels ou *hacktivistes*. Par ailleurs, l'ANSSI a observé une surmédiatisation, plus particulièrement au cours de la période des JOP 2024, de fausses annonces de vol de données par des acteurs malveillants. Ces annonces sont généralement constituées d'anciennes données déjà publiées ou de faibles quantités d'informations. Les levées de doute liées à ces revendications mensongères demandent un temps conséquent à l'entité victime concernée et aux professionnels de sécurité, alors que leur médiatisation peut entraîner un impact réputationnel pour les victimes. Par exemple, entre juin et août 2024, plus de 15 alertes ont été portées à la connaissance de l'ANSSI concernant de fausses publications provenant de plusieurs canaux Telegram se faisant passer pour le groupe de rançongiciel LockBit. ←

32
Un *exit scam*, ou escroquerie de sortie en français, consiste pour une entreprise ou ici pour un groupe cybercriminel à cesser de fournir le service vendu puis de disparaître avec l'ensemble des dus financiers de ses clients ou affiliés.

Les opérations de démantèlement

Les opérations internationales de démantèlement menées par les forces de l'ordre visent des maillons essentiels de l'écosystème cybercriminel.

Plusieurs forums de revente d'accès et de données ont ainsi fait l'objet d'opérations de lutte contre la cybercriminalité. En mars 2024, la Police allemande de Düsseldorf a ainsi saisi le forum cybercriminel germanophone CrimeMarket qui comptabilisait environ 200 000 utilisateurs [56]. En réaction, les cybercriminels s'appliquent à reprendre ou créer de nouveaux forums, en capitalisant sur la réputation, la base d'utilisateurs, l'identité graphique ou encore les catégories de contenu des précédents forums. C'est notamment le cas de RaidForums, saisi en 2022 puis repris et renommé BreachForums. Les arrestations régulières d'administrateurs de forums comme en mars 2023 [57] et en mai 2024 n'ont eu jusqu'à présent que des impacts temporaires sur l'existence de ces communautés.

Outre les plateformes cybercriminelles, plusieurs opérations de démantèlement ont également eu lieu au cours de l'année 2024 afin de déstabiliser les groupes d'attaquants et l'écosystème cybercriminel. En février 2024, l'opération CRONOS, menée par une coalition internationale d'agences de lutte contre la cybercriminalité dont l'Unité nationale cyber (UN Cyber) de la Gendarmerie nationale française, a permis de perturber significativement les activités du groupe de *ransomware-as-a-service* LockBit [58]. Ce groupe, actif depuis 2019, était devenu le groupe de rançongiciel le plus actif et attractif de l'écosystème en comptabilisant à lui seul environ 30% des attaques par rançongiciels en 2023 [58] [59].

Entre le 27 et le 29 mai 2024, une opération de démantèlement de plusieurs infrastructures liées à des *loaders*[31] comme IcedID et SmokeLoader a été menée dans le cadre d'une coopération judiciaire internationale impliquant les autorités allemandes, néerlandaises, danoises, françaises (coordonnées par l'Office anticybercriminalité de la police judiciaire (OFAC)), britanniques et américaines. Cette opération nommée ENDGAME faisait suite à l'opération de démantèlement du botnet Qakbot lancée par les États-Unis en août 2023. Dans le cadre de cette opération, l'ANSSI a apporté son soutien pour l'identification et la notification des victimes. Les codes malveillants visés étaient principalement utilisés comme point d'entrée sur le réseau des victimes pour déployer, entre autres, des outils génériques offensifs comme Cobalt Strike et des rançongiciels [60] [61]. L'ANSSI n'a pas observé en propre de résurgence significative des *loaders* ciblés par le démantèlement, à l'exception de BumbleBee dont l'activité reste cependant très limitée.

Si les effets de ces opérations sont limités dans le temps, elles permettent de désorganiser efficacement les acteurs qui doivent réinvestir du temps et de l'argent pour reconstruire leurs infrastructures. De plus, les multiples arrestations de cybercriminels comme lors de l'opération CRONOS ont pu engendrer une perte de confiance et une atteinte à la réputation des groupes concernés, qui doivent regagner leur prestige au sein de l'écosystème [62].

31 Un *loader* ou chargeur est un code malveillant dont la fonctionnalité principale est de déposer ou exécuter un autre code malveillant sur la machine compromise.

B
DÉSTABILISATION

Les attaques à but de déstabilisation ciblant des entités françaises ont été particulièrement nombreuses au cours de cette année. Fortement liées à l'actualité internationale, elles sont principalement l'œuvre de groupes *hacktivistes* cherchant à attirer l'attention. Les grands événements politiques ou sportifs constituent une caisse de résonance pour ces attaques, contribuant ainsi largement à leur objectif de déstabilisation.

Les groupes *hacktivistes* ont traditionnellement recours aux attaques par DDoS, à la défiguration de sites Web ou à la revendication d'exfiltration de données. Plus récemment, des tentatives de sabotage de petites installations industrielles ont été observées : si les conséquences de ces attaques restent limitées, elles représentent une évolution vers une logique de sabotage pour laquelle une vigilance s'impose.

1 SABOTAGE DE PETITES INSTALLATIONS INDUSTRIELLES

En 2024, plusieurs groupes *hacktivistes* ont revendiqué la prise de contrôle de petites installations industrielles, majoritairement utilisées pour la production d'énergie renouvelable. Ces attaques visaient des installations appartenant à des particuliers ou à des TPE/PME, et dont l'interface de gestion était exposée sur Internet sans authentification ou avec un mot de passe par défaut.

Ces attaques techniquement peu avancées sont exploitées surtout sur le plan médiatique. L'ANSSI observe ainsi une disproportion entre les revendications des attaquants et les conséquences des attaques : dans la grande majorité des cas, les *hacktivistes* ont exagéré l'impact de leurs actions dans le but d'accroître leur visibilité.

L'ANSSI considère que les actions mises en œuvre pour sécuriser les équipements industriels et réduire leur exposition sur Internet amoindrissent significativement les opportunités d'attaque.

Ciblage de petites installations industrielles

L'ANSSI a traité en 2024 de multiples signalements relatifs au ciblage par des groupes *hacktivistes* ayant un faible niveau de technicité mais une forte capacité à médiatiser leurs activités, d'entités des secteurs de la production d'énergie renouvelable et de l'assainissement de l'eau. Les opérateurs de Cyber Army of Russia Reborn (CARR) et Lulzsec Muslims sont notamment parvenus à accéder à des interfaces de gestion exposées sur Internet. L'action la plus aboutie a mené à l'arrêt pendant quelques heures d'un parc éolien, entraînant pour la victime une perte financière de quelques milliers d'euros.

Des revendications régulières de compromission d'équipements liés au secteur de l'eau ont été faites par des groupes *hacktivistes* pro-russes durant l'année 2024. Le secteur de l'eau, critique par essence à la fois pour la population et les industries, et cela d'autant plus dans le contexte des JOP 2024, a fait l'objet d'une attention particulière par des attaquants. CARR a notamment revendiqué des attaques de faible sophistication technique contre des systèmes industriels de microcentrales hydroélectriques, dont la prise de contrôle à distance de la centrale hydroélectrique de Courlon-sur-Yonne qui concernait en réalité le moulin de Courlandon [65]. Le groupe a par la suite revendiqué la prise de contrôle à distance d'une station italienne de traitement des eaux à Dittaino (Sicile) et annoncé le ciblage de stations d'épuration de la Seine en vue de perturber les épreuves des JOP 2024 qui devaient s'y dérouler. Les efforts de sensibilisation et l'accompagnement des entités susceptibles d'être ciblées ont permis qu'aucune attaque ne soit relevée sur ce périmètre durant les Jeux.

Les efforts de sécurisation sont en particulier à mener par les fabricants et distributeurs, qui doivent sensibiliser leurs clients aux problématiques de sécurité et communiquer des règles claires de mise en œuvre sécurisée des équipements. Par ailleurs, les installateurs, bien qu'étant souvent des professionnels du secteur, ne sont que rarement sensibilisés à mettre en œuvre les mesures d'hygiène informatique et de sécurité.

2 UNE INTENSITÉ ACCRUE DES ATTAQUES PAR DDOS

Les attaques par DDoS sont les attaques à but de déstabilisation les plus fréquentes. Très prisées par les *hacktivistes*, elles sont désormais utilisées par des acteurs aux profils divers (acteurs cybercriminels, mais aussi des groupes soutenus par des États).

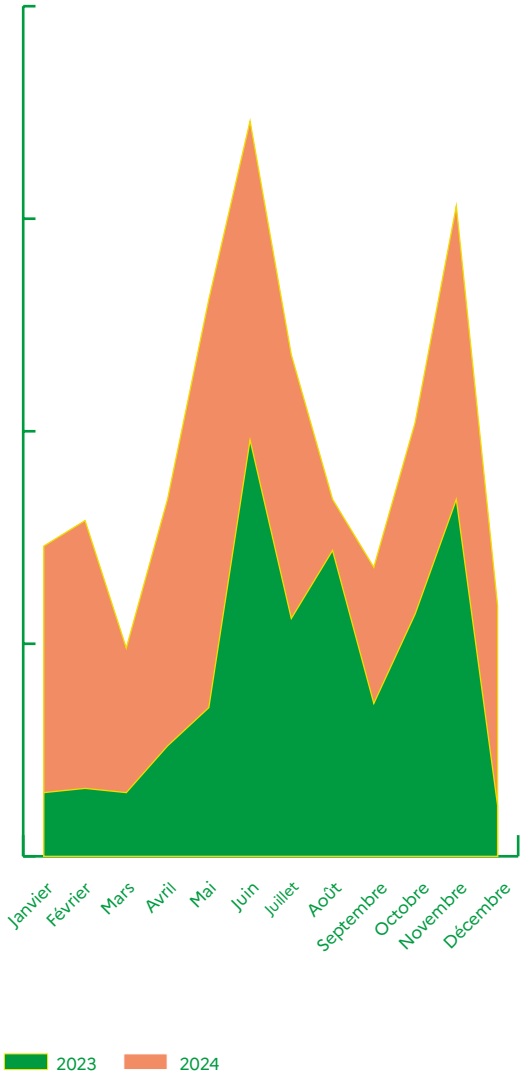
Des attaques par DDoS ont été menées en 2024 contre des entités françaises publiques comme privées avec une intensité marquée. Le graphique ci-contre illustre cette tendance, où l'on peut globalement observer un doublement de ce type d'attaque en 2024 par rapport à 2023, ainsi qu'une activité accrue pendant la période des JOP 2024.

Fait marquant de 2024, certaines rares attaques DDoS d'ampleur visant des infrastructures de télécommunications ont eu des conséquences importantes sur la disponibilité de services critiques.

Du 10 au 12 mars 2024, le Réseau interministériel de l'État (RIE) a ainsi été ciblé pendant plusieurs jours, avec des impacts significatifs sur l'activité de plusieurs ministères malgré les mesures de blocage rapidement mises en œuvre. À la suite de ces attaques, des mesures de sécurité complémentaires ont été prises par le RIE, notamment en prévision des JOP 2024.

L'hébergeur et opérateur de télécommunications OVH a également été visé par une attaque DDoS de très forte intensité, dont la finalité n'a pu être précisément démontrée faute de revendication [66].

Nombre d'attaques par DDoS observées par l'ANSSI contre des cibles françaises



NB.
Une attaque DDoS est considérée avec impact lorsqu'elle porte atteinte à la disponibilité du service visé

Ces attaques illustrent la capacité de nuisance ponctuelle des DDoS ciblant des infrastructures essentielles.

En septembre 2024, le Département de Justice des États-Unis a annoncé le démantèlement d'un réseau de bot (*botnet*) mondial composé de centaines de milliers d'appareils connectés, dont des caméras et appareils de stockage. Ce *botnet*, baptisé Raptor Train par l'entreprise Lumen, était mis au service du MOA réputé étatique Flax Typhoon, potentiellement opéré par l'entreprise chinoise Integrity Technology Group. *Raptor Train* était doté de capacités d'exploitation de vulnérabilités, de commande et contrôle, d'exécution de commande à distance ainsi que d'attaque par DDoS. Avant son démantèlement, ce réseau aurait été utilisé pour cibler plusieurs infrastructures critiques dans le monde, dont des entités taïwanaises et états-uniennes, dans un objectif de déstabilisation. [67] [68]

3 SABOTAGE ET PRÉ-POSITIONNEMENT[33] PAR DES ACTEURS AVANCÉS

En 2024, l'ANSSI n'a pas traité d'incident issu d'actions de sabotage par un acteur avancé. Ce type d'actions ciblant des SI critiques a plutôt été observé dans des contextes de tensions géopolitiques, mené par des acteurs étatiques ou engagés dans les conflits, afin de déstabiliser et amoindrir les capacités adverses voire appuyer des objectifs militaires.

Certains groupes *hacktivistes* pro-russes ou pro-ukrainiens revendiquent également des attaques à finalité destructrice. Ces dernières sont aussi potentiellement associées à des opérateurs étatiques, qui exploitent des canaux *hacktivistes* authentiques ou des faux-nez à des fins de publicité et d'influence.

En janvier 2024, le groupe *hacktiviste* pro-ukrainien BlackJack a revendiqué sur son canal Telegram la compromission de l'opérateur télécom moscovite M9com. Cette revendication s'inscrivait, d'après le groupe *hacktiviste*, dans les actions en représailles à l'attaque contre l'opérateur télécom ukrainien Kyivstar en décembre 2023, qui avait été revendiquée par le groupe *hacktiviste* pro-russe Solntsepëk[34]. Les *hacktivistes* pro-ukrainiens BlackJack auraient remplacé le nom du système autonome utilisé par M9com par « SLAVAUKRAINI-AS » [35] et publié des données présentées comme exfiltrées. L'attaque aurait détruit 20TB de données appartenant à M9com et aurait interrompu la fourniture d'accès à Internet d'habitants de Moscou [69]. D'après le média spécialisé *The Record*, l'attaque aurait été conduite en coopération avec le Service de sécurité d'Ukraine (SBU) [70]. Le SBU aurait déjà coopéré avec des groupes *hacktivistes* pro-ukrainiens par le passé, notamment lors de l'attaque contre la banque russe Alpha Bank en octobre 2023 [70].

Le CERT ukrainien (CERT-UA) [71] a décrit une campagne attribuée au MOA Sandworm qui a ciblé en mars 2024 une vingtaine d'entreprises des secteurs de l'énergie, de l'eau et de la fourniture de chaleur, dans dix régions d'Ukraine. Sandworm, également appelé APT44 [72], est un MOA réputé russe associé à des attaques à des fins d'espionnage et de sabotage contre plusieurs entités dans le monde, et notamment en Ukraine dans le cadre de la guerre déclenchée par la Russie. L'objectif de ces attaques, qui ont été déjouées, était de compromettre le fonctionnement des systèmes de contrôle industriel (ICS) des entités ciblées. Le CERT-UA est parvenu à prévenir les entités concernées et a contribué à contrer ces attaques informatiques avant que les codes de sabotage ne soient déclenchés. Il estime que cette campagne d'attaques avait pour objectif d'amplifier les effets des bombardements de certaines infrastructures énergétiques en Ukraine durant le printemps 2024. ←

33 Le pré-positionnement renvoie à la stratégie d'attaquants informatiques associés à des capacités étatiques, qui cherchent à s'introduire et se maintenir sur des systèmes critiques, potentiellement dans l'objectif de réaliser ultérieurement des actions de sabotage.

34 Le groupe Solntsepëk est décrit comme un faux-nez des opérateurs du MOA Sandworm, associé en sources ouvertes au service russe de renseignement militaire (GRU). [72].

35 (« GLOIRE A L'UKRAINE-AS »)

C
ESPIONNAGE

→ À l'instar des années précédentes, les attaques à finalité d'espionnage sont celles qui ont le plus mobilisé les équipes opérationnelles de l'ANSSI en 2024. Caractérisées par des périmètres de compromission larges et s'inscrivant sur le temps long, ces attaques demandent des moyens importants tant pour les investigations numériques que pour la remédiation et la caractérisation de la menace.

Les entités stratégiques, qu'elles appartiennent au périmètre gouvernemental ou constituent des infrastructures essentielles, sont des cibles récurrentes qui répondent aux objectifs d'espionnage stratégique des États adverses. Des cas de recompromissions et de poly-compromissions sont toujours observés, montrant la persévérance et les moyens que les acteurs à l'origine de ces attaques sont disposés à mobiliser pour arriver à leurs fins.

1 CIBLAGES LIÉS À DES INTÉRÊTS STRATÉGIQUES ÉTATIQUES

En 2024, des modes opératoires d'attaque réputés liés aux intérêts stratégiques russes ont été employés pour des compromissions à but d'espionnage. Ces campagnes d'attaques prennent place depuis février 2022 dans le contexte de la guerre en Ukraine et semblent orientées principalement par la recherche d'informations pouvant soutenir les efforts militaires ou diplomatiques russes.

Au cours de l'année, les opérateurs du MOA APT28, associé en sources ouvertes au service de renseignement militaire russe (GRU), ont poursuivi leurs attaques contre des secteurs d'intérêt stratégique pour la Russie, notamment en Ukraine et au sein des pays de l'OTAN. La victimologie associée à ces campagnes d'attaques comprend en 2024 des entités appartenant prioritairement aux secteurs gouvernemental, diplomatique, et de la recherche ou des *think tanks* [73]. Certaines campagnes ont été dirigées contre des entités publiques françaises. L'ANSSI constate que les campagnes associées au MOA APT28 semblent répondre à des besoins de renseignement stratégique immédiat et présentent des niveaux de sophistication variables. Certaines campagnes d'hameçonnage reposent sur des comptes légitimes compromis, des services de création d'adresses de messagerie temporaires ou encore de l'usurpation d'adresses légitimes. Les opérateurs mènent également des attaques par force brute contre des *webmails*. Les opérateurs du MOA APT28 ont également exploité des vulnérabilités, y compris jour-zéro (CVE-2023-23397).

D'autres campagnes associées à des MOA réputés liés à la Russie ont été observées en 2024. Ainsi, l'éditeur de sécurité Google TAG [45] a publié des informations concernant le MOA Nobelium [21], qui aurait été employé pour mener des campagnes d'attaques par point d'eau exploitant des sites gouvernementaux mongols en 2023 et 2024. Les attaquants auraient utilisé des kits d'exploitation de vulnérabilité similaires à ceux conçus par les entreprises productrices de logiciels de surveillance NSO Group et Intellexa. Cette campagne interroge sur la manière dont les opérateurs du MOA ont pu accéder à ces outils. En effet, les outils issus de l'écosystème de LIOP sont rarement utilisés hors du cadre de la relation entre les vendeurs et leurs clients, et les capacités offensives liées à la Russie sont connues pour être traditionnellement issues de son écosystème national. Le risque de prolifération issu de la commercialisation large d'outils offensifs par des entreprises privées, identifié de longue date par l'ANSSI, trouve ici une illustration nouvelle.

L'activité associée aux modes opératoires réputés chinois a été particulièrement dense et documentée au cours de l'année 2024. De larges secteurs et zones géographiques ont été ciblés à des fins de captation de renseignement d'ordre stratégique et économique. À titre d'exemple, plusieurs pays participant au sommet « ASEAN-Australia Special Summit » entre le 4 et le 6 mars 2024 auraient été ciblés par au moins deux MOA réputés chinois, dont

le MOA Mustang Panda [74]. Le secteur des transports a aussi été touché par ces activités d'espionnage.

Les modes opératoires associés par différents éditeurs de sécurité à la Chine auraient été employés en 2024 pour cibler le secteur du transport maritime en Europe, certains implants malveillants ayant été retrouvés sur des équipements embarqués [75]. L'Asie reste une région privilégiée du ciblage offensif lié aux MOA réputés chinois, ceux-ci ayant mené des attaques ciblant de nombreux secteurs gouvernementaux ou privés. Ainsi, le mode opératoire RedJuliette aurait notamment été employé contre de nombreuses cibles à Taïwan, dont des représentations diplomatiques [76].

Fait nouveau, des MOA employés dans des campagnes traditionnellement menées en Asie ont été observés ciblant en 2024 des entités situées en Afrique et dans les Caraïbes [77]. Enfin, plusieurs MOA réputés chinois ont également ciblé avec intensité le secteur des télécommunications notamment en France (voir section suivante).

Des acteurs offensifs réputés iraniens ont quant à eux été associés à des opérations d'espionnage à l'encontre de *think tanks*, d'organismes de recherche d'universités françaises [73]. Le MOA réputé iranien APT42 a été employé dans le cadre d'opérations d'espionnage et de surveillance d'individus, et dans une moindre mesure d'organisations, présentant une menace pour la stabilité du régime iranien[36]. Sa victimologie comprend des chercheurs, des journalistes, des dissidents, des membres de la diaspora iranienne, des représentants de gouvernements occidentaux, des *think tanks*, des universités et des organisations non gouvernementales (ONG). Néanmoins, depuis fin 2023, les activités associées au MOA semblent indiquer que les opérations d'espionnage à l'encontre d'entités comme les ONG, les centres de recherche et les universités représentent une part plus importante des activités de ses opérateurs. Cette activité a plus récemment été observée par Microsoft contre des entités localisées en Belgique, en France, à Gaza, en Israël, au Royaume-Uni et aux États-Unis [78].

2 CIBLAGE DU SECTEUR DES TÉLÉCOMMUNICATIONS

Le ciblage d'opérateurs de télécommunications à des fins d'espionnage est intense [1]. En France, l'ANSSI a traité des compromissions importantes de SI d'opérateurs de ce secteur à des fins d'espionnage, menées par des MOA ayant développé des techniques et outils avancés spécifiques à ce domaine.

Aux États-Unis, le MOA Salt Typhoon a été employé contre des infrastructures de télécommunications, et aurait notamment visé des dispositifs d'interception légale (voir focus page 43).

Le secteur des télécommunications dans son ensemble est ciblé de façon régulière et importante par les groupes d'attaquants réputés liés à la Chine, particulièrement en Asie. Les nombreuses compromissions décrites par les éditeurs de sécurité font état d'exfiltration de données, sans que la nature exacte de ces dernières ne soit toujours détaillée.

Ces deux dernières années, l'ANSSI a traité plusieurs incidents affectant des entités du secteur des télécommunications en France à des fins d'espionnage.

Parmi ces incidents figure la compromission du cœur de réseau mobile d'un opérateur de télécommunications. Le mode opératoire observé lors de cette compromission a pour caractéristiques principales d'avoir une bonne connaissance des protocoles de communication spécifiques au secteur et d'avoir concentré ses activités sur des équipements peu conventionnels ou rarement supervisés par des solutions de sécurité – témoignant ainsi de son niveau de sophistication ainsi que d'une forte

36 L'éditeur de sécurité américain Mandiant [81] établit avec un niveau de confiance fort que les opérateurs du MOA APT42 agissent pour le compte de l'Organisation du renseignement du Corps des Gardiens de la révolution islamique (IRGC-IO).

Salt Typhoon

Une campagne d'attaques menées au moyen du MOA Salt Typhoon ciblant les principales entités du secteur des télécommunications aux États-Unis a été rapportée septembre 2024. Plusieurs entreprises du secteur des télécommunications américaines auraient été compromises à des fins d'espionnage. À la suite de cette campagne, plus de 150 victimes auraient été alertées par le FBI. Les investigations toujours en cours laissent apparaître que l'usurpation d'un compte à très hauts privilèges et insuffisamment protégé a permis la prise de contrôle de 100 000 routeurs dans le monde. Les opérateurs du MOA auraient particulièrement ciblé la zone de Washington D.C. et pourraient avoir visé les systèmes d'interceptions légales dans l'objectif de connaître les agents chinois sous surveillance. [79].

capacité d'adaptation. Les investigations menées par l'ANSSI indiquent l'adéquation du mode opératoire avec des intérêts stratégiques étatiques.

L'Agence a également accompagné un opérateur dont les infrastructures de communications satellitaires ont fait l'objet d'une compromission en profondeur depuis plusieurs années. Durant cette attaque – probablement menée à des fins d'espionnage – l'attaquant était également en capacité de mener des actions de sabotage dont les conséquences auraient pu s'avérer critiques au vu des contraintes de haute disponibilité auxquelles sont soumises les infrastructures du secteur satellitaire. Les éléments issus des communications interceptées par l'attaquant ont potentiellement permis à ce dernier de mener d'autres attaques, ou ont pu bénéficier à d'autres groupes d'attaquants liés au même acteur stratégique. L'ANSSI estime très probable que le même acteur poursuive le ciblage de ce type d'infrastructure et préconise aux acteurs du secteur des télécommunications une prise en compte accrue de la menace.

L'ANSSI a enfin assisté un autre opérateur de télécommunications dans l'éviction d'un acteur malveillant présent depuis au moins décembre 2022 au sein de son SI. Le niveau de privilèges atteint par cet attaquant – connu pour concentrer son ciblage sur des entités de ce secteur d'activité – lui a conféré des capacités de latéralisation, d'espionnage et de sabotage au sein du SI de la victime. Les investigations de l'Agence ont notamment permis de confirmer une des finalités de l'attaque, à savoir l'interception de communications de cibles précises.

Les compromissions d'opérateurs de télécommunications sont susceptibles de porter atteinte à la confidentialité des données échangées par les clients. Toutefois, dans les attaques à but d'espionnage, les accès et privilèges obtenus par les attaquants leur permettent de réaliser des actions de sabotage, sans que cela n'ait été constaté par l'ANSSI en pratique. Les infrastructures satellitaires, traditionnellement utilisées comme moyen de communication de secours, sont très exposées à ce risque, en témoigne l'attaque subie par le réseau de communication satellitaire KA-SAT en 2022 [80].

Dans les attaques observées par l'ANSSI, les attaquants emploient fréquemment des codes malveillants développés pour des technologies ou des équipements très spécifiques. Le faible potentiel de réutilisation de ce type d'outil illustre l'importance des moyens mis en œuvre. Par ailleurs, dans ces compromissions, l'attaque a souvent été détectée plusieurs années après la compromission.

ANNEXES
BIBLIOGRAPHIE

[01] CERT-FR.
Panorama de la cybermenace 2023.
23 février 2024.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-001/

[02] GRANDS ÉVÈNEMENTS SPORTIFS EN FRANCE.
Évaluation de la menace 2024.
11 avril 2024.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-003/.

[03] THE NEW YORK TIMES.
Polish anti-doping agency targeted by cyber attack, 'fake' test results leaked.
14 août 2024.
https://www.nytimes.com/athletic/5700428/2024/08/14/polish-anti-doping-cyber-attack/

[04] SGDSN.
Synthèse de la menace informationnelle ayant visé les Jeux Olympiques et Paralympiques de Paris 2024.
13 septembre 2024.
https://www.sgdsn.gouv.fr/publications/synthese-de-la-menace-informationnelle-ayant-vise-les-jeux-olympiques-et-paralympiques

[05] FBI.
New Tradecraft of Iranian Cyber Group Aria.
30 octobre 2024.
https://www.ic3.gov/CSA/2024/241030.pdf

[06] IC3.
New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad.
30 octobre 2024.
https://www.ic3.gov/CSA/2024/241030.pdf

[07] CERT-FR.
L'ANSSI publie un corpus de guides dédiés à la remédiation d'incidents cyber.
16 janvier 2024.
https://cyber.gouv.fr/actualites/lanssi-publie-un-corpus-de-guides-dedies-la-remediation-dincidents-cyber

[08] CERT-FR.
Vulnérabilité dans Microsoft Netlogon.
11 mars 2021.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-020/

[09] SEKOIA.
Mamba 2FA: A new contender in the AiTM phishing ecosystem.
07 octobre 2024.
https://blog.sekoia.io/mamba-2fa-a-new-contender-in-the-aitm-phishing-ecosystem/

[10] CERT-FR.
Classe de vulnérabilités en environnement Active Directory.
15 octobre 2021.
https://www.cert.ssi.gouv.fr/dur/CERTFR-2021-DUR-001/

[11] CERT-FR.
Failles sur les équipements de sécurité : retour d'expérience du CERT-FR.
12 juin 2024.
https://www.cert.ssi.gouv.fr/uploads/20240612_NP_ANSSI-SDO_Retex-Vuln_vf.pdf

[12] FORTINET.
Burning Zero Days: Suspected Nation-State Adversary Targets Ivanti CSA.
11 octobre 2024.
https://www.fortinet.com/blog/threat-research/burning-zero-days-suspected-nation-state-adversary-targets-ivanti-csa

[13] UNION EUROPÉENNE.
Règlement (UE) 2024/2847 du Parlement Européen et du Conseil concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 20.
20 novembre 2024.
https://eur-lex.europa.eu/eli/reg/2024/2847/j?eliuri=eli%3Areg%3A2024%3A2847%3Aoj&locale=fr

[14] CERT-FR.
Signalements du CERT-FR.
https://www.cert.ssi.gouv.fr/signalements/

[15] CERT-FR.
Signalement de vulnérabilité significative ou d'incident affectant significativement un logiciel (Art. L. 2321-4-1 du code de la Défense).
https://www.cert.ssi.gouv.fr/signalement-vulnerabilite-incident-2321-4-1/

[16] CERT-FR.
Incident affectant les solutions AnyDesk.
15 avril 2024.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2024-ALE-003/

[17] L'USINE DIGITALE.
Cybersécurité : Après Boulanger, Cultura révèle une fuite de données clients.
10 septembre 2024.
https://www.usine-digitale.fr/article/cybersecurite-apres-boulanger-cultura-revele-une-fuite-de-donnees-clients.N2218245

[18] MANDIANT.
IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders.
22 mai 2024.
https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks/?hl=en

[19] LUMEN.
KV-Botnet: Don't call it a Comeback.
07 fevrier 2024.
https://blog.lumen.com/kv-botnet-dont-call-it-a-comeback/

[20] CISA.
MAR-10448362-1.v1 Volt Typhoon.
07 février 2024.
https://www.cisa.gov/news-events/analysis-reports/ar24-038a

[21] CERT-FR.
Malicious activities linked to the Nobelium intrusion set.
19 juin 2024.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-006/

[22] MICROSOFT.
Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard.
19 janvier 2024.
https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

[23] SECURITIES AND EXCHANGE COMMISSION.
Hewlett Packard Enterprise company.
19 janvier 2024.
https://www.sec.gov/Archives/edgar/data/1645590/000164559024000009/hpe-20240119.htm

[24] CERT-PL.
Russian Foreign Intelligence Service (SVR) Cyber Actors Use JetBrains TeamCity CVE in Global Targeting.
13 décembre 2023.
https://cert.pl/en/posts/2023/12/apt29-teamcity/

[25] MORPHISEC.
Unveiling UAC-0184: The Steganography Saga of the IDAT Loader Delivering Remcos RAT to a Ukraine Entity in Finland.
26 février 2024.
https://www.morphisec.com/blog/unveiling-uac-0184-the-remcos-rat-steganography-saga/

[26] CERT-UA.
UAC-200: Cyberattaques ciblées utilisant DarkCrystal RAT et Signal comme véhicule de distribution de confiance (CERT-UA #9918) - UAC-0200: Цільові кібератаки з використанням DarkCrystal RAT та Signal як засобу довіреного розповсюдження (CERT-UA#9918).
https://cert.gov.ua/article/6279561

[27] ESENTIRE.
Blind Eagle's North American Journey.
20 février 2024.
https://www.esentire.com/blog/blind-eagles-north-american-journey

[28] GOOGLE THREAT INTELLIGENCE GROUP.
Hybrid Russian Espionage and Influence Campaign Aims to Compromise Ukrainian Military Recruits and Deliver Anti-Mobilization Narratives.
28 octobre 2024.
https://cloud.google.com/blog/topics/threat-intelligence/russian-espionage-influence-ukrainian-military-recruits-anti-mobilization-narratives?hl=en

[29] BSI.
The state of IT security in Germany in 2024.
18 novembre 2024.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2024.pdf?__blob=publicationFile&v=5

[30] SENTINELONE.
ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware.
Juin 2024.
ChamelGang & Friends | Cyberespionage Groups Attacking Critical Infrastructure with Ransomware

[31] GOOGLE TAG.
We're All in this Together | A Year in Review of Zero-Days Exploited In-the-Wild in 2023.
Mars 2024.
https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf

[32] MICROSOFT.
Frequent freeloader part I: Secret Blizzard compromising Storm-0156 infrastructure for espionage.
04 décembre 2024.
https://www.microsoft.com/en-us/security/blog/2024/12/04/frequent-freeloader-part-i-secret-blizzard-compromising-storm-0156-infrastructure-for-espionage/

[33] ESET.
RomCom exploits Firefox and Windows zero days In-The-Wild.
26 novembre 2024.
https://www.welivesecurity.com/en/eset-research/romcom-exploits-firefox-and-windows-zero-days-in-the-wild/

[34] FORBES.
Exclusive: Israeli Surveillance Companies Are Siphoning Masses Of Location Data From Smartphone Apps.
11 décembre 2020.
https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/

[35] WALL STREET JOURNAL.
How ads on your phone can aid government surveillance.
13 octobre 2023.
https://www.wsj.com/tech/cybersecurity/how-ads-on-your-phone-can-aid-government-surveillance-943bde04

[36] KTLA.
LAPD using Israeli spy company to gather personal data, report says.
28 novembre 2023.
https://ktla.com/news/local-news/lapd-using-israeli-spy-company-to-gather-personal-data-report-says/

[37] IRISH COUNCIL FOR CIVIL LIBERTIES.
Europe's hidden security crisis.
https://www.iccl.ie/digital-data/europes-hidden-security-crisis/

[38] KREBSONSECURITY.
Stark Industries Solutions: An Iron Hammer in the Cloud.
23 mai 2024.
https://krebsonsecurity.com/2024/05/stark-industries-solutions-an-iron-hammer-in-the-cloud/

[39] SEKOIA.
NoName057(16)'s DDoSia project: 2024 updates and behavioural shifts.
23 février 2024.
https://blog.sekoia.io/Noname05716-Ddosia-project-2024-updates-and-behavioural-shifts/

[40] TEAM-CYMRU.
FIN7: The Truth Doesn't Need to be so STARK.
13 août 2024.
https://www.team-cymru.com/post/fin7-the-truth-doesn-t-need-to-be-so-stark

[41] CISA.
New Tradecraft of Iranian Cyber Group Aria.
30 octobre 2024.
https://www.ic3.gov/CSA/2024/241030.pdf

[42] SECURITY INTELLIGENCE.
Hive0051 goes all in with a triple threat.
09 avril 2024.
https://securityintelligence.com/x-force/hive0051-all-in-triple-threat/

[43] SEKOIA.
WebDAV-as-a-Service: Uncovering the infrastructure behind Emmenhtal loader distribution.
19 septembre 2024.
https://blog.sekoia.io/webdav-as-a-service-uncovering-the-infrastructure-behind-emmenhtal-loader-distribution/

[44] LE MONDE.
Le logiciel espion Pegasus détecté dans le téléphone de Nathalie Loiseau et d'une autre eurodéputée.
22 février 2024.
https://www.lemonde.fr/elections-europeennes/article/2024/02/22/le-logiciel-espion-pegasus-detecte-dans-le-telephone-de-nathalie-loiseau-et-d-une-autre-eurodeputee_6217981_1168667.html

[45] GOOGLE.
State-backed attackers and commercial surveillance vendors repeatedly use the same exploits.
29 août 2024.
https://blog.google/threat-analysis-group/state-backed-attackers-and-commercial-surveillance-vendors-repeatedly-use-the-same-exploits/

[46] MINISTÈRE DE L'EUROPE ET DES AFFAIRES ETRANGÈRES.
Processus de Pall Mall : Lutter contre la prolifération et l'usage irresponsable des capacités d'intrusion cyber disponibles sur le marché (Lancaster House, Londres, 6 février 2024).
06 février 2024.
https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/actualites-et-evenements-lies-a-la-securite-au-desarmement-et-a-la-non/2024/article/processus-de-pall-mall-lutter-contre-la-proliferation-et-l-usa

[47] SEKOIA.
Active Lycantrox infrastructure illumination.
02 octobre 2023.
https://blog.sekoia.io/active-lycantrox-infrastructure-illumination/

[48] GOOGLE.
Buying Spying: How the commercial surveillance industry works and what can be done about it.
06 février 2024.
https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/

[49] TECHCRUNCH.
Spyware startup Variston is losing staff — some say it's closing.
15 février 2024.
https://techcrunch.com/2024/02/15/variston-spyware-losing-staff-some-say-closing/

[50] TECHCRUNCH.
Lawyer allegedly hacked with spyware names NSO founders in lawsuit.
13 novembre 2024.
https://techcrunch.com/2024/11/13/lawyer-allegedly-hacked-with-spyware-names-nso-founders-in-lawsuit/

[51] AMNESTY INTERNATIONAL.
Indonesia: A web of surveillance: Unravelling a murky network of spyware exports to Indonesia.
01 mai 2024.
https://www.amnesty.org/en/documents/asa21/7974/2024/en/

[52] ZDNET.
Rançongiciels : pourquoi la justice française a ouvert moins de nouvelles enquêtes l'an passé.
06 janvier 2025.
https://www.zdnet.fr/actualites/rancongiciels-pourquoi-la-justice-francaise-a-ouvert-moins-de-nouvelles-enquetes-lan-passe-403845.htm

[53] RECORDED FUTURE.
RansomHub Draws in Affiliates with Multi-OS Capability and High Commission Rates.
20 juin 2024.
https://www.recordedfuture.com/research/ransomhub-draws-in-affiliates-with-multi-os-capability-and-high-commission-rates

[54] GROUP-IB.
RansomHub r ansomware-as-a-service.
28 août 2024.
https://www.group-ib.com/blog/ransomhub-raas/

[55] CISA.
#StopRansomware: RansomHub Ransomware.
29 août 2024.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a

[56] BLEEPINGCOMPUTER.
Germany takes down cybercrime market with over 180,000 users.
01 mars 2024.
https://www.bleepingcomputer.com/news/legal/germany-takes-down-cybercrime-market-with-over-180-000-users/

[57] LE MONDE.
BreachForums : le fondateur du plus important site de vente de données personnelles volées condamné par la justice.
20 janvier 2024.
https://www.lemonde.fr/pixels/article/2024/01/20/breachforums-le-fondateur-du-plus-important-site-de-vente-de-donnees-personnelles-volees-condamne-par-la-justice_6211870_4408996.html

[58] EUROPOL.
Law enforcement disrupt world's biggest ransomware operation.
20 février 2024.
https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[59] TRENDMICRO.
Unveiling the Fallout: Operation Cronos' Impact on LockBit Following Landmark Disruption.
03 avril 2024.
https://www.trendmicro.com/en_us/research/24/d/operation-cronos-aftermath.html

[60] CERT-FR.
Opération ENDGAME.
30 mai 2024.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-004/

[61] PARQUET DE PARIS.
Communiqué de presse.
2024.
https://www.linkedin.com/posts/parquet-de-paris_communiqu%C3%A9-de-presse-endgame-activity-7201856692140056576-v3jT

[62] EUROPOL.
LockBit power cut: four new arrests and financial sanctions against affiliates.
01 octobre 2024.
https://www.europol.europa.eu/media-press/newsroom/news/lockbit-power-cut-four-new-arrests-and-financial-sanctions-against-affiliates

[63] MINISTÈRE DE L'INTÉRIEUR.
Une lettre-plainte pour la violation des données personnelles via Viamedis et Almerys. Ministère de l'intérieur.
01 septembre 2025.
https://www.masecurite.interieur.gouv.fr/fr/actualites/lettre-plainte-vol-donnees-personnelles-viamedis-almerys

[64] CERT-FR.
Exfiltration de données du secteur social - retour d'expérience du CERT-FR.
24 septembre 2024.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-009/

[65] LE MONDE.
Comment Sandworm, les hackeurs d'élite de l'armée russe, ont piraté un moulin français en pensant attaquer un barrage.
17 avril 2024.
https://www.lemonde.fr/pixels/article/2024/04/17/comment-sandworm-les-hackeurs-d-elite-de-l-armee-russe-ont-pirate-un-moulin-francais-en-pensant-attaquer-un-barrage_6228320_4408996.html

[66] OVH.
The Rise of Packet Rate Attacks: When Core Routers Turn Evil.
01 juillet 2024.
https://blog.ovhcloud.com/the-rise-of-packet-rate-attacks-when-core-routers-turn-evil/

[67] U.S JUSTICE.
Departement of Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers.
18 septembre 2024.
https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state

[68] LUMEN.
Derailing the Raptor Train.
18 septembre 2024.
https://blog.lumen.com/derailing-the-raptor-train/

[69] REUTERS.
Hackers hit Moscow internet provider in response to Kyivstar cyber attack.
01 septembre 2024.
https://www.reuters.com/technology/cybersecurity/hackers-hit-moscow-internet-provider-response-kyivstar-cyber-attack-source-2024-01-09/

[70] THE RECORD.
Pro-Ukraine hackers claim breach of Russian internet provider.
09 janvier 2024.
https://therecord.media/ukraine-blackjack-hackers-sbu-claim-breach-russia-M9com

[71] CERT-UA.
Le mode opératoire UAC-0133 (Sandworm) prévoit un cyber-sabotage sur près de 20 infrastructures critiques en Ukraine (Плани UAC-0133 (Sandworm) щодо кібердиверсії на майже 20 об'єктах критичної інфраструктури України).
19 avril 2024.
https://cert.gov.ua/article/6278706

[72] MANDIANT.
APT44: Unearthing Sandworm.
2024.
https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf

[73] CERT-FR.
Organismes de recherche et think tanks - État de la menace informatique.
02 semptembre 2024.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-008/

[74] UNIT 42.
ASEAN Entities in the Spotlight: Chinese APT Group Targeting.
26 mars 2024.
https://unit42.paloaltonetworks.com/chinese-apts-target-asean-entities/

[75] ESET.
Iran - Aligned Cyberattacks: Rise in Disruptive Operations.
2024.
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2023-q1-2024.pdf

[76] RECORDED FUTURES.
Chinese State-Sponsored RedJuliett Intensifies Taiwanese Cyber Espionage via Network Perimeter Exploitation.
24 juin 2024.
https://www.recordedfuture.com/research/redjuliett-intensifies-taiwanese-cyber-espionage-via-network-perimeter

[77] CHECKPOINT.
Chinese Espionage Campaign Expands to Target Africa and The Caribbean.
23 mai 2024.
https://blog.checkpoint.com/research/chinese-espionage-campaign-expands-to-target-africa-and-the-caribbean/

[78] MICROSOFT.
New TTPs observed in Mint Sandstorm campaign targeting high-profile individuals at universities and research orgs.
17 janvier 2024.
https://www.microsoft.com/en-us/security/blog/2024/01/17/new-ttps-observed-in-mint-sandstorm-campaign-targeting-high-profile-individuals-at-universities-and-research-orgs/

[79] WALL STREET JOURNAL.
How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons.
04 janvier 2025.
https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95?msockid=30240784eaf162d40dae1208eb9e631d

[80] CERT-FR.
Panorama de la cybermenace 2022.
10 février 2023.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/

[81] MANDIANT.
APT42: Crooked Charms, Cons and Compromises.
Septembre 2022.
https://www.mandiant.com/sites/default/files/2022-09/apt42-report-mandiant.pdf

[82] APPLE.
À propos du mode Isolement.
https://support.apple.com/fr-fr/105120

[83] GOOGLE.
Bringing Access Back — Initial Access Brokers Exploit F5 BIG-IP (CVE-2023-46747) and ScreenConnect.
21 mars 2024.
https://cloud.google.com/blog/topics/threat-intelligence/initial-access-brokers-exploit-f5-screenconnect?hl=en

[84] HAARETZ.
Israel Tried to Keep Sensitive Spy Tech Under Wraps. It Leaked Abroad.
11 avril 2024.
https://www.haaretz.com/israel-news/security-aviation/2024-04-11/ty-article/.premium/israel-tried-to-keep-sensitive-spy-tech-under-wraps-it-leaked-abroad/0000018e-c948-d480-a99e-cf5f24900000

RESSOURCES

PANORAMA DE LA CYBERMENACE 2024

Édité par l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Direction artistique, maquette et illustrations : Cercle Studio (*www.cerclestudio.com*)

DÉPÔT LÉGAL

Février 2025

ISSN : 2970-4413

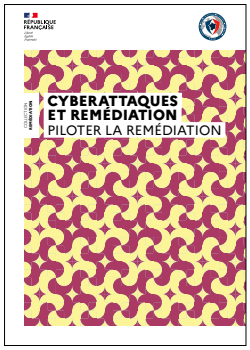
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

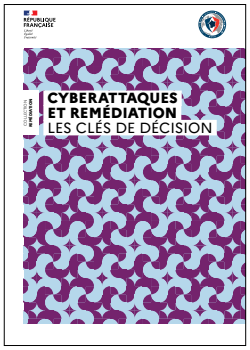
ANSSI
51 boulevard de la Tour-Maubourg
75700 PARIS 07 SP
www.cyber.gouv.fr
www.cert.ssi.gouv.fr
cert-fr@ssi.gouv.fr

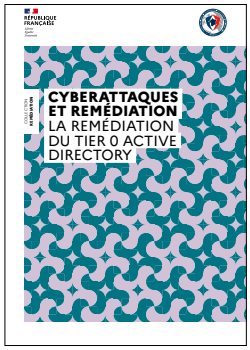
RETROUVEZ TOUS NOS GUIDES DE BONNES PRATIQUES SUR

www.cyber.gouv.fr/publications

Collection Cyberattaques et remédiation

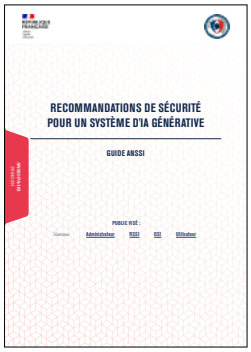


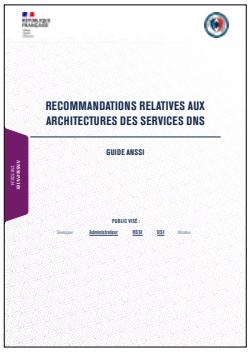


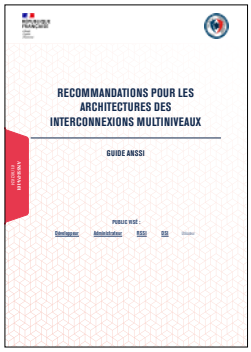


Collection Gestion de crise cyber

Les guides techniques







Retrouvez également les bulletins d'actualité, les alertes et les avis de sécurité, les fiches réflexes ou encore les états de la menace informatique sectorielle du CERT-FR sur *www.cert.ssi.gouv.fr*