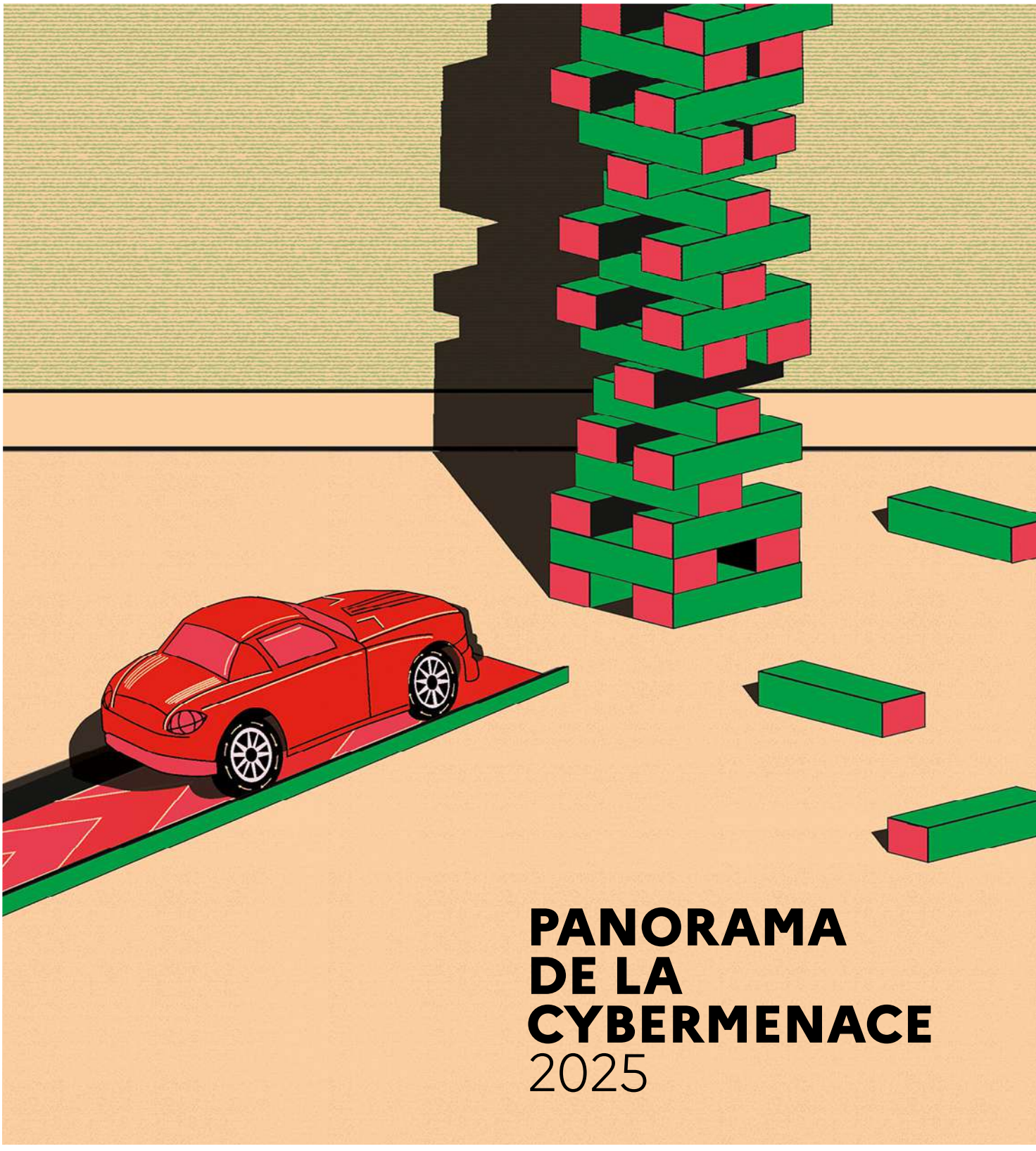
RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité



PANORAMA DE LA CYBERMENACE 2025

CERT-FR

2025

PANORAMA DE LA CYBERMENACE

ÉDITO

L'année 2025 s'est terminée sur un événement qui devrait collectivement nous alarmer : une série d'attaques informatiques coordonnées à visée destructive contre les infrastructures électriques polonaises. Il s'agit d'une première pour un État membre de l'Union européenne, alors que de tels événements constituent désormais le quotidien ukrainien. Si le pire semble avoir été évité, l'objectif était clair : provoquer des coupures d'électricité et de chauffage pour un nombre conséquent de citoyens. Cela illustre concrètement le scénario auquel la France se prépare[1] : une augmentation massive – d'ici 2030 – des attaques dites « hybrides », dont les cyberattaques constituent un pan majeur, avec des effets concrets voire destructeurs sur nos infrastructures critiques, et ce, en parallèle d'un engagement majeur des armées françaises en dehors du territoire national.

Après une année 2024 marquée par le caractère exceptionnel et la belle réussite de l'organisation et la tenue des Jeux Olympiques et Paralympiques de Paris 2024, il serait facile de croire que la pression créée par les attaquants du fait de l'événement est retombée : il n'en est rien. En 2025, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) constate un niveau de cybermenace qui reste élevé, qui n'épargne personne et qui est le fait d'attaquants toujours plus difficiles à suivre. Les frontières entre acteurs étatiques et cybercriminels s'érodent. Les attaquants se spécialisent mais partagent outils et méthodes, ils profitent de faiblesses dans des produits ou équipements peu supervisés, ils revendiquent bruyamment – et pas toujours sincèrement – ou se cachent silencieusement pour préparer des actions futures dont les objectifs inconnus doivent collectivement nous alarmer. En bref, s'il a toujours été complexe d'imputer une attaque informatique à un mode opératoire ou à un groupe d'attaquants, il est aujourd'hui également difficile de détecter et de faire sens de leurs traces dissimulées dans la complexité générale des environnements numériques.

C'est justement cette complexité que le *Panorama de la cybermenace* de l'ANSSI entend – au moins en partie – démêler et éclairer. Il le fait en levant le voile sur le travail des analystes en cybermenaces, essentiel dans la communauté de cyberdéfendeurs – pour prévenir les attaques, orienter les audits, alimenter les systèmes de détection d'intrusion ou nourrir la réponse aux incidents.

Pour autant, ce *Panorama* ne peut à lui seul constituer une vision exhaustive de toutes les cybermenaces qui ciblent la France. Il n'éclaire qu'une partie circonscrite des enjeux qui y sont associés et ajoute une pierre à l'édifice que constitue l'action de l'ensemble des acteurs de la cybersécurité : les éditeurs spécialisés, les centres de réponse à incident cyber, l'InterCERT France[2], le Groupement d'Intérêt Public Action contre la Cybermalveillance (GIP ACYMA), les campus cyber, ou encore les prestataires de confiance. L'articulation entre tous ces acteurs est un pan essentiel de la nouvelle stratégie nationale de cybersécurité 2026-2030, dont une des priorités est le renforcement de la résilience de la Nation. L'ANSSI n'est pas seule, et ne doit pas l'être dans ce contexte où la menace cyber est devenue systémique et touche l'ensemble du tissu économique et social du pays.

Établir un tel *Panorama* ne doit cependant pas nous décourager. Au contraire, mieux comprendre et anticiper les cybermenaces permet de nous doter d'outils efficaces pour lutter contre leurs effets. Les règlementations françaises et européennes – comme la transposition de la directive NIS2 ou la mise en œuvre du *Cyber Resilience Act* – en sont un axe essentiel. Elles permettent de définir et imposer des socles de mesures de sécurité et d'élever le niveau de maturité global de la Nation.

Nous avons les moyens de contrer, décourager ou au moins complexifier grandement la vie des attaquants.

Vincent Strubel
Directeur général de l'ANSSI

1
Revue nationale stratégique 2025.

2
Première communauté de centres de réponse à incident cyber en France.

AVANT-PROPOS

Le Panorama de la cybermenace est une production annuelle de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dans laquelle sont partagées de grandes tendances observées en matière de menace sur les systèmes d'information. Ce document ne se prétend pas exhaustif et représente une vision qui se base principalement sur les incidents marquants qui ont été traités ou portés à la connaissance de l'Agence.

Dans un contexte réglementaire qui se consolide, en particulier avec la transposition de la directive NIS2[3], il vise à la fois à sensibiliser et à contribuer aux réflexions de tous ceux qui s'intéressent aux questions de cybersécurité.

En 2025, les frontières qui existent traditionnellement entre acteurs étatiques et cybercriminels ont continué de s'éroder. L'émergence d'un brouillard technologique et organisationnel, qui avait déjà été soulignée dans la dernière édition du *Panorama*, tend à s'installer comme conséquence d'un partage de capacités plus prononcé entre ces acteurs, mais aussi de l'adoption croisée de pratiques qui caractérisaient jusqu'à présent davantage certains acteurs plus que d'autres.

3
Directive « *Network and Information Security* », ou « sécurité des réseaux et des systèmes d'information » en français.

Ainsi, le détournement, à des fins malveillantes, d'outils et de services légitimes, classiquement observé de la part d'acteurs réputés liés à des États, est en recrudescence parmi les acteurs cybercriminels. Si cela contribue à brouiller les pistes, les attaquants cherchent aussi à dissimuler leurs actions parmi des flux qui ne sont pas caractérisés comme malveillants et à échapper ainsi à la détection.

Cette tendance, associée à la répartition des tâches entre plusieurs acteurs qui se spécialisent chacun sur certaines phases de la compromission, complique aussi le processus d'imputation. Dans ce contexte qui oblige l'Agence à regarder à travers un écran de fumée, les fuites de données qui ont encore cette année affecté des opérateurs de modes opératoires d'attaques (MOA) réputés étatiques, des entreprises de lutte informatique offensive (LIO) ou des groupes cybercriminels, ont permis de mieux appréhender leur fonctionnement interne.

L'ANSSI constate un effort continu d'acteurs étatiques pour compromettre les réseaux des entités diplomatiques à des fins de collecte de renseignement stratégique, dans un contexte d'aggravation des tensions géopolitiques mondiales. Le ciblage d'infrastructures critiques, à l'image de celui des secteurs des télécommunications ou de l'énergie par exemple, reste aussi très prisé de ces acteurs. En particulier, cela leur permet d'obtenir des informations susceptibles de servir directement dans des campagnes d'attaques ultérieures.

En la matière, et dans la lignée des précédentes éditions du *Panorama*, les activités des MOA réputés liés aux services de renseignement russes ou chinois à l'encontre d'une variété de cibles ont encore été régulièrement observées.

Sur le volet cybercriminel, si le nombre d'attaques par rançongiciel est légèrement en baisse par rapport à 2024, le nombre d'incidents relatifs à des exfiltrations de données connus de l'ANSSI a significativement augmenté. Ces dernières sont parfois consécutives à la compromission d'un prestataire, qui peut elle-même résulter de la divulgation des secrets de comptes sur des forums cybercriminels.

Plus généralement, du fait de l'adoption croissante des services cloud par de nombreuses organisations, l'Agence a observé davantage de cas de compromission de ces environnements, pouvant aboutir au chiffrement des ressources et entraîner une indisponibilité temporaire de services pour des clients professionnels ainsi que pour des services grand public en France. Dans au moins un cas, l'attaquant a exploité une vulnérabilité présente sur un équipement de sécurité de bordure.

Comme les années précédentes, ces équipements ont été affectés par de nombreuses vulnérabilités, quand il ne s'agissait pas de faiblesses techniques inhérentes à leur conception. La compromission répétée de ces équipements a largement mobilisé les équipes de réponse à incident, soulignant ainsi les multiples enjeux relatifs à la gestion des vulnérabilités.

Enfin, le ciblage d'environnements mobiles a fait l'objet de plusieurs publications, notamment de la part de l'ANSSI dans une optique de sensibilisation plus large. Ce ciblage, portant autant sur des équipements personnels que professionnels, témoigne de capacités de recherche sophistiquées et d'une volonté d'atteindre un large panel d'utilisateurs. Les sociétés privées qui développent ces capacités sont susceptibles de les mettre à disposition de plusieurs commanditaires, ce qui peut augmenter le risque de prolifération et par conséquent une élévation du niveau global de la menace. ←

ÉLÉMENTS QUANTITATIFS

Comparatif du nombre d'incidents et signalements 2024/2025

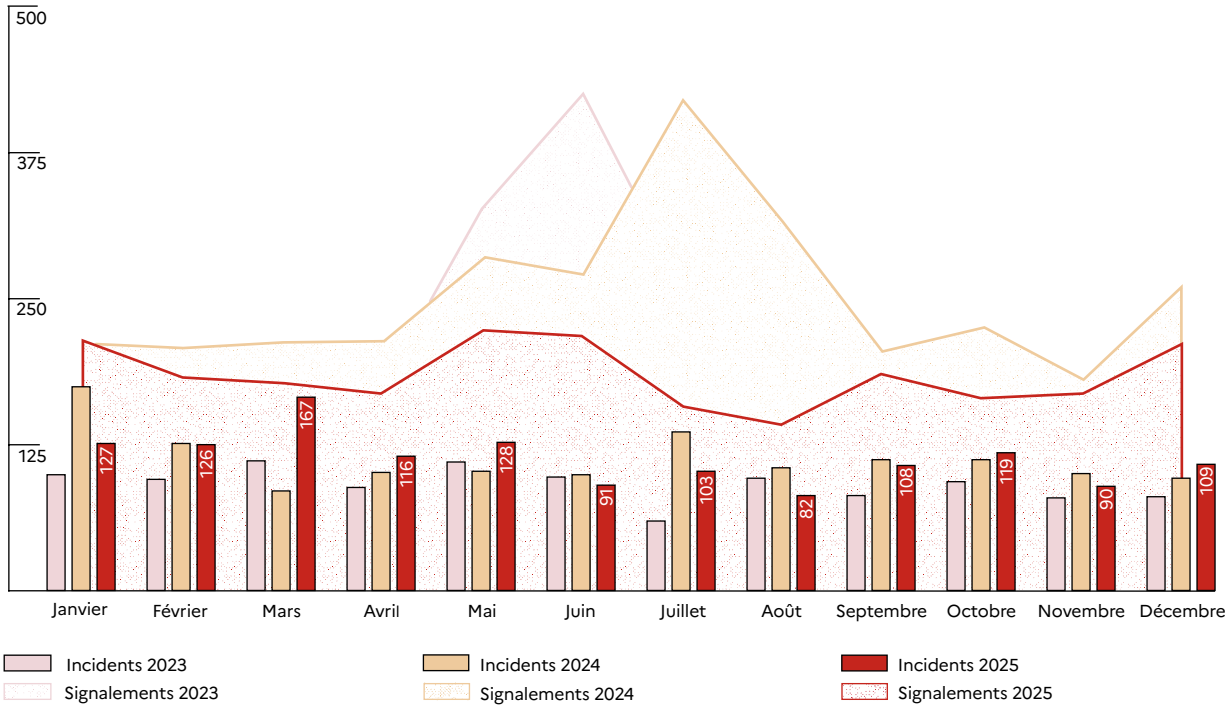
Au cours de l'année 2025, l'ANSSI a traité, avec un degré d'engagement variable, 3586 événements[4] de sécurité, soit une diminution de 18 % par rapport à l'année 2024. Cette diminution peut s'expliquer par la tenue des Jeux Olympiques et Paralympiques à Paris, qui avait suscité un pic de signalements[5] entre les mois de mai et d'août de cette année.

En 2025, sur l'ensemble des événements de sécurité, 1366 incidents[6] ont été portés à la connaissance de l'ANSSI, un nombre qui reste stable par rapport à 2024 (1361), après une croissance les années précédentes (1112 en 2023 et 831 en 2022).

Répartition sectorielle des incidents traités en 2025

En 2025, quatre secteurs d'activité concentrent 76 % des 1366 incidents portés à la connaissance de l'ANSSI : l'éducation et la recherche (34 %), les ministères et les collectivités territoriales (24 %), la santé (10 %) et les télécommunications (9 %). Ces quatre secteurs particulièrement affectés confirment la tendance observée depuis plusieurs années par l'Agence et qui peut être expliquée par le nombre important d'entités – notamment publiques – présentes dans ces différents secteurs. Ces chiffres correspondent à la vision de l'ANSSI consolidée par les signalements émis par ses bénéficiaires, et ne sont pas nécessairement représentatifs de l'ensemble des événements de sécurité qui touchent les différents secteurs d'activité en France.

Comparaison annuelle du nombre d'incidents et de signalements



4
Événements portés à la connaissance de l'ANSSI et qui ont donné lieu à un traitement par les équipes opérationnelles.

5
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 système d'information (SI).

6
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.

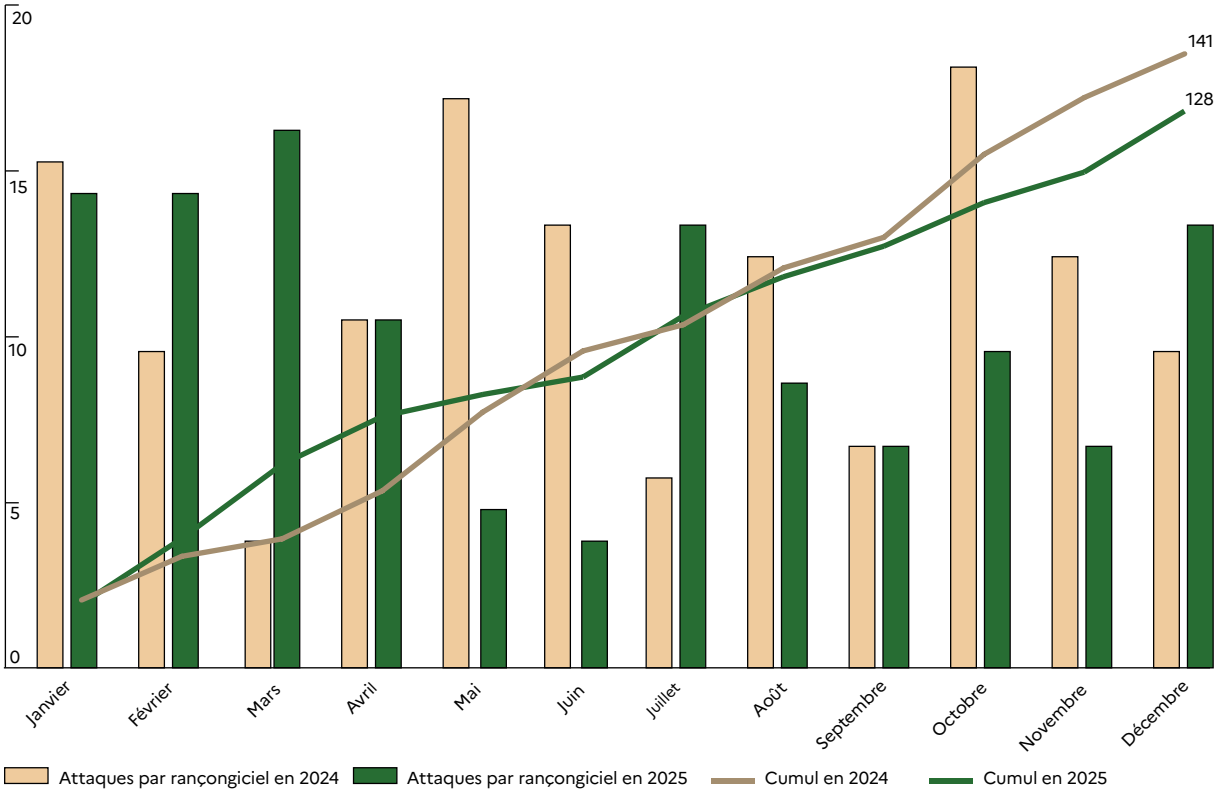
1

EXTORSION DE FONDS, ESPIONNAGE ET DÉSTABILISATION : LES MOTIVATIONS DES ATTAQUANTS

A
EXTORSION DE FONDS

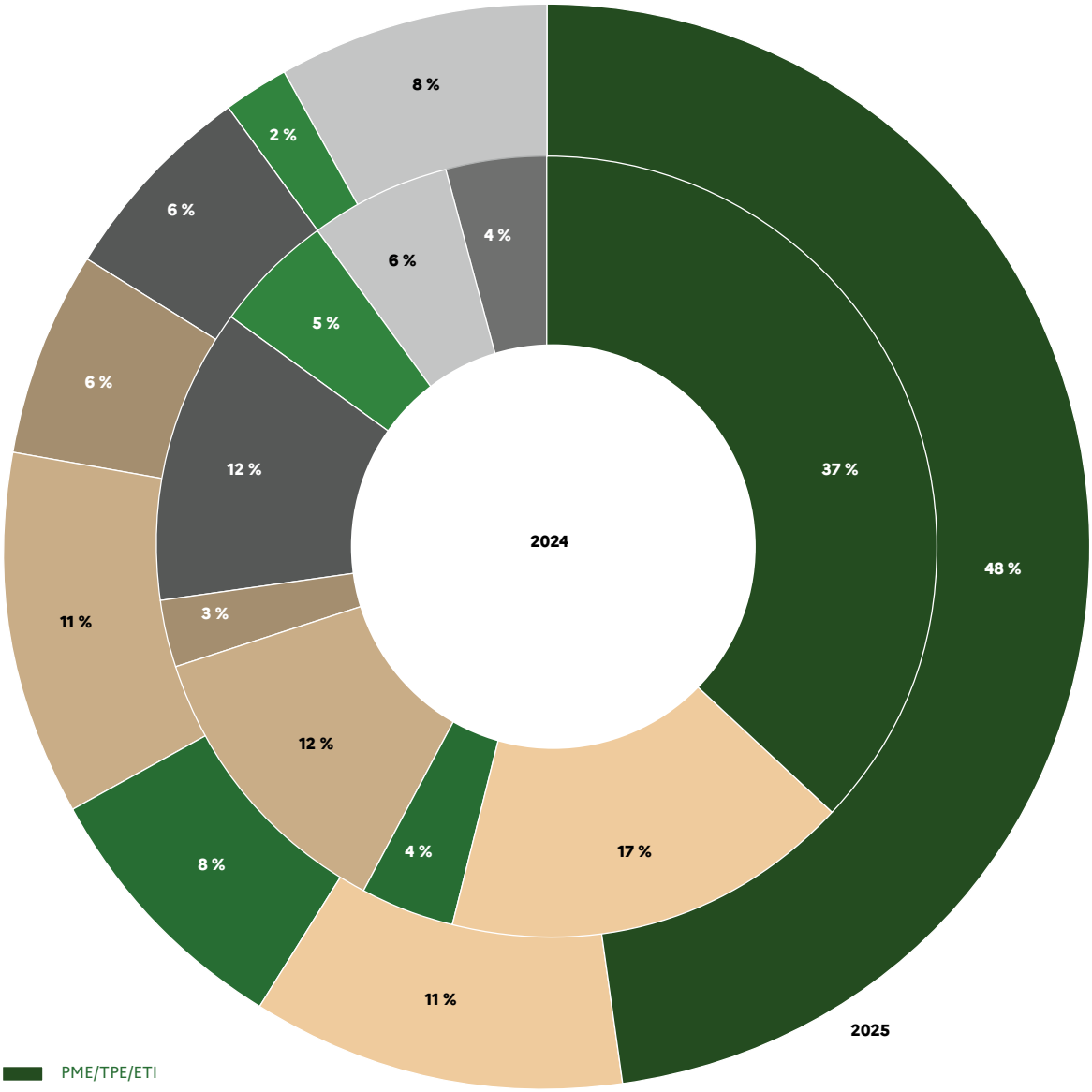
Différents profils d'attaquants mènent des attaques à motivation financière. Les attaquants cybercriminels continuent de mener des attaques par rançongiciel en pratiquant la double voire la triple extorsion[7] au détriment notamment d'entreprises de taille intermédiaire à très petite, de collectivités territoriales et d'établissements de soin ou d'enseignement français. Quelques groupes et acteurs cybercriminels favorisent toutefois l'exfiltration de données sans chiffrement. Par ailleurs, des attaquants étatiques habituellement connus pour des attaques à des fins d'espionnage ont été observés conduire des activités visant à extorquer des fonds.

Répartition mensuelle et cumulative par année du nombre de rançongiciels recensé par l'ANSSI



7
La double extorsion consiste à faire pression sur les victimes en exfiltrant et chiffrant les données de son système d'information d'une part et en menaçant de les divulguer d'autre part. Cette double approche peut être complétée par d'autres moyens de pression comme des attaques en déni de service distribué (DDoS) ou encore des tentatives d'extorsion auprès de partenaires ou de clients de l'entité victime dans des attaques dites par triple extorsion.

Répartition des victimes d'attaque par le biais d'un rançongiciel



1/PAR DES ACTEURS CYBERCRIMINELS

Les éditeurs de sécurité ou partenaires de l'ANSSI font état d'une accentuation de la tendance d'extorsion sans déploiement de rançongiciel au sein de l'écosystème cybercriminel. Si elle est également constatée, cette tendance reste encore limitée dans les incidents traités en 2025 par l'ANSSI.

Les rançongiciels[8]

En 2025, 128 compromissions par rançongiciel ont été portées à la connaissance de l'ANSSI. Ce nombre est légèrement en baisse par rapport à l'année 2024. Les compromissions par rançongiciels demeurent cependant une menace importante en France et représentent une part significative de l'activité cybercriminelle observée par l'Agence.

Si les PME/TPE/ETI restent la catégorie d'entités la plus affectée par des rançongiciels, la proportion d'incidents de ce type ayant touché des établissements de santé (8 %) est de nouveau en hausse par rapport à 2024. Plusieurs centres hospitaliers ont subi des perturbations de leurs activités d'accueil et de traitement de patients. Les petites structures de santé telles que les EHPAD et les cliniques sont également affectées par ce type d'incident. La part des collectivités territoriales (11 %) a en revanche légèrement diminué.

Fait notable, les établissements scolaires, notamment d'enseignement primaire et secondaire, ont été particulièrement touchés en 2025. Ces incidents ont pu avoir des impacts conséquents et visibles sur ces structures, forçant parfois la mise en œuvre d'un mode de fonctionnement dégradé pendant plusieurs semaines, avec notamment des difficultés d'accès à des ressources internes aux établissements.

Les acteurs cybercriminels mènent des attaques à l'aide de rançongiciels en ciblant indistinctement la plupart des secteurs et des zones géographiques. Ces attaques opportunistes peuvent cependant avoir des conséquences majeures en entraînant, entre autres, l'interruption des chaînes de production et des services fournis par la victime.

En octobre 2025, l'attaque de l'entreprise Collins Aerospace, revendiquée par le groupe cybercriminel Everest, a ainsi entravé le fonctionnement de plusieurs aéroports européens, entraînant des retards conséquents et des annulations de vols pendant plusieurs jours [1].

Les souches les plus représentées en 2025 sont Qilin (21 %), Akira (9 %) et Lockbit 3.0/Lockbit Black (5 %). En complément, plus d'une dizaine de souches (Nova, Warlock, Sinobi notamment) ont été observées pour la première fois en 2025 sur au moins un incident. Certaines anciennes franchises de *ransomware-as-a-service*[9] (RaaS) sont également parvenues à fidéliser leurs affiliés et à maintenir un haut niveau d'activité comme Akira, Inc Ransom et Qilin. Qilin est par ailleurs la franchise rançongiciel la plus populaire de l'année 2025 avec plus de 700 victimes revendiquées sur l'année, dont 185 en octobre 2025 [2].

8
Un rançongiciel est un code malveillant déployé par des attaquants dans l'objectif d'obtenir le paiement d'une rançon par la victime. L'attaquant empêche cette dernière d'accéder au contenu de ses fichiers – généralement en les chiffrant – et lui propose de lui fournir le moyen de déchiffrer ou récupérer les données contre le paiement de la rançon.

9
Ce terme désigne le 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.

→ L'opération de coopération judiciaire internationale ENDGAME lancée en mai 2024, a mené à plusieurs actions de démantèlement contre des infrastructures liées à des codes cybercriminels, deux d'entre elles ayant pris place en 2025 à 6 mois d'intervalle [3]. Ainsi la dernière occurrence, en novembre 2025, a donné lieu au démantèlement d'infrastructures se rapportant au code malveillant Rhadamanthys quand la première, en mai 2025, visait d'autres codes et notamment Lumma Stealer. Ces opérations ont impliqué les autorités allemandes, américaines, australiennes, britanniques danoises, françaises – coordonnées par l'Office anticybercriminalité de la police judiciaire – OFAC – et néerlandaises. Dans ce contexte, en collaboration avec l'OFAC, l'ANSSI apporte son soutien pour l'identification et la notification des victimes et partage des recommandations de sécurité.

Ces opérations illustrent le besoin de coopération internationale pour adresser la distribution de ces infrastructures malveillantes qui n'opèrent pas dans un strict respect des frontières. Par ailleurs, elles montrent aussi qu'au niveau national, la collaboration avec les forces de l'ordre et l'écosystème judiciaire offre une complémentarité permettant de nuire efficacement, au moins pendant un temps, aux groupes cybercriminels. En perspective, une dynamique de collaboration plus large, et en particulier avec les écosystèmes de CERTs[10], pourra contribuer à faire progresser l'efficacité de ces opérations notamment dans l'accompagnement des victimes. ←

Les enjeux de l'endiguement d'un incident de cybersécurité

Certaines entités subissent de lourdes conséquences à la suite de la mise en œuvre de mesures d'endiguement précipitées. À titre d'exemple, l'ANSSI a traité une compromission d'ampleur en 2025, détectée en amont du chiffrement du système d'information. Les dispositions hâtives prises par l'entité victime, notamment le débranchement électrique de son *data center*, ont entraîné un arrêt total et une perturbation de ses activités sur le long cours.

Ces mesures d'endiguement précipitées ont certes pu éviter une aggravation de l'incident, mais doivent être maîtrisées pour éviter des effets de bord :

- Un des premiers effets indésirables des actions de remédiation est l'absence de garantie de retour à l'état nominal dans le cas de redémarrage de systèmes complexes. En effet, une extinction brutale de matériels électroniques et d'applications peut en affecter le redémarrage et le fonctionnement. Par ailleurs, les conséquences engendrées sur l'activité et sa reprise doivent aussi être considérées – certains systèmes ont de fortes contraintes de disponibilité et la coupure en est donc redoutée ;
- Les interactions avec les systèmes compromis et a fortiori leur extinction peuvent altérer ou supprimer des traces de l'attaque. La compréhension de l'incident s'en trouve alors limitée. Ainsi, la neutralisation précoce d'un accès connu peut entraîner une perte de visibilité sur les actions adverses et l'impossibilité d'identifier l'ensemble des chemins d'accès utilisés par l'attaquant ;
- Enfin, chaque action effectuée sur un système compromis est potentiellement observée et interprétée par l'attaquant. En cas d'incident, l'usage est de privilégier l'extinction et l'isolation des systèmes compromis tout en révoquant les authentifiants utilisés par l'attaquant. Face à l'imminence d'une action destructive, la priorité est d'entraver les actions de l'adversaire. Cependant, ces actions engendrent à la fois des effets attendus et des effets de bord. Chacune d'elles nécessite donc un arbitrage par la cellule de gestion crise. La préparation à ces décisions est déterminante dans la capacité à faire face à un incident. L'élaboration en amont d'un plan de continuité d'activité (PCA) et d'un plan de reprise d'activité (PRA) est indispensable [4].

10
CERT : un *computer emergency response team* (CERT) ou *computer security incident response team* (CSIRT) est un centre d'alerte et de réaction aux attaques informatiques.

Les exfiltrations de données

Certains acteurs cybercriminels exfiltrent des données sans déployer de rançongiciels. Ces acteurs malveillants monétisent leurs attaques en revendant les données à d'autres acteurs à des fins de compromission ultérieure, à l'image des courtiers en accès initiaux, ou utilisent ces données pour extorquer directement les victimes. D'autres exfiltrations de données sont réalisées par des acteurs *hacktivistes* dans le cadre d'opérations de déstabilisation.

En 2025, l'ANSSI a été informée de 196 incidents relatifs à des exfiltrations de données associées ou non à des attaques par rançongiciels. En comparaison, 130 incidents de ce type avaient été traités par l'ANSSI en 2024. Ces actions malveillantes sont souvent publiquement revendiquées, notamment sur des forums cybercriminels ou sur des réseaux sociaux comme Telegram. Néanmoins, il arrive régulièrement que ces revendications reprennent des données publiques ou précédemment divulguées. Ainsi, l'ANSSI n'a été en mesure de confirmer la véracité que de 80 revendications d'exfiltrations de données parmi toutes celles portées à sa connaissance.

Certains acteurs cybercriminels exfiltrent des données sans déployer de rançongiciels à l'image du groupe cybercriminel Cl0p. Ce groupe cybercriminel, actif depuis 2019 exploite régulièrement des vulnérabilités affectant des solutions de transfert de fichiers sécurisées. En août 2025, Cl0p a exploité la vulnérabilité jour-zéro CVE-2025-6182 de la solution Oracle E-Business Suite pour exfiltrer les données de centaines d'entreprises à travers le monde, notamment en France [5]. Cette tendance de chantage à la publication de données sans déploiement de rançongiciel, observée depuis plusieurs années par l'Agence, s'est accentuée mais reste encore limitée.

D'autres acteurs malveillants monétisent leurs attaques en revendant les données exfiltrées à des fins de compromission ultérieure, à l'image des courtiers en accès initiaux (*Initial Access Broker* ou IAB). Positionnés en début de chaîne d'infection, ces IAB et les clusters de distribution sont des intermédiaires indispensables de l'écosystème cybercriminel notamment celui des rançongiciels.

En parallèle, l'ANSSI a constaté un recours récurrent aux *infostealers*[11] dans les attaques ayant conduit à des fuites de données. Plusieurs entreprises du secteur de l'agroalimentaire ont ainsi identifié en février 2025 la présence de l'*infostealer* EpiBrowser sur de nombreux postes de travail de leurs employés. Le déploiement de ce code malveillant est la conséquence de l'installation d'un logiciel gratuit se présentant comme un navigateur Chromium. Une fois installé sur le poste victime, le programme malveillant redirige les recherches, affiche des publicités malveillantes et collecte les identifiants et mots de passe renseignés par la victime. Il est parfois difficile pour les entités victimes de réagir face à ce type d'attaques dont elles ne maîtrisent pas toujours le vecteur d'intrusion notamment en l'absence de cloisonnement des usages professionnels et personnels.

Les fuites de données

Des éléments parfois considérés comme peu sensibles individuellement peuvent être plus critiques une fois agrégés. Il convient cependant de différencier les fuites de données personnelles d'usagers ou d'utilisateurs des fuites de données métiers, dont la criticité peut être très variable pour les entités victimes. Ces exfiltrations de données – quelle que soit leur nature – et leur médiatisation font peser un risque réputationnel substantiel sur les victimes. Ces dernières risquent de perdre la confiance de leurs usagers, utilisateurs ou de leurs clients, ou voir leur survie économique affectée.

De surcroît, le traitement d'une revendication d'exfiltration de données nécessite un engagement important des victimes, que la compromission soit avérée ou non et quel que soit le niveau de sophistication des actions attaquantes. Les données prétendument exfiltrées doivent être qualifiées afin d'en identifier la source et le cas échéant d'évaluer l'impact de leur fuite.

Les données publiées par des attaquants peuvent par ailleurs provenir d'anciennes fuites ou de sources multiples. Une fois une exfiltration avérée, outre les actions de réponse à incident, les victimes doivent également procéder aux communications éventuelles vers les entités affectées et répondre à leurs obligations réglementaires, comme la déclaration de l'incident auprès de la CNIL. La reprise médiatique des revendications des attaquants peut engendrer une pression supplémentaire.

L'ANSSI accompagne ses bénéficiaires dans la gestion de ce type d'incidents tout en œuvrant également à leur prévention. À cet égard, des recommandations ont été publiées sur le site du CERT-FR [6].

11
Un *infostealer* est un code malveillant conçu pour collecter des informations sur le poste de travail de la victime, notamment des authentifiants enregistrés dans les navigateurs Web, des adresses de portefeuille de crytoactifs, des cookies de session, etc.

2/PAR DES ACTEURS ÉTATIQUES

Depuis plusieurs années, l'ANSSI a connaissance d'attaques menées par certains acteurs étatiques dont l'objectif est le gain financier, comme les opérateurs de MOA réputés nord-coréens, qui ciblent les cryptoactifs. En 2025, à plusieurs reprises, des MOA réputés liés à des États ont mis en œuvre des rançongiciels dont certains habituellement déployés comme RaaS. Par exemple, le MOA réputé lié à la Corée du Nord Moonstone Sleet aurait été employé pour déployer le RaaS Qilin dans un nombre limité d'attaques en 2025 [7]. Si les modes opératoires liés à la Corée du Nord sont connus pour déployer régulièrement des rançongiciels comme Maui entre mai 2021 et juillet 2022 [8], leur utilisation de RaaS habituellement déployés par des groupes cybercriminels représente une tendance nouvelle.

L'utilisation de rançongiciels à des fins d'extorsion par des MOA réputés chinois semble aussi être une tendance relativement nouvelle, observée à plusieurs reprises en sources ouvertes et par l'Agence au cours de l'année 2025. Ces attaques à finalités lucratives ne sont pas une nouveauté en soi : en 2012, les opérateurs du MOA réputé chinois APT41 ciblaient déjà l'industrie des jeux vidéo dans ce but [9].

À partir du deuxième semestre de l'année 2024, une campagne d'attaques mêlant des activités d'espionnage et le déploiement d'un rançongiciel appelé NailaoLocker a été rapportée en sources ouvertes [10] [11] [12]. Le MOA associé par les éditeurs de sécurité à cette campagne d'attaques, est connu de l'ANSSI depuis 2016 pour ses opérations motivées par la collecte de renseignement stratégique, notamment au travers d'attaques par la chaîne d'approvisionnement [13] ; en revanche, l'utilisation d'un rançongiciel marque un changement important dans ses techniques, tactiques et procédures (TTP) connues.

De même, le rançongiciel RA World aurait été observé dans des chaînes de compromission en parallèle d'autres outils habituellement associés à des MOA réputés chinois comme PlugX. Depuis juillet 2024, ces mêmes codes malveillants auraient été utilisés à la fois pour des attaques à des fins d'espionnage et des attaques à des fins d'extorsion de fonds, à l'encontre de victimes en Asie. Une rançon aurait par ailleurs été réclamée et une négociation menée entre la victime et l'attaquant [14]. ←


DONNÉES
DONNÉES

B
CIBLAGE À DES FINS DE RENSEIGNEMENT PAR DES ATTAQUANTS RÉPUTÉS RUSSES ET CHINOIS

→ Les attaques informatiques menées à des fins d'espionnage sont le plus souvent menées contre des entités liées au périmètre gouvernemental ou fournissant des services essentiels, ou contre des individus qui constituent des cibles d'espionnage stratégique d'intérêt pour des États adverses. Au cours de l'année 2025, ces types d'attaques ont continué de mobiliser les équipes opérationnelles de l'ANSSI.

1/CIBLAGE À DES FINS D'ESPIONNAGE STRATÉGIQUE

Les activités d'espionnage des MOA réputés liés aux services de renseignement russes ou chinois sont régulièrement rapportées par différentes sources à l'encontre d'une grande variété de cibles appartenant aux secteurs gouvernementaux, mais également de membres d'organisations non gouvernementales (ONG), de médias et journalistes, des entités des secteurs de la cybersécurité ainsi que de la base industrielle et technologique de défense (BITD).

En mars 2025, des membres de l'ONG française Reporters Sans Frontières (RSF) auraient été la cible de courriels d'hameçonnage. Les investigations menées par l'ONG et l'éditeur de sécurité Sekoïa ont permis d'associer ce ciblage au MOA réputé lié à l'État russe Callisto[12]. Ce MOA est employé pour cibler des entités des secteurs gouvernemental, académique, de la défense, des groupes de réflexion, des journalistes et des organisations non gouvernementales notamment en Europe, en Amérique du Nord et dans le Caucase [15] [16] [17] [18].

En mai 2025, deux agences gouvernementales néerlandaises (AIVD et MIVD) [19] ont fait état dans une publication de l'identification d'un nouveau MOA potentiellement aligné sur les intérêts de l'État russe, baptisé Laundry Bear. Ce MOA serait utilisé depuis 2024 lors d'attaques informatiques à des fins d'espionnage contre des entités gouvernementales, non gouvernementales, militaires, des entreprises de la BITD et de l'aérospatial, des organisations sociales, culturelles et de l'éducation, des médias, et dans une moindre mesure contre des infrastructures critiques, ainsi que des fournisseurs de services numériques dans les pays de l'Union Européenne et de l'OTAN.

En lien avec cette publication, entre 2023 et 2024, l'ANSSI a traité des incidents ayant affecté des entités françaises du secteur gouvernemental et des médias et qui pourraient être liés au MOA Laundry Bear, d'après les investigations techniques menées par l'ANS. Dans le cadre de ces incidents, des attaques par pulvérisation de mots de passe auraient été menées contre des panels d'authentification à des comptes de messagerie. L'infrastructure

12
Le MOA Callisto, actif depuis au moins 2015, est attribué par différentes sources au service de renseignement intérieur russe (FSB).

associée à ces attaques reposait notamment sur des services de proxy commerciaux, des services VPN ainsi que sur le réseau TOR. Afin d'atténuer le risque de détection, les opérateurs du MOA ont également exfiltré des comptes de messageries pendant des heures et jours de travail ouvrés.

En outre, en 2024 et 2025, plusieurs éditeurs de sécurité et agences gouvernementales ont observé le ciblage d'infrastructures critiques au moyen de MOA réputés liés à la Chine. Le 28 mai 2025, le ministère tchèque des Affaires étrangères a attribué une attaque informatique menée contre une infrastructure critique de ce pays à des opérateurs du MOA réputé chinois APT31, associé publiquement [20] à une entreprise travaillant au profit du ministère de la Sécurité d'État [21]. L'éditeur de sécurité Talos a également observé les opérateurs du MOA UAT-5918, actif depuis au moins 2023, compromettre des infrastructures critiques à Taïwan à des fins d'espionnage, en exploitant des vulnérabilités sur des services Web exposés, par l'utilisation notamment des outils disponibles en sources ouvertes [22].

La compromission du réseau fédéral de l'armée américaine, de mars à décembre 2024, par les opérateurs du MOA réputé chinois Salt Typhoon, s'inscrit dans la continuité des activités observées en 2024 contre le secteur des télécommunications. Les attaquants pourraient notamment avoir obtenu des informations à caractère personnel, des identifiants d'accès administrateurs et des schémas d'architecture réseau, qui pourraient servir aux attaquants dans le cadre de campagnes ultérieures. Outre le secteur des télécommunications, Salt Typhoon aurait été employé pour cibler une douzaine d'autres secteurs en 2024 aux États-Unis : énergie, communications, transports et traitement de l'eau. Au moins un fichier de configuration exfiltré aurait par la suite servi dans le cadre de la compromission d'une autre agence gouvernementale américaine [23]. L'élargissement de la victimologie associée au MOA Salt Typhoon a également été observée par l'ANSSI en France, et l'ANSSI a aussi pu observer un équipement informatique compromis être utilisé comme rebond afin de mener une autre attaque. Ces méthodes et observations compliquent l'analyse du ciblage et des objectifs des attaquants. L'ANSSI n'est ainsi pas en mesure de déterminer à date si le MOA Salt Typhoon poursuit un ciblage stratégique du secteur des télécommunications ou un ciblage plus opportuniste lié aux équipements, plus répandus, utilisés par les opérateurs de communications électroniques.

2/DES ENTITÉS DIPLOMATIQUES PARTICULIÈREMENT CIBLÉES

L'ANSSI constate un effort continu d'acteurs étatiques pour compromettre les réseaux des entités diplomatiques à des fins de collecte de renseignement stratégique, dans un contexte d'aggravation des tensions géopolitiques mondiales. En 2025, l'ANSSI a ainsi assisté une entité française liée à un organe diplomatique victime de la compromission de son système d'information. L'acteur étatique a

pris pied sur le SI via l'exploitation de vulnérabilités d'équipements de bordure, puis s'est octroyé un niveau de privilèges élevé sur ce dernier, à des fins d'espionnage.

Un rapport publié par l'éditeur de sécurité Microsoft en juillet 2025 a ainsi mis en évidence le ciblage d'ambassades localisées à Moscou à des fins d'espionnage depuis au moins 2024 par les opérateurs du MOA Turla[13]. Dans le cadre de cette campagne, les opérateurs de Turla utiliseraient la technique *Adversary-in-the-middle*[14] pour déployer une chaîne de compromission conduisant notamment à la distribution du code malveillant ApolloShadow. Ce code malveillant permettrait aux attaquants d'obtenir des privilèges élevés leur permettant d'assurer une présence persistante sur les appareils compromis et potentiellement d'exfiltrer des informations. Selon l'éditeur de sécurité, cette campagne représenterait notamment un risque pour le personnel diplomatique présent à Moscou et ayant recours aux fournisseurs d'accès Internet ou services de télécommunications locaux. En effet, la mise en œuvre de ces attaques serait facilitée par le « système pour les activités opérationnelles d'enquête » (SORM), un système d'interception légale des télécommunications contrôlé par le service de renseignement intérieur russe (FSB) et qui aurait déjà été utilisé pour surveiller des opposants politiques [24].

Ce ciblage présente des similitudes avec un incident traité en 2022 par l'ANSSI, lié à une attaque contre un réseau diplomatique, vraisemblablement menée à des fins d'espionnage par des attaquants employant un MOA réputé russe. Tout en cherchant à exfiltrer des communications, les attaquants avaient pu obtenir une connaissance fine du réseau de communication compromis, susceptible d'être réutilisée lors d'attaques ultérieures.

En outre, des MOA réputés liés à la Chine sont régulièrement utilisés pour cibler des entités diplomatiques. En mars 2025, le MOA réputé chinois UNC6384 aurait été utilisé à l'encontre d'entités diplomatiques en Asie du Sud-Est et en Europe. Les opérateurs du MOA auraient notamment ciblé la Hongrie, la Belgique, l'Italie ou encore la Serbie au moyen de courriels d'hameçonnage utilisant des thématiques liées à l'OTAN ou à la Commission européenne. Selon Google Threat Intelligence Group (GTIG), ce MOA serait lié au MOA réputé chinois Mustang Panda, en raison de similarités dans la victimologie de leurs compromissions, à des outils et techniques, tactiques et procédures (TTP) utilisés, ainsi qu'à un recoupement observé dans les serveurs de commande et contrôle (C2[15]) employés. Les opérateurs auraient notamment distribué les codes malveillants StaticPlugin, CanonStager et PlugX [25] [26].

L'ANSSI a de son côté observé une campagne rattachée au cluster RedDelta – lié au MOA Mustang Panda – menée en septembre 2025 à l'encontre de plusieurs entités diplomatiques européennes, dont la France. RedDelta était notamment jusqu'ici connu pour être utilisé pour cibler des entités diplomatiques en Europe centrale et orientale ainsi qu'en Asie. ←

13
Le MOA Turla, actif depuis au moins 2004, est attribué par différentes sources au 16e Centre du service de renseignement intérieur russe (FSB). Ce MOA est employé pour cibler des entités des secteurs gouvernementaux, dont la diplomatie et le secteur de la défense en Europe, notamment en Ukraine, et en Amérique du Nord (sources : US, UK, Estonie, Tchéquie, Kaspersky, Trend Micro).

14
Une attaque par *Adversary-in-the-middle* est une forme plus évoluée des attaques dites *Man-in-the-middle* ou Homme-au-milieu en français. Elles vont au-delà d'une interception passive des communications entre deux parties, pour collecter ou manipuler des données permettant ensuite de mener d'autres actions offensives.

15
C2 (ou Command & Control) désigne l'infrastructure de serveurs et de logiciels utilisée par un attaquant pour piloter à distance des services compromis.

C
DÉSTABILISATION : OPÉRATIONS DE SABOTAGE ET DÉNIS DE SERVICE

→ Si l'espionnage peut rendre possible aux attaquants un pré-positionnement latent et durable, il peut être également une étape préalable à des opérations à but de sabotage.

1/POURSUITE DES ACTIVITÉS DE SABOTAGE RUSSES CONTRE L'UKRAINE

L'ANSSI suit les attaques informatiques susceptibles d'être le fait de la Russie (voire dans certains cas attribuées à la Russie), dans un objectif d'anticipation de la menace à des fins de déstabilisation, susceptible de cibler la France en tant que pays soutenant l'Ukraine mais également dans le contexte d'organisation de grands évènements en 2026 et 2027 (élections, présidence du G7, etc.).

En Ukraine, ces attaques ont, en 2025, toujours été menées à des fins de sabotage et de destruction, et s'inscrivent dans une stratégie adoptée dès le début de la guerre d'agression de la Russie contre l'Ukraine en 2022. Elles ciblent notamment des infrastructures critiques à l'aide de codes de sabotage (*wipers*). Certains de ces codes sont rattachés par des éditeurs de sécurité à des attaquants d'origine russe disposant de capacités avancées et présentent des similarités avec des codes rattachés au MOA Sandworm (réputé lié au service russe de renseignement militaire)[16] employés au début de l'invasion à grande échelle de l'Ukraine en 2022.

La poursuite d'attaques informatiques à des fins de sabotage en Ukraine montre la persistance de l'effort mis par des acteurs offensifs réputés liés aux intérêts stratégiques russes dans le développement de capacités de sabotage qui peuvent également être utilisées hors de l'Ukraine. Ainsi, l'éditeur de sécurité Microsoft a décrit une campagne baptisée BadPilot associée à un sous-groupe du mode opératoire Sandworm, actif depuis au moins 2021 [27], qui montre le ciblage d'entités en Ukraine, en Europe, aux États-Unis, en Asie centrale et au Moyen-Orient appartenant à des secteurs critiques (énergie, agriculture, ferroviaire, etc.). Les attaquants opèreraient en scannant Internet à la recherche d'équipements de bordure vulnérables afin de garantir leur accès initial, l'implantation de moyens de persistance et la latéralisation au sein du réseau de la victime. Dans au moins trois cas, l'obtention de ces accès initiaux aurait permis la conduite d'attaques destructrices qui ont par la suite été attribuées au MOA réputé russe Sandworm. La Pologne a fait l'objet à la fin 2025 d'attaques coordonnées à but de déstabilisation sur ses infrastructures énergétiques, qu'elle a imputées à des acteurs liés à la Russie. [28]

2/ATTAQUES PAR DÉNI DE SERVICE ET SABOTAGE DE PETITES INSTALLATIONS INDUSTRIELLES PAR DES GROUPES *HACKTIVISTES*

Les *hacktivistes* ne se limitent plus nécessairement aux attaques de type déni de service distribué (DDoS), à la défiguration de site web et à l'exfiltration de données. Ainsi, l'ANSSI constate en 2025 la poursuite des tentatives de sabotage déjà observées en 2024 à l'encontre de petites installations industrielles, telles des micro-installations d'énergies renouvelables, exposant des interfaces de contrôle faiblement sécurisées.

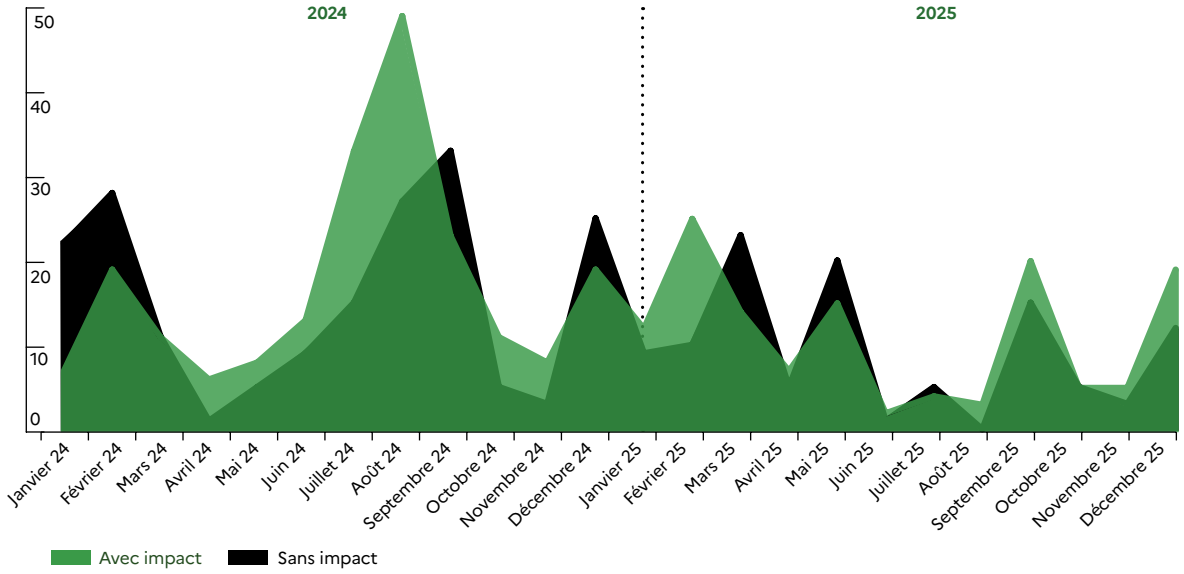
Attaques par déni de service (DDoS)

En 2025, l'ANSSI constate que les actions malveillantes les plus fréquentes employées à des fins de déstabilisation sont les DDoS. Malgré une baisse notable par rapport à l'année 2024 – qui avait été marquée en France par de grands événements et un contexte géopolitique dense – de multiples attaques DDoS ont été menées en 2025 à la faveur d'une actualité toujours riche en événements et du maintien d'un bruit de fond continu par des acteurs malveillants.

Si elles sont traditionnellement menées par des *hacktivistes* (agissant parfois de façon alignée sur les intérêts stratégiques d'États), il apparaît que ces attaques sont aussi de plus en plus le fait d'acteurs cybercriminels.

16
Sandworm, également appelé APT44, est un MOA réputé lié au service russe de renseignement militaire, le GRU. Il est associé à des attaques à des fins d'espionnage et de sabotage graves contre plusieurs entités de secteurs critiques dans le monde, notamment en Ukraine et les pays qui la soutiennent dans le cadre de la guerre d'agression déclenchée par la Russie en 2022.

Évolution des attaques par déni de service portées à la connaissance de l'ANSSI en 2024 et 2025 selon l'impact subi



D'un niveau de technicité peu sophistiqué, comparé aux efforts à mettre en œuvre pour concevoir un code malveillant ou encore se latéraliser sur un système compromis, les attaques par DDoS portées à la connaissance de l'ANSSI visent principalement à nuire à la réputation de leur victime, à travers la médiatisation d'incidents aux conséquences majoritairement limitées à la disponibilité de leurs services. En 2025, cependant, les entités visées ont dû faire face à des attaques d'une envergure croissante, réalisées sur des temps courts, rendant complexes la qualification de l'attaque et la limitation de ses effets. Ces attaques, qui par ailleurs peuvent impressionner par leur volumétrie, n'impliquent pas pour autant de compromission en profondeur. Pour mieux y faire face, l'ANSSI met à disposition sur le site du CERT-FR des fiches réflexes qui visent à apporter une aide à la qualification et à l'endiguement de ce type d'attaque [29] [30].

Sabotage de petites installations industrielles

Les systèmes de contrôle industriel exposés sur Internet et faiblement sécurisés offrent aussi aux *hacktivistes* des cibles à moindres frais.

L'ANSSI traite depuis 2024 de multiples signalements relatifs au ciblage d'entités du secteur de la production d'énergie renouvelable par des groupes *hacktivistes*. Ceux-ci visent des automates dont l'interface de gestion est exposée sur Internet sans authentification ou avec un mot de passe par défaut. L'accès à cette interface peut notamment permettre d'agir sur les vannes et les turbines des installations.

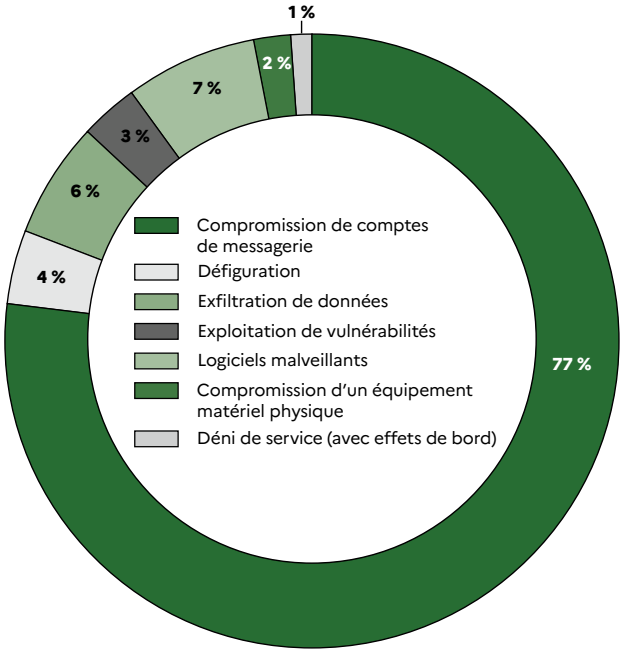
Au cours de l'année 2025, les groupes *hacktivistes* pro-russes ont continué de revendiquer des compromissions d'équipements liés au secteur de l'eau

en France et en Europe, à des fins de déstabilisation. Cependant, les attaques traitées par l'ANSSI en 2025 n'ont pas eu d'effet physique majeur. Dans un seul cas, les actions illégitimes sur les vannes ont entraîné une augmentation du débit de l'eau – dont l'impact a été limité par les faibles réserves en eau de l'installation. Bien que ces attaques soient souvent peu sophistiquées d'un point de vue technique, elles sont cependant fortement médiatisées par leurs auteurs, qui en exagèrent souvent les effets.

Ainsi, des groupes *hacktivistes* pro-russes tels que Z-Pentest Alliance revendiquent leurs attaques sur Telegram en visant à maximiser leur portée médiatique, par la publication de nombreuses vidéos de revendication montrant des actions sur des interfaces de gestion d'automates, et en exagérant régulièrement les conséquences réelles de celles-ci sur leurs victimes. L'ANSSI a récemment publié des recommandations de sécurisation minimales à destination des acteurs concernés [31].

Des compromissions d'équipements similaires ont également été recensées ailleurs en Europe. Ainsi, en août 2025, le service norvégien de renseignement intérieur (Politiets Sikkerhetstjeneste) a formellement attribué à des attaquants russes une attaque informatique ayant conduit à la prise de contrôle à distance d'un barrage dans l'ouest du pays en avril 2025 [32]. ←

Type d'incidents dans le secteur recherche et éducation



Ciblage des secteurs de la recherche et de l'éducation

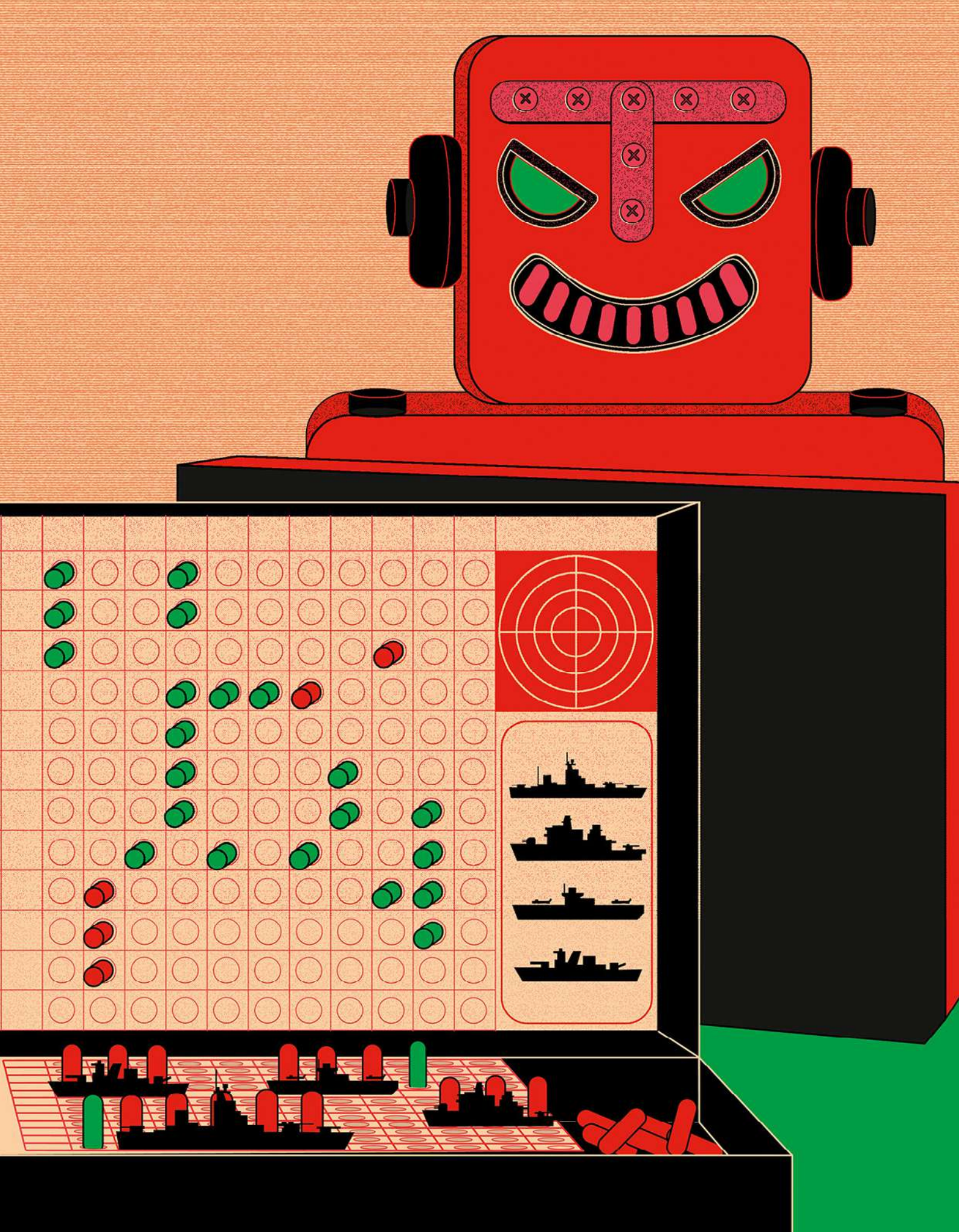
En 2025, l'éducation et la recherche constituent les secteurs les plus représentés parmi les incidents traités par l'ANSSI, regroupant à eux seuls 34 % des cas. Ces chiffres sont à mettre en perspective avec le nombre important d'entités publiques dans ces secteurs, plus enclines à contacter l'ANSSI en cas d'incident, même de faible criticité.

Une part importante de ces attaques est menée de manière opportuniste par des acteurs cybercriminels. Les établissements d'enseignement supérieur subissent régulièrement des compromissions de comptes de messagerie de leurs personnels ou étudiants, à des fins de diffusion de campagnes d'hameçonnage. Plusieurs entités du secteur de l'éducation ont également été victimes de la compromission de leurs sites Internet, via une compromission de compte administrateur et l'exploitation de vulnérabilités, menant à la modification de leurs contenus (défigurations). La menace d'attaque par rançongiciel pèse aussi sur ces secteurs. Ces incidents peuvent avoir des impacts importants et visibles sur la continuité de service. En février 2025 un établissement d'enseignement supérieur a ainsi été contraint d'assurer ses cours en format distanciel à la suite d'une compromission de ce type qui a rendu indisponible l'ensemble de son système d'information.

En outre, en 2025 l'ANSSI a traité plusieurs attaques contre des établissements d'enseignement secondaire, menées par des attaquants d'un niveau technique limité, mais tirant parti du faible niveau de sécurisation de ces entités.

Par ailleurs, des entités de ces secteurs hébergeant des activités plus sensibles ont été ciblées au cours de l'année. À titre d'exemple, l'ANSSI a eu connaissance de la compromission de ressources d'intérêt appartenant à un institut de recherche français. Si les motivations de ces attaques sont difficiles à établir avec certitude, ce ciblage indique l'intérêt des attaquants pour les entités du secteur de la recherche, potentiellement à des fins d'espionnage ou de pré-positionnement[17].

17
Le pré-positionnement renvoie à la stratégie d'attaquants informatiques, qui cherchent à s'introduire et se maintenir sur des systèmes critiques, potentiellement dans l'objectif de réaliser ultérieurement des actions malveillantes.



2

ÉVOLUTIONS ET SUIVI DES CAPACITÉS DES ATTAQUANTS

A
ÉVOLUTION DE L'OUTILLAGE DES ATTAQUANTS : EMPLOI DE SERVICES LÉGITIMES ET UTILISATION DES CAPACITÉS ISSUES DE L'INTELLIGENCE ARTIFICIELLE

→ Le recours croissant à des composants et services légitimes par les attaquants leur permet de dissimuler leurs actions parmi des flux qui ne sont pas caractérisés comme malveillants et de réduire le coût de maintien d'une infrastructure d'attaque. L'utilisation de capacités issues de l'intelligence artificielle leur permet également d'améliorer le niveau, la quantité, la diversité et l'efficacité de leurs attaques. L'ANSSI a observé un usage de ces pratiques par l'ensemble des typologies d'acteurs offensifs, liés à des États ou acteurs cybercriminels.

1/UTILISATION DE SERVICES LÉGITIMES À DES FINS DE COMPROMISSION ET DE MAINTIEN DES INFRASTRUCTURES D'ATTAQUE

L'ANSSI a observé au cours de l'année 2025 le détournement d'outils et de services informatiques légitimes à des fins malveillantes. Cette tendance n'est pas nouvelle concernant des activités associées à des acteurs malveillants réputés liés à la Chine ou à la Russie, mais en recrudescence concernant les acteurs cybercriminels.

Ces outils et services sont des outils d'accès à distance (RMM[18]), des outils de stockage en ligne y compris dans le *cloud*, ou encore des services Web d'aide au développement ou à l'intégration.

Ils sont employés dans le cadre d'attaques informatiques en raison de leur disponibilité, de leur facilité d'utilisation et de la difficulté de détection des usages malveillants qui peuvent en être faits. Les outils et services légitimes sont utilisés par les attaquants à toutes les étapes de la chaîne de compromission afin de collecter et exfiltrer des données, télécharger des codes malveillants, maintenir une persistance sur un système d'information compromis dans le cadre d'actions préparatoires à des attaques par rançongiciel, ou encore se latéraliser. Les attaquants peuvent tirer plusieurs bénéfices de l'utilisation de ce type d'outils et de services légitimes : d'une part, cette technique réduit le coût de maintien d'une infrastructure de commande et contrôle ; d'autre part, cette technique complique l'identification des compromissions, du fait de la difficulté pour les victimes et les équipes de cyberdéfense de distinguer les communications légitimes des communications malveillantes. Cela permet aux attaquants de dissimuler leur trafic vis-à-vis des dispositifs de supervision, tout en contournant les éventuelles contre-mesures mises en place. Dans ce contexte, une cartographie de l'utilisation

18
Remote monitoring and management: solutions de supervision et d'accès à distance des SI, ou *Remote management tools*.

de ces services peut se révéler déterminante, pour identifier ceux dont la présence n'est pas attendue ou dont l'usage n'est pas conforme à ce qui a été initialement prévu.

Au sein de l'écosystème cybercriminel, l'utilisation de plus en plus courante de ces outils en début de la chaîne de compromission coïncide avec la diminution de l'utilisation de *loaders* et *botnets* par les courtiers en accès initiaux (IAB)[19]. Plusieurs de ces IAB comme TA577, TA571 et TA544 ont par exemple abandonné ou largement diminué l'utilisation de codes malveillants au profit d'outils de RMM ou de techniques de LOLBins[20] [33]. Par exemple, le MOA Scattered Spider utilise rarement des codes malveillants et son accès au SI est quasi systématiquement obtenu grâce à la compromission d'accès légitimes [34]. L'ANSSI a observé l'utilisation, par des attaquants cybercriminels, d'outils et services commerciaux disponibles en sources ouvertes lors d'attaques à l'encontre d'entités françaises. Ces outils et services sont employés de plusieurs manières : par la mise en œuvre des techniques d'ingénieries sociales pour récupérer des identifiants, par hameçonnage téléphonique pour convaincre directement la victime de procéder au téléchargement d'un outil, ou après avoir obtenu un accès initial à l'ordinateur ciblé, par exemple suite à l'installation d'une porte dérobée via un courriel d'hameçonnage.

Les opérateurs de MOA réputés russes détournent régulièrement des services Web légitimes lors de leurs attaques informatiques. Ce type d'attaque, déjà observé en 2023 et 2024[21], se poursuit en 2025 [35] [36] [37]. L'éditeur de sécurité informatique Sekoia a par exemple documenté, en septembre 2025, l'utilisation par les opérateurs du MOA russe APT28 des outils de stockage de fichiers en ligne Koofr, Icedrive ou encore Filen.io à différentes étapes de la chaîne de compromission [38]. Ces services seraient notamment utilisés pour stocker des charges malveillantes, récupérées par des codes utilisés par les opérateurs d'APT28 tels que Covenant ou BeardShell [39] [38].

Enfin, les opérateurs du MOA réputé iranien MuddyWater ont eux aussi utilisé des outils de RMM à des fins offensives, comme AteraAgent [40], SimpleHelp ou ScreenConnect [41].

19
En anglais *initial access brokers* ou *IAB*.

20
Les LOLBins, pour *Living Off the Land Binaries*, sont des binaires légitimes d'un système d'exploitation détournés pour réaliser des activités malveillantes, de manière furtive.

21
Des attaques commises au moyen du MOA APT28, attribué au GRU, ont ainsi exploité en 2023 et 2024 des outils tels que webhook[.]site, run.mocky[.]io, ou Pipedream.

Outils et services légitimes observés par l'ANSSI lors d'incidents

Les outils commerciaux disponibles en sources ouvertes et exploités par des attaquants les plus observés par l'ANSSI au cours des six derniers mois sont entre autres :

LISTE NON EXHAUSTIVE	OUTILS ET SERVICES LÉGITIMES UTILISÉS PAR DES MOA RÉPUTÉS ÉTATIQUES	OUTILS ET SERVICES LÉGITIMES UTILISÉS PAR DES ACTEURS CYBERCRIMINELS
OUTILS D'ACCÈS À DISTANCE	• AteraAgent • SimpleHelp • ScreenConnect	• AnyDesk • TeamViewer • VNC (UltraVNC, TightVNC…) • Atera • LogMeIn
SERVICES LÉGITIMES DE STOCKAGE/PARTAGE	• Google Calendar • Google Drive • Google SpreadSheet • Google Docs • Open Drive • DropBox • Koofr • Icedrive • Filen[.]io	• MEGA
SERVICES WEB D'AIDE AU DÉVELOPPEMENT ET À L'INTÉGRATION	• WebHook.site • Mocky.io • Pipedream • Cloudflare Workers • AWS Lambda URL	

La majorité des incidents recensés concerne le logiciel Anydesk. Le téléchargement et le déploiement de cette solution ont notamment été effectués par les attaquants en lien avec le groupe Inc Ransom lors d'une attaque par rançongiciel ayant affecté un centre hospitalier en octobre 2025.

Des solutions de RMM open-source sont enfin utilisées par certains groupes cybercriminels à l'instar de l'utilisation de l'outil MeshAgent observée cette année dans le cadre de cyberattaques impliquant la souche rançongiciel Nova.

2/INTELLIGENCE ARTIFICIELLE: UNE ÉVOLUTION TECHNOLOGIQUE PORTEUSE D'OPPORTUNITÉS SAISIES PAR LES ATTAQUANTS

L'IA générative et l'évolution rapide de ses usages représentent un potentiel accélérateur des capacités offensives associées aux cybermenaces, qui appelle à une réévaluation régulière de la menace. Toutefois, leur utilisation par des attaquants dépend de leurs objectifs et surtout de leur niveau de maturité.

Les services d'IA générative peuvent également être la cible d'attaquants, qui cherchent à en altérer les données d'entraînement. La multiplication de contenus fallacieux générés par IA sur Internet pourrait polluer les données d'entraînement des modèles d'agent conversationnel comme ChatGPT, et participer à la diffusion de fausses informations à grande échelle.

L'évolution des usages de services d'IA générative notamment dans un contexte professionnel et leur intégration dans des flux opérationnels sont susceptibles d'augmenter la surface d'attaque en l'absence de cloisonnement, sur le plan physique ou des usages. La compromission d'un système d'IA pourrait ainsi porter atteinte à la confidentialité des données traitées et à l'intégrité des SI auxquels il est connecté. Dans un contexte de développement logiciel, la compromission d'un système d'IA spécialisé dans la génération de code informatique pourrait constituer une nouvelle forme d'attaques par chaîne d'approvisionnement. Une synthèse de la menace relative à l'IA générative et un guide ANSSI contenant des recommandations de sécurité pour la mise en œuvre de solutions d'IA générative reposant sur des Large Language Models (LLMs) au sein d'entités publiques et privées sont disponibles respectivement sur les sites du CERT-FR (source : https://www.cert.ssi.gouv.fr) et de l'ANSSI [42]. ←

→ Dans le cadre de ses investigations sur la lutte informatique offensive privée (LIOP), l'ANSSI a pu identifier à plusieurs reprises des sites Internet semblant avoir été générés par des systèmes d'IA générative. Ces sites à l'apparence légitime servent à héberger des charges malveillantes ou à effectuer de la caractérisation[22]. L'utilisation de l'IA a notamment été rendue visible par l'insertion anormale de texte au milieu de certains paragraphes, sans lien avec le reste du contenu. ←

22
La caractérisation ou *profiling* consiste à récupérer des données techniques des visiteurs ayant consulté la page et ainsi identifier des cibles avant de les compromettre.

B
POURSUITE DE L'EXPLOITATION DE TECHNIQUES D'INGÉNIERIE SOCIALE DIVERSIFIÉES

Sans avoir besoin d'une haute technicité, les attaquants continuent d'exploiter les biais inhérents à la nature humaine, entre autres en s'appuyant sur le bon vouloir des personnes ciblées.

1/EMPLOI CROISSANT DE TECHNIQUES D'INGÉNIERIE SOCIALE SOPHISTIQUÉES

En 2025, l'ANSSI a observé l'emploi de techniques d'ingénierie sociale avancées telles que le SIM-Swapping[23], le MFA Fatigue[24], l'usurpation d'identité ou l'hameçonnage vocal[25] par des acteurs cybercriminels. Ces techniques consistent à leurrer un utilisateur pour l'amener à accomplir des actions qu'il considère comme légitimes alors qu'elles compromettent en réalité son système d'information. L'ANSSI a ainsi observé plusieurs cas d'arnaques au faux support informatique, incitant des employés à télécharger des solutions de RMM comme vecteur initial de compromission. Lors de l'installation de ces outils, les acteurs malveillants peuvent contourner les règles de pare-feu ou modifier les clés de registres avec un ajout de la fonctionnalité de lancement du programme légitime lors d'un démarrage en mode sans échec ; et ce dans l'objectif d'éviter la détection des anti-virus et des outils de type Endpoint Detection and Response (EDR).

Le MOA Scattered Spider s'est notamment démarqué par sa maîtrise de ces techniques visant au déploiement de rançongiciels et/ou à l'exfiltration de données. L'efficacité de ces techniques s'explique principalement par la connaissance de l'attaquant des processus internes aux entreprises, mais également par l'importante phase de reconnaissance et de collecte de données à caractère personnel liées aux employés ciblés en amont de l'attaque. Elles témoignent aussi des capacités de contournement et de l'adaptabilité des attaquants aux mesures de cybersécurité, notamment celles relatives à l'authentification multifactorielle [43] [44]. Plusieurs entreprises françaises, dont des entités du secteur du luxe, ont été compromises en 2025 au moyen du MOA Scattered Spider. Dans au moins un des cas, les attaquants auraient usurpé le service informatique pour obtenir les accès d'une application de gestion des relations clients.

En outre, en juin 2025, l'éditeur de sécurité Google Threat Intelligence Group (GTIG) et le groupe de recherche académique Citizen Lab ont publié simultanément sur le ciblage informatique de spécialistes de la Russie entre avril et juin 2025, dont le chercheur britannique Keir Giles, dans le cadre de campagnes d'hameçonnage au long cours associées au MOA UNC6293. Selon GTIG, ce dernier serait potentiellement lié au MOA réputé

23
Technique d'ingénierie sociale visant à transférer le numéro de téléphone d'une victime vers une carte SIM contrôlée par l'attaquant. Cela permet de contourner les authentifications basées sur des SMS ou des appels vocaux.

24
Attaquant bombardant la victime avec des demandes d'authentification multifactorielle (MFA) jusqu'à ce que celle-ci, accepte la demande par inadvertance.

25
Technique malveillante où l'attaquant utilise un appel téléphonique pour encourager la victime à révéler des informations sensibles ou effectuer des actions compromettantes, souvent en imitant une autorité de confiance (service informatique, banque, etc.).

russe Nobelium[26]. Durant plusieurs semaines, les opérateurs du MOA UNC6293 auraient utilisé des méthodes d'ingénierie sociale personnalisées pour inciter Keir Giles à créer et partager un mot de passe d'application lié à son compte Google. Ce mot de passe d'application aurait ensuite permis aux attaquants d'accéder à ses comptes. [45] [46].

En février 2025, des chercheurs français, dont certains spécialistes de la Russie, ont reçu des messages d'hameçonnage via les applications de messagerie Signal et WhatsApp usurpant des personnalités politiques américaines et ukrainiennes. Ce ciblage pourrait s'inscrire dans le cadre de campagnes d'hameçonnage plus larges exploitant des environnements mobiles pour collecter des codes d'association liés à des comptes ou services Microsoft. Les TTP mises en œuvre dans le cadre de ces attaques correspondent à celles de MOA potentiellement liés à la Russie décrites par plusieurs éditeurs de sécurité [47] [48].

2/UTILISATION NOTABLE DE LA TECHNIQUE « CLICKFIX »

Depuis l'automne 2024, les acteurs cybercriminels ont multiplié les campagnes s'appuyant sur la technique « Clickfix », qui consiste à inciter une victime à exécuter elle-même des commandes pour télécharger et exécuter un programme malveillant. Selon plusieurs éditeurs, l'utilisation de cette technique serait en augmentation en 2025. De nombreux RAT et infostealers ont été déployés par ce moyen, tels que Lumma Stealer, Rhadamanthys, XWorm ou AmadeyLoader [49] [50]. Au moins une campagne d'attaques mettant en œuvre cette technique a par ailleurs été portée à la connaissance de l'ANSSI.

En 2025, des opérateurs de MOA réputés étatiques ont également eu recours à cette technique. À titre d'exemple, dans un rapport du 25 octobre 2024, le CERT-UA aurait identifié une campagne d'hameçonnage des opérateurs du MOA russe APT28 contre des entités gouvernementales ukrainiennes. Cette campagne s'appuyait notamment sur l'utilisation d'un faux captcha visant à faire copier à la victime une commande malveillante dans son presse-papier puis à l'inciter au moyen d'instructions à ouvrir un terminal et à y coller le contenu copié. L'exécution de cette commande dans un terminal permettrait ensuite aux attaquants de compromettre l'appareil de la victime [51].

Plus récemment, en septembre 2025, les opérateurs du MOA Callisto[27] auraient également utilisé cette technique dans le cadre de campagnes ciblant des membres de la société civile en Russie ou encore des organisations non gouvernementales impliquées en Ukraine [52] [53]. ←

26
Le MOA Nobelium est réputé lié au service de renseignement extérieur russe (SVR). Selon l'éditeur de sécurité Microsoft, les activités associées au MOA remonteraient à 2018. Il aurait notamment été mis en œuvre contre des entités gouvernementales, diplomatiques et du secteur des technologies en Amérique du Nord et en Europe [97].

27
Le MOA Callisto, actif depuis au moins 2015, est attribué par différentes sources au service de renseignement intérieur russe (FSB).

C
SUIVI DES CAPACITÉS DES ATTAQUANTS

1/DES OUTILS ET PRATIQUES QUI COMPLEXIFIENT LE PROCESSUS D'IMPUTATION

Lors de ses investigations, l'ANSSI a rencontré différentes difficultés liées à l'utilisation par les opérateurs des MOA de chaînes d'anonymisation d'outils non signants ou partagés et de techniques du faux drapeau, complexifiant le suivi des menaces et le processus d'imputation[28].

Par exemple, depuis plusieurs années, l'ANSSI note l'utilisation croissante d'outils de sécurité offensifs, développés et mis en ligne publiquement par des entreprises et individus reconnus au sein de l'écosystème de prestataires privés de sécurité offensive chinois, et pouvant être réutilisés par les opérateurs de nombreux MOA. Ces outils, de différents types pour chaque étape de la *killchain*, sont employés de façon quasi exclusive lors de campagnes d'attaques menées par des MOA réputés liés aux intérêts stratégiques chinois, notamment par des prestataires de sécurité offensive (comme la société I-SOON). Seule une minorité de ces outils est utilisée plus largement par d'autres attaquants non réputés liés à la Chine. Ainsi, les outils FRP et aspxspy ont été respectivement utilisés par les opérateurs des MOA réputés iraniens, Charming Kitten et APT39 [54] [55].

En parallèle, l'ANSSI constate une forte utilisation d'outils de reconnaissance et de *tunneling*[29], ces derniers étant employés en tant qu'outils d'intrusion, mais également pour administrer des réseaux d'anonymisation utilisés par les opérateurs de plusieurs MOA réputés chinois. Entre 2024 et 2025, l'emploi des outils vShell (dont le répertoire Github a été supprimé en 2024), Asset Reconnaissance Lighthouse, fscan, Neo-Regeorg, Rakshasa ou Stowaway, a été rapporté à plusieurs reprises en sources ouvertes, tandis que l'ANSSI a également observé l'utilisation des outils Ladon, NPS ou encore iox [56] [57] [58].

Ainsi, l'accessibilité publique de ces outils complexifie l'imputation des attaques informatiques à un MOA spécifique, et est à mettre en parallèle avec le développement du partage de codes non accessibles publiquement entre acteurs offensifs chinois (PlugX, ShadowPad ou KeyPlug) et la mise en place d'infrastructures d'attaque communes à plusieurs opérateurs de MOA (dont les réseaux d'anonymisation réputés chinois).

L'utilisation de ressources malveillantes associées à plusieurs MOA tout au long de la chaîne d'infection peut aussi complexifier l'imputation des cyberattaques. L'ANSSI a par exemple observé l'emploi d'un MOA réputé chinois, Houken, à l'encontre d'entités gouvernementales françaises, du secteur des télécommunications, des médias, de la finance et des transports à la fin de l'année 2024. Les attaquants ont exploité plusieurs vulnérabilités jour-zéro, affectant des équipements Ivanti (CVE-2024-8190, CVE-2024-8963 et CVE-2024-9380) pour réaliser leur compromission initiale puis se sont latéralisés plus en profondeur sur les systèmes d'information avec notamment des outils génériques et en laissant de nombreuses traces. La différence de sophistication entre l'exploitation des vulnérabilités initiales et le

28
Le processus d'imputation consiste à associer une activité malveillante à un mode opératoire ou à un groupe d'attaquants, en s'appuyant sur des éléments techniques et contextuels, dans un objectif d'enrichissement de la connaissance et de suivi de la menace. L'acte d'attribution lui, associe une attaque ou un mode opératoire à un commanditaire, sur la base d'éléments précis, dans un objectif politique ou géopolitique.

29
Le *tunneling* est une méthode pour transporter des données sur un réseau en utilisant des protocoles qui ne sont pas pris en charge par ce réseau. Les tunnels fonctionnent en encapsulant les paquets réseaux : ils enveloppent les paquets dans d'autres paquets.

reste de la compromission pourrait ainsi laisser supposer que le MOA Houken est employé par un initial *access broker* (IAB) puis que d'autres MOA réputés chinois sont employés pour la suite de l'attaque. Cette répartition des tâches entre plusieurs MOA peut complexifier les travaux d'imputation et le suivi des acteurs malveillants [59].

Dans le même esprit, les 5 et 6 juin 2025, l'éditeur de sécurité ESET a observé le déploiement du code malveillant Kazuar v2 associé au MOA Turla via un code malveillant associé au MOA Gamaredon sur deux machines appartenant à des organisations non identifiées en Ukraine. Ces observations pourraient entre autres suggérer une collaboration entre les opérateurs des MOA Turla et Gamaredon[30], tous deux réputés liés au service de renseignement intérieur russe (FSB) mais à des centres différents, et contribuent ainsi à brouiller les frontières entre les MOA réputés liés au FSB [60].

Pour ajouter à la complexité d'imputation, l'ANSSI a également observé la revendication d'attaques par des cybercriminels usurpant l'identité d'autres groupes cybercriminels connus, soulignant la problématique des attaques sous faux drapeaux et l'enjeu de la médiatisation des attaques pour les groupes cybercriminels. Par exemple, en mars 2025, des attaquants auraient usurpé l'identité du groupe Cl0p en envoyant de faux mails indiquant avoir exfiltré des données de l'entreprise destinataire en utilisant une vulnérabilité dans Cleo [61]. La campagne d'attaque contre Salesforce[31], revendiquée en août 2025 par un groupe se présentant comme une alliance de Scattered Spider, Lapsus$ et ShinyHunters, a également illustré des problématiques d'imputation. En effet, bien que les opérateurs de ces trois MOA aient évolué au sein de la même communauté (TheCom), il n'a pas été possible de confirmer leur implication réelle dans cette campagne, en raison d'un manque de TTPs suffisamment discriminantes [62].

Enfin, des liens entre des acteurs cybercriminels et l'État russe sont régulièrement effectués en sources ouvertes par des personnalités publiques. Pourtant, ces relations sont loin d'être systématiques et relèveraient davantage d'opportunités temporaires, de chantage ou de connaissances interpersonnelles. Les fuites de données de BlackBasta publiées en février 2025 en révèlent ainsi la complexité, en exposant les liens personnels entre acteurs cybercriminels et personnels des services russes. Ainsi, si dans un contexte géopolitique complexe les autorités russes protègent de manière tacite les cybercriminels des extraditions, il est hautement probable que la plupart de ces groupes soient autonomes et n'agissent pas en général suivant les ordres de l'État russe.

2/UN BROUILLARD TECHNOLOGIQUE OU ORGANISATIONNEL COMPLEXIFIANT LA DISCRIMINATION ENTRE ACTEURS OFFENSIFS CYBERCRIMINELS

Le suivi des capacités attaquantes peut également être complexifié par la volatilité de certaines menaces ou leur organisation et développement. C'est par exemple le cas pour les codes cybercriminels vendus sur étagère et les groupes qui les opèrent.

30
Le MOA Gamaredon est attribué publiquement par le *Security Service of Ukraine* (SSU) au service de renseignement intérieur russe (FSB). Actif depuis au moins 2014, le MOA est essentiellement associé au ciblage de secteurs stratégiques en Ukraine tels que les secteurs gouvernementaux, de l'énergie, et de la défense, notamment à des fins d'espionnage [98].

31
Éditeur américain de logiciels de Gestion de la Relation Clients (CRM).

Les groupes de *ransomware-as-a-service* sont volatiles et composés d'affiliés hétérogènes. Ces rançongiciels sont en effet déployés par de nombreux cybercriminels et disposent d'une durée de vie relativement courte. En 2023, la durée de vie moyenne d'un groupe de rançongiciels était estimée à 262 jours [63]. Au-delà du suivi de ces franchises, l'identification d'affiliés pérennes dans le temps au travers de marqueurs techniques est également nécessaire. La plupart du temps, ces groupes d'affiliés déploient différents rançongiciels à travers les années ou concomitamment. Le groupe EvilCorp aurait notamment été un affilié majeur du groupe LockBit en 2022, responsable de 60 versions du rançongiciel et de l'extorsion de plus de 100 millions d'euros. Il est notamment suivi grâce à son utilisation du code malveillant SocGolish (FakeUpdates). Entre juillet 2024 et début 2025, il aurait déployé le rançongiciel RansomHub [64].

Les *malware-as-a-service* (MaaS) mettent également en lumière plusieurs problématiques de suivi liées à la complexité des codes cybercriminels et à la massiveté de leur déploiement par de nombreux affiliés. Lumma Stealer, vendu comme MaaS sur des forums russophones depuis au moins août 2022, dispose à la fois de capacités de vol d'information (portefeuilles de crypto, authentification), d'exécution de code sur la machine infectée et de déploiement de charges supplémentaires. L'ANSSI a rencontré plusieurs difficultés lors de son analyse :

- **Massivité** : traitement de plusieurs dizaines de milliers d'échantillons et nombre important de chaînes d'infections ;
- **Complexité et actualisation du code** : le code est régulièrement mis à jour, et évolue à chaque nouveau variant. Il présente des techniques d'obfuscation de code sophistiquées et adaptées au maliciel, et utilisées ailleurs dans l'écosystème cybercriminel, telles que le *control flow flattening*[32] ;
- **Résilience** : la résurgence de l'activité du code après le démantèlement de son infrastructure le 21 mai 2025 démontre également la résilience des acteurs responsables du développement de Lumma Stealer ;
- **Instabilité** : les domaines de commande et contrôle sont modifiés plusieurs fois par semaine, et un même échantillon peut contenir jusqu'à une dizaine de noms de domaine, actifs ou non au moment du déploiement du maliciel. En outre, une partie non négligeable de ces noms de domaine est gérée par des infrastructures – légitimes, mais louées par les cybercriminels – de type *Content Delivering Network*. L'utilisation de ces infrastructures comme Cloudflare permet une anonymisation partielle des domaines de commande et contrôle en masquant l'adresse IP réelle du serveur par le CDN, rendant les efforts d'analyse et de détection plus ardus. Ces difficultés se retrouvent dans le suivi de nombreuses menaces et notamment des menaces liées à la LIOP.

Lumma Stealer est ainsi représentatif des problématiques liées à l'étude et au suivi de codes cybercriminels.

32
Ou aplatissement du *flow* de contrôle, technique visant à transformer la structure d'un code pour en dissimuler la logique d'exécution.

3/DES DIVULGATIONS DE DONNÉES PERMETTENT DE MIEUX COMPRENDRE LES ACTEURS OFFENSIFS

Dans la continuité de l'année 2024, plusieurs fuites de données affectant des opérateurs de MOA réputés étatiques, des entreprises de LIO ou des groupes cybercriminels ont été publiées en sources ouvertes et ont permis de mieux appréhender le fonctionnement interne de ces divers groupes. D'une part, elles renseignent à court terme sur l'organisation de ces entités, une partie des outils et codes qui ont pu être utilisés lors des attaques (via par exemple de la documentation interne) ou encore leurs cibles potentielles ou avérées. D'autre part, ces fuites de données peuvent amener à la dissolution, la suspension ou encore la réorganisation des activités des attaquants identifiées, entraînant sur le plus long terme une perte de visibilité pour les entités suivant leurs travaux.

De nouveau en 2025, des groupes de rançongiciels majeurs ont fait l'objet de fuite de données et de dissensions internes menant à leur disparition. Fin mars 2025, les activités du groupe RansomHub, responsable de près de 239 attaques en 2024 [65], ont pris fin suite à des dissensions avec d'autres groupes cybercriminels [66]. À la même période, le groupe BlackBasta, actif depuis 2022 [67] puis le groupe LockBit [68], ont fait l'objet de fuites de données majeures. Ces sources d'information sont à chaque fois déterminantes pour comprendre les rouages de ces groupes, leurs organisations internes, confirmer des liens entre les acteurs, les codes et les campagnes d'attaque. Si rien ne permet de vérifier avec certitude leur authenticité, les informations sont crédibles et peuvent recouper des investigations préalablement effectuées.

→ Depuis plusieurs années, il convient de noter la multiplication de ces fuites de données de groupes cybercriminels majeurs. Ces divulgations semblent être pour les membres d'un groupe puissant une des actions les plus efficaces pour dénoncer des comportements (*exitscam*, non-paiement de rançons) ou réparer un affront. Elles font aujourd'hui partie intégrante de la dynamique de l'écosystème et de ses principales restructurations.←

D'autre part, des fuites de données exposant des prestataires privés de LIO chinoise ont été constatées ces dernières années [69] et 2025 ne fait pas figure d'exception en la matière. À titre d'exemple, en mai 2025, deux bases de données relatives à des opérateurs du MOA Salt Typhoon et de l'entreprise VenuTech ont été mises en vente sur le forum cybercriminel anglophone DARKFORUMS et ont fait l'objet d'un article par l'entreprise de cybersécurité américaine SpyCloud le 1er juillet 2025 [70]. Une large partie des informations contenues dans ces documents est corroborée par des sources ouvertes, ce qui suggère l'authenticité de l'ensemble. Ces collections de documents internes présentent un intérêt indéniable sur le plan de la connaissance de la menace chinoise. Elles précisent les intentions et capacités des attaquants au regard du ciblage d'organismes étrangers et le type d'informations recherchées par les opérateurs (tel que du contenu de serveurs courriels). Elles participent également à la compréhension de l'organisation des attaquants, en spécifiant des noms de clients gouvernementaux, des services offensifs proposés par ces prestataires, les relations commerciales entre prestataires ainsi que l'ordre de prix indiqué pour ces services, ce qui permet d'estimer leur valeur sur le marché chinois. De fait, il peut être constaté un décalage certain entre les « faibles » moyens alloués à ce type de prestations offensives en Chine et les ressources conséquentes déployées à des fins défensives par les entités et pays ciblés. Plus récemment encore, en novembre 2025, l'entreprise chinoise Knownsec[33] a subi une fuite de données. Celle-ci contiendrait de la documentation interne sur des codes malveillants ainsi que des listes de potentielles victimes dans plus d'une vingtaine de pays, dont le Japon, le Vietnam, l'Inde ou encore la Corée du Sud [71].

Les attributions réalisées dans le cadre de ces expositions publiques de données doivent cependant être lues avec prudence. Par exemple, une divulgation de données supposément liée à des opérateurs nord-coréens et présentée à la conférence DEF CON 33 de Las Vegas a fait ensuite l'objet de plusieurs publications d'éditeurs de sécurité, questionnant l'hypothèse initiale d'attribution et réorientant les analyses vers de potentiels opérateurs chinois. ←

33
Connue pour ses activités en lien avec les services de renseignement chinois.

3

CIBLAGE ET OPPORTUNITÉS D'ACCÈS

A
OPPORTUNITÉS CRÉÉES PAR UN CONTEXTE SPÉCIFIQUE

→ Les attaquants cherchent ou profitent d'opportunités pour mener leurs attaques. Certaines de ces opportunités sont offertes par le contexte global dans lequel évoluent leurs cibles (organisation d'événement, échéance électorale, conflit, etc.), d'autres relèvent davantage de l'environnement administratif (cadre légal favorable à la collecte de données ou de vulnérabilités). Le niveau de sécurisation des entités ciblées représente également un contexte qui peut être favorable dans les cas où les faiblesses techniques ou les mauvaises pratiques de sécurité sont structurelles.

1/STRATÉGIES DE SÉCURITÉ INADÉQUATES OCCASIONNANT DES OPPORTUNITÉS POUR LES ATTAQUANTS

Dans le cadre de ses missions, l'Agence effectue des audits de sécurité au profit d'administrations publiques, mais également d'opérateurs d'importance vitale (OIV), d'opérateurs de services essentiels (OSE) et de victimes d'incidents. Ces audits montrent régulièrement que des stratégies de sécurité inadéquates laissent des opportunités pour les attaquants, de par l'étendue des techniques, tactiques et procédures utilisées par ceux-ci. Plusieurs constats peuvent être établis, en particulier sur les réseaux bureautiques d'organismes dont le parc informatique est composé de dizaines ou centaines de milliers de postes.

Tout d'abord, peu d'audits globaux, permettant d'obtenir une vision globale du niveau de sécurité du SI bureautique, sont effectués. Des périmètres d'audit trop restreints risquent d'en faire perdre la pertinence. À titre d'exemple, les situations suivantes ont été rencontrées :

- L'audit d'une application sans inclure le fournisseur d'authentification (tel que l'Active Directory) utilisée par l'application ;
- L'audit d'une application sans le serveur sous-jacent qui expose une interface IPMI[34] non à jour et est exposée à l'ensemble du réseau bureautique.

De plus, les audits réalisés peuvent être des audits dits « *redteam* » où une grande partie de l'audit est consacrée à l'obtention d'un accès initial au sein du SI depuis Internet. Ce type de prestation, assez courant, est censé simuler l'attaque d'un MOA sur le système d'information. Si, de manière générale, un audit sur un SI n'est que rarement complet, une prestation dite de *redteam* est souvent encore plus parcellaire. En effet, le but étant prioritairement d'obtenir un accès au sein du SI pour se procurer l'information recherchée ou démontrer sa perméabilité, il n'y a pas de recherches exhaustives de l'ensemble des chemins de compromission possibles et des potentielles vulnérabilités existantes.

Ainsi, l'ANSSI recommande de réaliser des audits larges, qui ont pour objectif l'obtention d'une vision

34
L'interface de gestion intelligente de matériel (ou IPMI, *Intelligent Platform Management Interface*) est un ensemble de spécifications d'interfaces pour un composant autonome des serveurs informatiques.

globale du niveau de sécurité de l'environnement et cherchent à identifier un maximum de moyens de compromission. Ceux-ci pourront être accompagnés le cas échéant d'activité de *redteam* ou d'évaluation de la détection d'intrusion mais constituent une brique essentielle d'une stratégie de sécurité réaliste et efficace.

Les accès initiaux fournis aux auditeurs peuvent être les suivants :

- Un accès au réseau bureautique d'entreprise sans privilège particulier pour simuler la compromission d'un accès physique au réseau ;
- Un accès au réseau bureautique (éventuellement au travers d'un VPN) accompagné d'un compte bureautique pour simuler la compromission d'un poste de travail ;
- Un accès à des ressources comme un conteneur, une machine virtuelle voire un serveur physique pour simuler la compromission d'une application.

Par ailleurs, l'équipe chargée de la détection d'intrusion (Centre opérationnel de sécurité ou SOC - *Security Operations Center*) ne devrait pas bloquer au fil de l'eau les accès obtenus par l'équipe d'audit et détectés par le SOC, l'audit n'ayant pas pour objectif d'évaluer la réactivité du SOC. Cependant, en fin d'audit, la présentation des chemins de compromission identifiés par les auditeurs au SOC est importante, car elle permet deux choses :

- Valoriser les scénarios de détection mis en place qui ont pu détecter les actions des auditeurs ;
- Mettre en place de nouveaux scénarios de détection pour les actions des auditeurs n'ayant pas fait l'objet de détection par le SOC.

Enfin, les équipes de l'ANSSI rencontrent parfois des organismes dont la stratégie de sécurité repose entièrement sur des produits. Il est important de rappeler que cela ne saurait suffire. En effet, bien que les EDR, les mécanismes d'authentification multi-facteurs (MFA) et les bastions puissent augmenter le niveau de sécurité du SI, ils possèdent également des limites :

- EDR : les attaquants rencontrent fréquemment ces outils et adaptent les leurs afin de ne pas être détectés ;
- MFA et bastion : en cas de compromission du poste de l'utilisateur, ces mécanismes ne permettent pas d'arrêter un attaquant. Celui-ci peut, en effet, s'injecter dans la session de l'utilisateur et utiliser le même canal que l'utilisateur légitime.

2/LAWFARE CYBER : QUAND LES OPPORTUNITÉS SONT FAÇONNÉES PAR UN CONTEXTE LÉGAL FAVORABLE

Plusieurs États à travers le monde ont pu utiliser leur cadre juridique afin de faciliter ou réaliser des compromissions à l'encontre d'intérêts français, sans s'y limiter pour autant. Dans certains cas, les cadres réglementaires de ces pays peuvent imposer aux entreprises ou entités implantées sur leur territoire l'utilisation de logiciels spécifiques. En particulier, depuis plusieurs années, l'ANSSI observe des cas de logiciels imposés en Chine [72].

En 2025, des entreprises d'un même secteur d'activité se sont vu imposer – suite à l'entrée en vigueur d'une nouvelle législation par les autorités chinoises – l'installation d'un logiciel dont les fonctions sont prétendument limitées à l'enregistrement administratif d'entreprises exportant sur leur territoire. L'analyse du code source par l'ANSSI a mis en exergue la présence de fonctionnalités jugées malveillantes au sein du programme. En effet, l'outil confère des accès étendus au

SI des entreprises ciblées, via des capacités d'énumération et de surveillance des périphériques USB, couplées à une capacité de mise à jour autonome.

Autre exemple, un groupe pharmaceutique français a signalé cette année la présence d'un programme malveillant sur le système d'information d'une de ses filiales localisées en Chine. Les autorités locales ont exercé une pression accompagnée de menaces sur un employé afin de contourner les politiques de sécurité informatique de l'entreprise et parvenir à leurs fins.

Si ces logiciels peuvent comporter des fonctionnalités malveillantes incluses par leurs éditeurs, ils pourraient aussi être victimes d'une attaque via la chaîne d'approvisionnement visant à compromettre ses clients. Les attaquants pourraient ainsi cibler spécifiquement ces logiciels dont l'utilisation est circonscrite géographiquement pour atteindre des entreprises dans un pays donné.

Afin de limiter l'impact de ces menaces, l'ANSSI recommande notamment, à chaque fois que cela est possible, d'installer le logiciel sur un poste isolé et dédié au système d'information de l'entité. Autrement, il est important de considérer la mise en place de mesures permettant de mitiger les risques de fuites de données et de compromission en isolant autant que possible ces logiciels qui doivent être considérés comme non maîtrisés. En complément, il peut être utile de surveiller les échanges d'information entretenus par ce composant logiciel.

3/OPPORTUNITÉS CRÉÉES PAR LES CONTEXTES ÉVÉNEMENTIELS

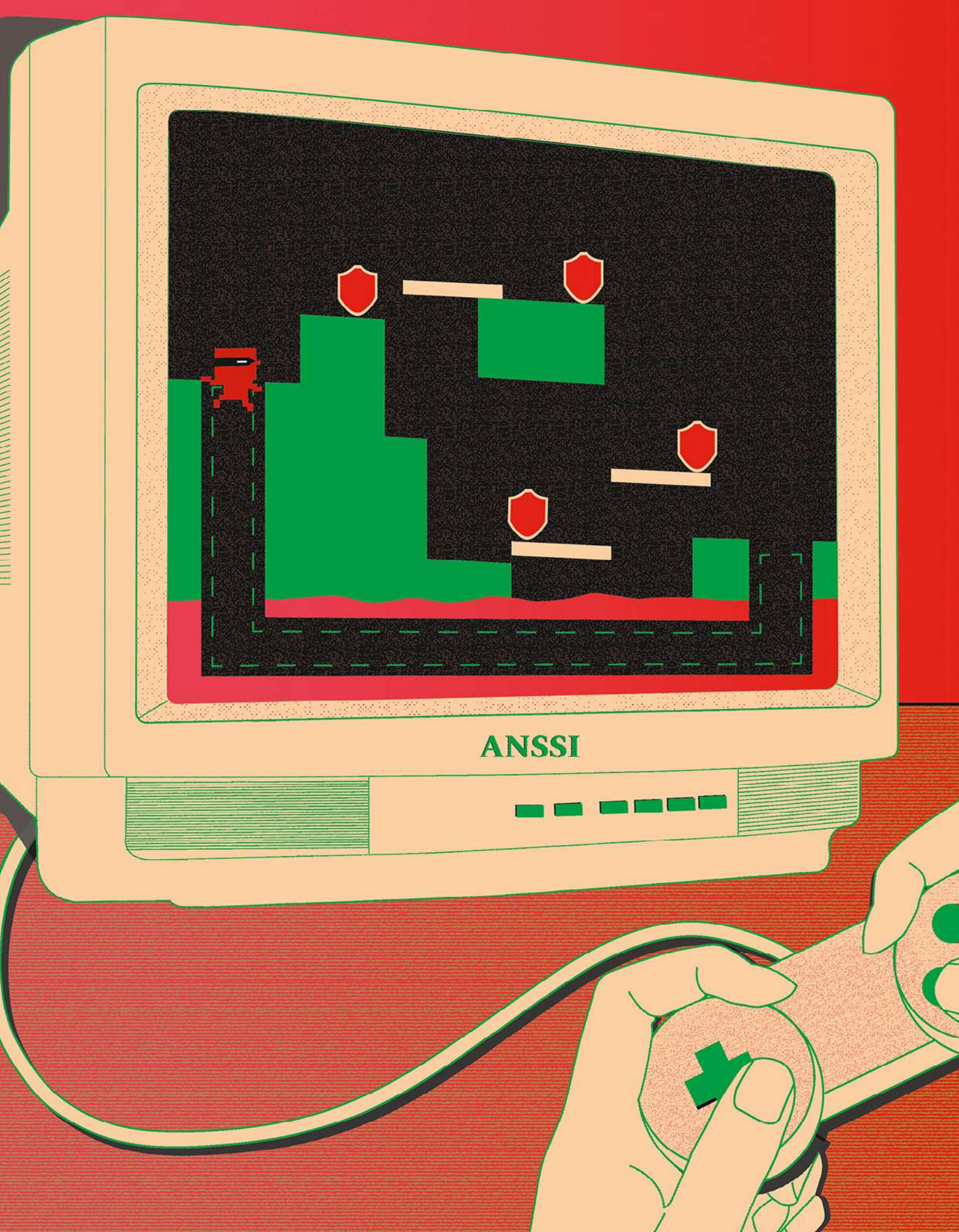
Des événements politiques et géopolitiques tels que des élections, des visites d'officiels ou des négociations diplomatiques sont des opportunités d'attaques à des fins d'espionnage, de déstabilisation ou encore d'influence. L'ANSSI continue d'observer en 2025 des activités offensives relatives à des MOA réputés russes ou chinois, liées à de telles opportunités politiques ou géopolitiques. Par exemple, l'éditeur de sécurité Recorded Future a observé la coïncidence de la visite du secrétaire de la Défense américain Pete Hegseth au Panama entre le 22 et le 24 avril 2025 avec des actions de reconnaissance massive d'entités panaméennes au moyen du MOA réputé chinois RedNovember[35].

En Europe, les élections qui ont eu lieu dans différents pays à la fin de l'année 2024 et courant 2025 ont constitué des opportunités d'attaques cyber ou à des fins d'influence. L'ANSSI et VIGINUM[36] sont particulièrement attentifs aux campagnes ciblant les contextes européens et aux menaces qui pourraient être transposées à l'encontre de la France. VIGINUM a notamment documenté des manipulations de l'information ayant ciblé l'élection présidentielle roumaine de 2024 lors de laquelle des modes opératoires informationnels ont artificiellement promu certains contenus sur la plateforme TikTok [73]. Les documents déclassifiés par la présidence roumaine ont également mentionné des attaques informatiques à l'encontre d'entités roumaines associées au processus électoral, qui pourraient être liées à des attaquants étatiques [74]. La présidence roumaine a par ailleurs rappelé que la Roumanie est une cible régulière d'attaques hybrides russes.

En novembre 2025, dans le contexte des élections municipales au Danemark, des sites Internet de partis politiques ainsi que celui du Parlement danois ont été la cible d'attaques DDoS revendiquées par le groupe hacktiviste pro-russe NoName057 [75] [76].←

35
Le MOA RedNovember, *alias* Storm-2077, serait utilisé à des fins d'espionnage et associé à la Chine d'après Microsoft [95].

36
Créé le 13 juillet 2021 et rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), VIGINUM est le service technique et opérationnel dont l'État s'est doté pour renforcer le dispositif national de lutte contre les manipulations de l'information. Ayant pour raison d'être la protection du débat public numérique touchant aux intérêts fondamentaux de la Nation, VIGINUM est en charge d'une mission défensive : la détection et la caractérisation des ingérences numériques étrangères.


ANSSI

B
OPPORTUNITÉS TECHNIQUES AMENÉES PAR LES VULNÉRABILITÉS

L'exploitation de vulnérabilités constitue encore cette année l'un des principaux vecteurs de compromission utilisés par les attaquants, qui ciblent notamment les équipements de bordure de SI (comme des pare-feu, serveurs mandataires, passerelle anti-spam etc.). Y réagir efficacement suppose une connaissance de leur cycle de vie et des enjeux associés.

1/ENJEUX ASSOCIÉS AU CYCLE DE VIE DES VULNÉRABILITÉS

Une vulnérabilité peut être identifiée par un éditeur, un chercheur, une entité tierce ou un attaquant. Suite à sa découverte, et selon le découvreur, elle fait l'objet d'une divulgation publique ou coordonnée, ou encore d'un premier code d'exploitation. Le cycle d'une vulnérabilité s'initie dès qu'elle est identifiée et se termine au moment où les défenseurs ont appliqué le correctif de sécurité. Lorsque l'éditeur est impliqué dans ce processus au plus tôt, le risque peut être endigué. En effet, l'éditeur peut produire puis distribuer le correctif de sécurité pour la vulnérabilité et quand les utilisateurs l'obtiennent, ils peuvent déployer le correctif. Cependant, la menace s'accroît quand un attaquant prend l'initiative de chercher, développer, exploiter et diffuser du code d'exploitation pour une vulnérabilité.

Au fur et à mesure que la connaissance sur une vulnérabilité s'accumule, le niveau de compétence nécessaire pour l'exploiter se réduit. En effet, les analyses différentielles de correctifs et les publications de documentation technique permettent à des attaquants aux compétences techniques moins sophistiquées de développer ou de se procurer des codes d'exploitation fiables et interopérables. Un équipement exposé et vulnérable finit toujours par être pris pour cible. Les défenseurs connaissant leurs systèmes d'informations et ayant une stratégie d'application effective et systématique des correctifs de sécurité peuvent anticiper cette démocratisation graduelle de la menace.

Les enjeux sont d'autant plus prégnants que le rythme de publication de vulnérabilités continue d'augmenter fortement, avec une croissance moyenne de 18 % par an depuis 2020. Si seuls 6 % des vulnérabilités sont exploitées [77], ce volume constitue un défi quotidien pour le maintien en condition de sécurité des systèmes d'informations. Prévenir, ou à défaut limiter, leurs conséquences implique donc plus que jamais de prioriser l'effort en fonction des risques encourus. Deux critères s'avèrent clés dans cette optique : la sévérité de la vulnérabilité, exprimée par le score CVSS[37], et la criticité du serveur affecté, exprimée par l'enjeu métier.

Les serveurs exposés sur Internet, en particulier, nécessitent une surveillance et une réactivité accrues. Ceux-ci, et en particulier les équipements de bordure et de sécurité, constituent une cible de choix et ont donné lieu à plusieurs alertes du CERT-FR.

L'observation des exploitations et de la publication de code d'exploitation doit également faire l'objet d'une veille permanente, notamment en s'appuyant sur les alertes du CERT-FR. En effet, selon les sources et les périmètres considérés, de l'ordre de 8 % des vulnérabilités exploitées le seraient avant leur publication ou celle d'un correctif [77], et, en 2025, environ 29 % l'auraient été le jour même ou avant leur publication [78]. Ces vulnérabilités nécessitent une réaction rapide et efficace afin de réduire les opportunités d'actions des attaquants.

37
Common Vulnerability Scoring System est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables [96].

→ Outre les vulnérabilités publiées en 2025 et exploitées rapidement après leur publication, des attaquants utilisent des vulnérabilités plus anciennes et non corrigées.
À titre d'exemple, en 2025 l'ANSSI a traité un incident au cours duquel la vulnérabilité CVE-2024-55591, publiée depuis plusieurs mois, a été utilisée pour mener une compromission d'envergure d'une entité française. L'exploitation de cette vulnérabilité permet à un attaquant de contourner le mécanisme d'authentification de l'interface d'administration d'un équipement Fortinet et d'obtenir un haut niveau de privilèges. Une fois administrateur du pare-feu, l'attaquant a restreint les droits des administrateurs légitimes, empêchant l'accès à l'équipement au bénéficiaire.
Cette vulnérabilité vient également rappeler combien les interfaces d'administration sont des cibles de choix, dont l'exposition sur Internet, encore fréquemment observée, est à proscrire. Lors du signalement de cette seule vulnérabilité aux entités concernées, le CERT-FR a ainsi constaté plus de 3700 interfaces d'administration exposées en France. ←

→ La gestion des vulnérabilités d'un système d'information ne peut être efficace que si les produits qui le composent font eux-mêmes l'objet d'une gestion efficace par leurs fabricants. C'est dans cet objectif que le Cyber Resilience Act (CRA) imposera aux fournisseurs de produits numériques commercialisés en Europe, à compter du 11 septembre 2026, de signaler aux CSIRT nationaux comme le CERT-FR de l'ANSSI toute vulnérabilité activement exploitée et tout incident grave ayant des répercussions sur la sécurité de leurs produits. Il est d'ailleurs déjà possible d'effectuer des signalements sur le site du CERT-FR [ClubSSI – Assistance et déclarations règlementaires].
À compter du 11 décembre 2027, ce dispositif imposera aux fournisseurs un certain nombre d'exigences complémentaires qu'ils devront respecter pour assurer la cybersécurité de leurs produits présents sur le marché européen :

- Recenser et documenter les vulnérabilités et les composants du produit ;
- Gérer et corriger sans retard les vulnérabilités qui touchent les produits ;
- Soumettre régulièrement les produits comportant des éléments numériques à des tests et examens de sécurité efficace ;
- Dès la publication d'une mise à jour de sécurité, communiquer sur les vulnérabilités corrigées ;
- Mettre en place et appliquer une politique de divulgation coordonnée des vulnérabilités ;
- Prendre des mesures pour faciliter le partage d'informations sur les vulnérabilités potentielles de leurs produits ;
- Prévoir des mécanismes de distribution sécurisée des mises à jour ;
- Veiller à diffuser sans retard les correctifs ou mises à jour de sécurité ;

Le contrôle de ces obligations sera assuré par l'ANFR (Autorité nationale des fréquences), désignée autorité de surveillance du marché, en coopération avec l'ANSSI. ←

On notera cependant que ces pratiques ne sont pour l'heure pas pleinement généralisées. En effet, on observe quasi systématiquement qu'après une baisse drastique du nombre d'actifs vulnérables exposés dans les jours qui suivent une alerte, une proportion non négligeable reste durablement vulnérable. Ainsi, plus de 6200 actifs en France sont encore, fin 2025, affectés par les principales vulnérabilités exploitées depuis 2023 et 2024 [79].

2/VULNÉRABILITÉS NOTABLES EN 2025 ET AUTRES FAIBLESSES D'ÉQUIPEMENTS DE BORDURE

Si de plus en plus de vulnérabilités sont identifiées et font l'objet d'une publication chaque année, les incidents traités par l'ANSSI montrent que quelques-unes d'entre elles ont été exploitées de manière récurrente et massive à des fins de compromission en 2025.

Les équipements de bordure restent des cibles privilégiées, d'autant plus quand ils sont largement répandus, offrant ainsi aux attaquants la possibilité d'un ciblage massif et opportuniste à même de leur fournir un accès initial ou de les enrôler dans des infrastructures d'anonymisation.

Certaines vulnérabilités peuvent aussi être exploitées de manière plus discrète, à la fois pour préserver les capacités qu'elles offrent aux attaquants, mais aussi contribuer à la furtivité de ces derniers. Par exemple, lors d'un incident traité par l'ANSSI, un attaquant a corrigé lui-même les vulnérabilités CVE-2024-8190, CVE-2024-8963 et CVE-2024-9380[38], après les avoir exploitées pour ensuite se latéraliser dans le réseau interne de l'entité victime. Lors des scans de vulnérabilités internes, ces équipements apparaissaient donc comme étant à jour. Cet exemple illustre que la gestion des correctifs doit impliquer un suivi méticuleux de leur mise en œuvre.

Depuis le début 2025, l'ANSSI a été alertée de multiples compromissions d'équipements VPN Connect Secure – commercialisés par Ivanti – par des attaquants exploitant les vulnérabilités CVE-2025-0282 et CVE-2025-0283 [80] [81]. Dans au moins deux cas, l'attaquant est parvenu à se latéraliser au sein du système d'information pour atteindre des ressources internes. Le jour de la publication du correctif, le 8 janvier 2025, l'éditeur de sécurité Mandiant publiait un rapport relatif à l'exploitation de la vulnérabilité CVE-2025-0282 depuis au moins mi-décembre 2024 par le MOA réputé chinois UNC5221[39]. Ce mode opératoire avait déjà été utilisé au moins à trois reprises entre décembre 2023 et mars 2025 pour exploiter des vulnérabilités jour-zéro affectant des équipements de sécurité Ivanti. Ces campagnes d'attaques ont mené à la compromission de plusieurs équipements Ivanti dans le monde, dont certains appartenant à des entités publiques et privées en France (sources : GTIG, Volexity, GTIG, justice.gov). Cela démontre l'intérêt tout particulier que peuvent porter certains acteurs à ces équipements.

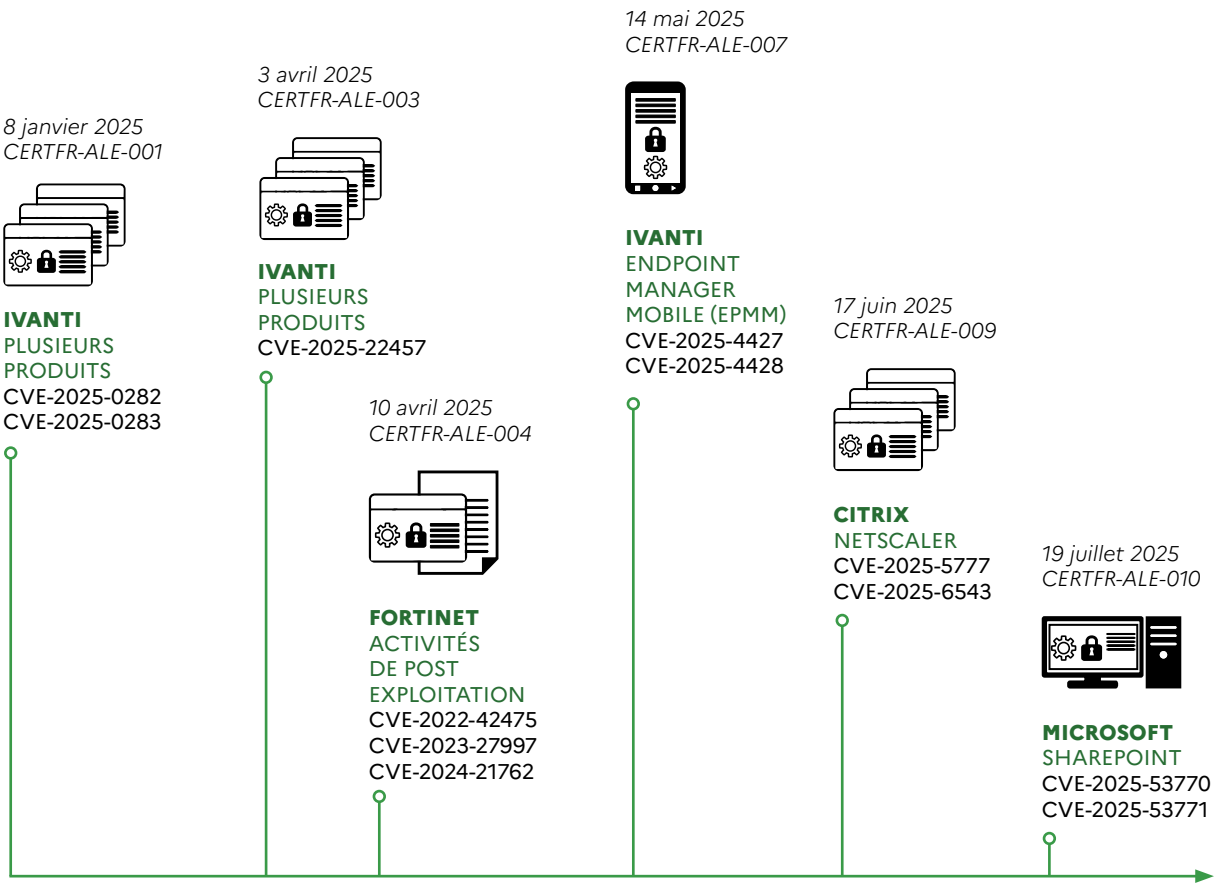
Les environnements serveur et bureautique ont également été victimes d'importantes vulnérabilités exploitées. Cela témoigne de l'intérêt des attaquants pour les données directement accessibles depuis les équipements qu'ils compromettent, tant à des fins d'espionnage que d'extorsion.

La solution Sharepoint de Microsoft a ainsi fait l'objet au cours de l'été 2025 de multiples vulnérabilités exploitées. Corrigées dans les mises à jour publiées respectivement les 8 puis 20 juillet 2025, les vulnérabilités CVE-2025-49704, CVE-2025-49706 puis CVE-2025-53771 et CVE-2025-53770 ont en effet donné lieu à de multiples vagues d'exploitation. Si l'exploitation à large échelle des deux premières vulnérabilités, baptisée « *toolshell* », a été rapportée publiquement pour la première fois par Eye Security le 18 juillet [82], l'ANSSI a observé leur exploitation en jour-zéro dès la fin du mois de juin 2025. Plusieurs preuves de concept d'exploitation ont ensuite été publiées à partir du 21 juillet, mettant leur usage à portée d'un plus grand nombre d'acteurs malveillants.

38
Vulnérabilités affectant les équipements Ivanti CSA.

39
Le MOA UNC5221, également suivi sous l'identifiant de MOA UTA0178 et considéré comme un sous-cluster de APT27 par les équipes de sécurité de Google.

Vulnérabilités les plus exploitées dans les incidents traités par l'ANSSI en 2025



→ Plusieurs compromissions d'équipements Ivanti VPN Connect Secure ont également été signalées à l'ANSSI à la suite de l'exploitation de la vulnérabilité CVE-2025-22457, pouvant aussi permettre l'exécution de code arbitraire à distance. Là encore, le délai entre la publication de l'alerte et l'analyse détaillée de la vulnérabilité a été très court.

Au-delà des vulnérabilités, il existe des faiblesses d'équipements de bordure qui ne font pas l'objet d'un identifiant CVE[40]. L'ANSSI a ainsi traité une large campagne de compromission d'équipements Cisco, lors de laquelle un attaquant a profité des faiblesses d'un protocole dénué de mécanisme d'authentification exposé sur Internet – Cisco Smart Install (SMI). Lors d'une première phase, l'attaquant a réalisé de premières actions massives et non ciblées visant à exposer la configuration des équipements sur Internet. Puis, des actions plus ciblées ont été observées sur certaines entités. L'ANSSI suspecte que ces fonctionnalités non documentées ont pu être utilisées de manière combinée avec d'autres vulnérabilités, permettant ainsi à l'attaquant de se latéraliser sur les SI de ses victimes. Au total, plus de 50 équipements ont été compromis lors de cette campagne.

Par ailleurs, dans de nombreux incidents traités en 2025, les attaquants ont compromis des comptes VPN – dépourvus de mécanismes d'authentification forte – pour s'introduire dans les réseaux internes de leurs cibles. Bien qu'il ne s'agisse pas d'une nouvelle tendance, cette méthode reste un vecteur d'intrusion privilégié par les attaquants qui tirent profit de ces passerelles insuffisamment protégées. Allant du simple compte utilisateur au compte d'un prestataire, l'ANSSI est intervenue sur de nombreux cas d'infection par rançongiciel où cette faiblesse technique était exploitée. ←

40 Common Vulnerabilities and Exposures (CVE) est un catalogue des vulnérabilités de sécurité informatique connues à l'échelle mondiale.

Parmi les nombreux cas de compromission de serveurs SharePoint, le groupe rançongiciel WarLock en a exploité les vulnérabilités pour prendre pied sur les réseaux internes d'entités françaises et procéder au chiffrement de leurs ressources. D'autres attaquants ont été vus exploiter ces vulnérabilités et accéder à des données métiers d'intérêt sans que leurs motivations ne soient précisément caractérisées. Parmi les actions effectuées par les attaquants, la récupération des *Machine Keys*, clés utilisées notamment pour le chiffrement des données sensibles, a été constatée. Cette pratique vient rappeler qu'en plus d'appliquer le correctif de sécurité et d'évincer un éventuel attaquant, la réaction à une vulnérabilité exploitée impose également un renouvellement des secrets qui sont associés à l'équipement affecté, ici les *Machine Keys*.

3/WEBMAIL, VIRTUALISATION ET MOBILES RESTENT DES CIBLES DE CHOIX

L'exploitation de vulnérabilités jour-zéro de type XSS[41] à l'encontre de clients *webmail* est une tendance importante observée en 2025, dans la continuité des années précédentes. Si le potentiel offensif de ce type de vulnérabilités est limité, notamment par l'impossibilité de persister sur la machine victime, il permet néanmoins différents effets intéressants pour un attaquant : vol de courriels ou de listes de contacts, récupération d'identifiants par une fausse page de connexion ou encore mise en place de filtres de redirection de courriels. De telles attaques ont notamment été associées à des modes opératoires réputés liés à la menace russe et potentiellement biélorusse comme UNC1151 [83] et APT28 [84] [85] en 2025 ou encore Winter Vivern dès 2023 [86].

Le succès des solutions de virtualisation ne faiblissant pas, celles-ci ont de nouveau été ciblées et compromises au moyen de vulnérabilités jour-zéro en 2025. En particulier, le 6 mars 2025 trois vulnérabilités critiques (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226) affectant VMware ESXi, Workstation et Fusion ont été publiées, en même temps que leur exploitation jour-zéro a été révélée [87].

Ce type de solution est particulièrement ciblé par les opérateurs de MOA réputés chinois. En 2025, les MOA UNC5221 et UNC5174 (suivi sous le nom de MOA Houken par l'ANSSI) ont ciblé et compromis de tels environnements [88] [89]. Les attaquants derrière le MOA UNC5221 auraient en outre démontré une très bonne compréhension de ces environnements, notamment en injectant un filtre Servlet en mémoire pour déposer une porte dérobée sur un serveur VMware vCenter. ←

41
Les vulnérabilités de type *cross site scripting* (XSS) ou par injection de code indirecte consistent à injecter des données arbitraires dans le code de pages HTML, par exemple dans l'optique de rediriger un utilisateur vers d'autres sites.

Ciblage de terminaux mobiles

Les téléphones mobiles font aujourd'hui partie du quotidien. L'augmentation croissante des usages, aussi bien liés à la vie personnelle que professionnelle, en font une cible de choix pour les attaquants, notamment pour les informations qui y sont concentrées. Des vulnérabilités au niveau des interfaces sans fil (réseau mobile, Wi-Fi, Bluetooth) ou au niveau du système d'exploitation sont ainsi régulièrement exploitées, tout comme certaines applications, de par la sensibilité des données qu'elles contiennent. Ainsi, comme tout équipement informatique, les téléphones mobiles exposent des opportunités à des attaquants aux motivations diverses.

Parmi ces menaces, l'ANSSI observe principalement des compromissions à des fins d'espionnage et de surveillance menées par des acteurs étatiques grâce à des capacités développées en interne ou acquises auprès d'entreprises privées spécialisées dans la lutte informatique offensive (LIOP). Ces dernières facilitent l'accès à des technologies sophistiquées, entraînant l'émergence de nouveaux acteurs offensifs, et augmentant ainsi le niveau de menace associé. Au-delà de l'espionnage, les téléphones mobiles sont aussi une cible de choix pour les cybercriminels, motivés notamment par des gains financiers ou, dans une moindre mesure, détournés pour de la surveillance privée ou des opérations de déstabilisation.

Des vulnérabilités avancées sont régulièrement corrigées dans les composants et applications. En août et septembre 2025, Apple, Samsung et Meta ont publié des mises à jour concernant des vulnérabilités (respectivement CVE-2025-43300, CVE-2025-21043 et CVE-2025-55177) activement exploitées, et dont la combinaison permet de compromettre des téléphones Apple ou Samsung à distance, sans action de l'utilisateur. Une première vulnérabilité, présente dans WhatsApp, était chaînée avec une vulnérabilité dans le composant de traitement d'images au format DNG du système d'exploitation (iOS ou Android). La concomitance des vulnérabilités ciblant le même format sur les systèmes iOS et Samsung, associée à une vulnérabilité zéro-clic dans une application de messagerie populaire, témoigne de capacités de recherche sophistiquées et d'une volonté de cibler un large panel d'utilisateurs.

Depuis 2021, Apple envoie des vagues de « notifications de menace » aux victimes dont les équipements mobiles ont été ciblés par des logiciels espions tels que Pegasus, Predator ou Triangulation[42]. L'ANSSI a choisi de communiquer sur ces alertes afin de sensibiliser les hautes autorités, les comités de direction d'entreprises et la société civile sur ces menaces. En complément, l'ANSSI a publié un document qui revient de manière plus détaillée sur les différents vecteurs techniques exploités par les attaquants pour compromettre des téléphones mobiles. Il propose aussi une vue d'ensemble sur les menaces pesant sur les utilisateurs en fournissant des exemples concrets d'attaques conduites en France ou à l'étranger. Enfin, des recommandations de sécurité à destination des utilisateurs accompagnent cet état de la menace [90]. Au niveau international, la France a initié le Processus de Pall Mall, qui vise à lutter contre la prolifération et l'usage irresponsable de capacités commerciales de cyber-intrusion.

42
En cas de réception de signalements (courriels, SMS) issus des éditeurs de solutions et avertissant d'une potentielle compromission d'un compte ou d'un appareil, il est fortement conseillé de ne pas manipuler votre téléphone et de contacter le CERT-FR
- par courriel → à l'adresse cert-fr@ssi.gouv.fr ou
- par téléphone → au 3218 (service gratuit + prix d'un appel) → ou +33 (0) 9 70 83 32 18.

C
LE CIBLAGE DES SOUS-TRAITANTS COMME VECTEUR DE COMPROMISSION

→ Les attaques contre la chaîne logistique ou d'approvisionnement (*supply-chain attack*) consistent à compromettre un tiers, comme un fournisseur de services logiciels ou un prestataire, afin de cibler la victime finale. Cette technique est éprouvée et exploitée par plusieurs acteurs étatiques et cybercriminels depuis au moins 2016. Cette méthode présente un risque de propagation rapide d'une attaque qui peut parfois concerner un secteur d'activité entier ou une zone géographique précise notamment lorsque l'attaque cible un fournisseur de logiciels largement répandus ou une entreprise de service numérique (ESN) locale ou spécialisée dans un secteur d'activité particulier [91]. Les attaquants à l'origine de ces attaques peuvent chercher à exfiltrer des informations via un tiers, réaliser des attaques lucratives ou alors paralyser de manière temporaire ou pérenne un secteur ou un ensemble d'entités données.

Avec le développement de la sous-traitance, assortie d'une délégation de compétences au sein de certains secteurs d'activités, les entreprises peuvent ne plus maîtriser l'intégralité des équipements qu'elles incorporent dans leurs réseaux. Cette situation de fait affaiblit le niveau de sécurisation des environnements, et les attaquants peuvent exploiter cette moindre maîtrise pour réaliser leurs compromissions.

Plusieurs acteurs étatiques réputés russes, chinois ou iraniens ont pu mener des attaques via la chaîne d'approvisionnement ces dernières années.

Les attaques via la chaîne d'approvisionnement ne sont cependant pas uniquement l'apanage des MOA réputés étatiques. Entre janvier et juin 2025, l'ANSSI a observé la compromission par rançongiciels de plusieurs entités industrielles impliquées dans la chaîne d'approvisionnement de la Base Industrielle et Technologique de Défense (BITD) française. Ces entreprises, à l'origine de la conception et de la fabrication de systèmes, de pièces et de logiciels liés aux secteurs de l'armement et de l'aéronautique peuvent disposer d'informations sensibles, potentiellement exposées lors de ces attaques. Si l'ANSSI ne considère pas que ces attaques ont été menées de manière coordonnée (les entreprises ont été compromises par des opérateurs de rançongiciels différents), ces événements de sécurité rappellent ainsi l'importance d'identifier ces sous-traitants essentiels et de les aider à améliorer leur sécurité informatique. Le secteur de la défense a également fait l'objet en 2025 d'actions de reconnaissance, de tentatives de compromissions et de compromissions par des modes opératoires réputés étatiques à des fins d'espionnage stratégique et de renseignement.

En 2025, l'ANSSI a été témoin de nombreuses compromissions d'entités par des attaquants en mesure de se latéraliser depuis les systèmes d'information de prestataires vers des clients. À titre d'exemple, un attaquant a compromis et exfiltré des ressources clientes chez un prestataire de nombreuses entités françaises. En tirant parti des interconnexions existantes avec les systèmes d'information des clients et grâce à des authentifiants volés, l'attaquant est parvenu à se latéraliser sur le système d'information de plusieurs clients.

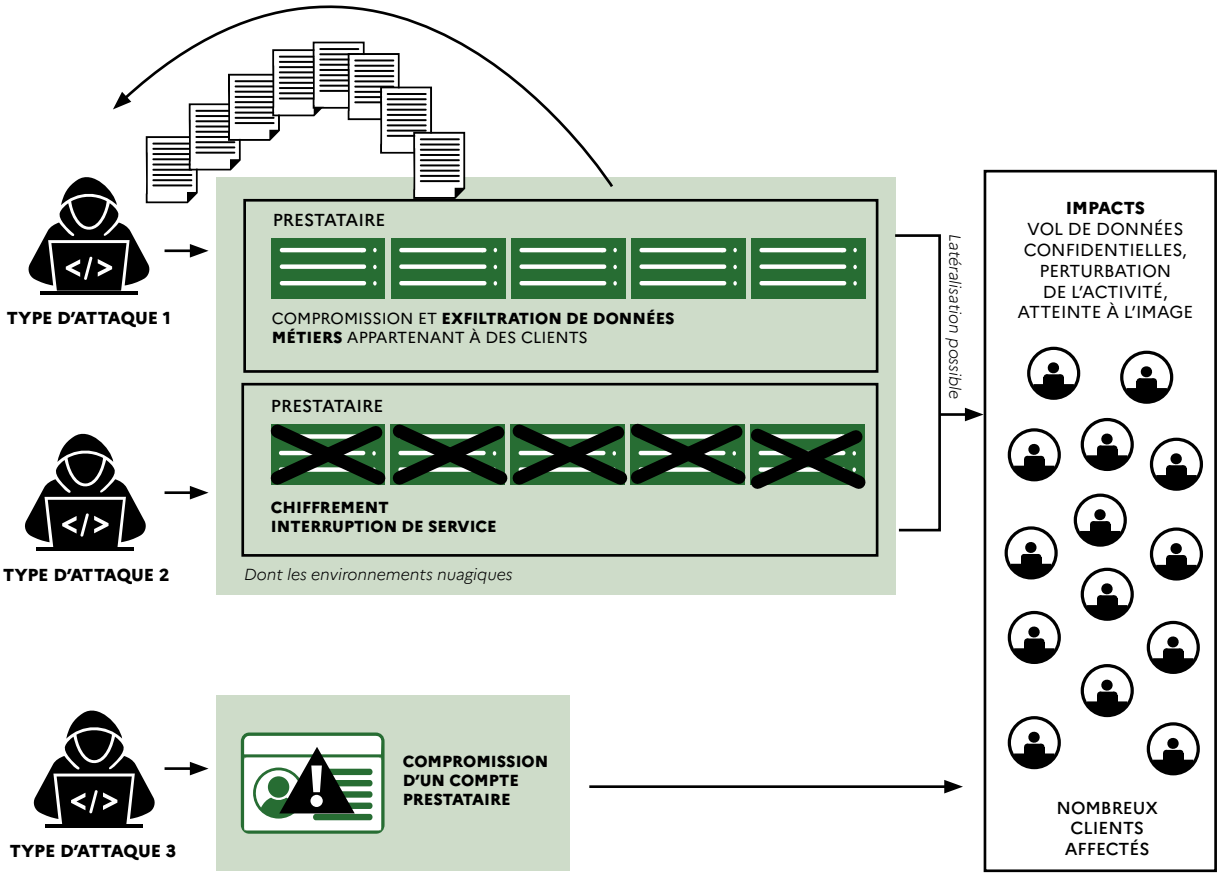
Dans d'autres cas observés par l'Agence, les attaquants ont réalisé des attaques par rebond en compromettant une victime initiale et en utilisant les ressources de celle-ci pour réaliser de nouvelles compromissions, sans qu'il ne s'agisse forcément de sous-traitant. Les ressources internes de la première entité compromise peuvent alors servir à forger ou utiliser des éléments crédibles permettant de mieux cibler une deuxième entité [92], [93].

Par ailleurs, l'ANSSI a été témoin de plusieurs compromissions par rançongiciel de prestataires causant des impacts forts sur les clients. Au cours de l'année, les ressources d'une entité française ont été

compromises par un rançongiciel perturbant ainsi l'accès de l'ensemble clients à l'application fournie. Cet incident a perturbé fortement les activités de nombreux acteurs d'un même secteur d'activité.

Les mesures d'endiguement prises dans ce type d'attaque peuvent également engendrer des impacts forts sur les clients qui perdent l'accès à certaines ressources. ←

Chaîne d'approvisionnement



Compromission des environnements cloud

Du fait de l'adoption croissante des services cloud par de nombreuses organisations, les cas de compromission de données présentes dans ces environnements sont régulièrement observés. De multiples cas d'attaques par rançongiciel impliquant le chiffrement de données présentes sur des ressources cloud ont notamment été portés à la connaissance de l'ANSSI en 2025, dénotant la prise en compte de cette évolution par de nombreux acteurs malveillants. La généralisation de cette pratique d'hébergement constitue une opportunité pour ces acteurs d'obtenir des données de multiples entités en compromettant un unique prestataire.

En octobre 2025, l'ANSSI a été informée d'une attaque par rançongiciel aboutissant au chiffrement de ressources liées à une solution *software-as-a-service* d'un éditeur français hébergée sur un environnement cloud Amazon Web Services.

Le manque de contrôle sur ces environnements de la part du client final peut parfois constituer un frein aux capacités d'analyse dans le cadre d'actions de réponse à incidents. Lors d'une compromission d'ampleur détectée en 2025, certaines levées de doute menées par l'entité victime avec l'appui de l'ANSSI n'ont pu aboutir du fait de la difficulté d'obtention de journaux d'activité (*logs*) relatifs à des ressources cloud possiblement compromises.

Il est également à noter que les incidents impliquant des fournisseurs de service cloud, maillons aujourd'hui critiques dans la chaîne d'approvisionnement de la quasi-totalité des secteurs d'activité, peuvent affecter un nombre important d'entités finales. En juillet 2025, la compromission et le chiffrement de ressources cloud d'une entité française d'importance est observée, entraînant une indisponibilité momentanée de services pour des clients professionnels ainsi que pour des services grand public en France.

L'ANSSI a été informée par l'un de ses bénéficiaires de la compromission d'une plateforme de développement hébergée dans le cloud. L'attaquant a exploité une vulnérabilité présente sur un équipement de bordure entraînant des interruptions de service au niveau de ce dernier. La réactivité de la victime à mener des actions de remédiation a permis de mettre un terme aux actions malveillantes.

Ces attaques peuvent également affecter la confidentialité des données hébergées à l'instar de la cyberattaque ayant visé la société RedHat, dont une instance GitLab a été compromise en octobre 2025, entraînant le vol de données liées à de nombreuses organisations à travers le monde, dont des entités françaises.

Plusieurs cas de déploiement de logiciels crypto-mineurs sur des ressources cloud sont enfin régulièrement observés. En juin 2025, l'ANSSI a ainsi été informée de la compromission d'instances cloud appartenant à une entité publique par un acteur malveillant permettant à celui-ci de tenter d'exploiter les ressources de calcul disponibles à des fins de minage de cryptomonnaies.

L'ANSSI a publié en 2025 un État de la menace ciblant le secteur du Cloud Computing, comprenant des recommandations à destination des fournisseurs de services cloud et de leurs clients [94].


SECURITY
PANORAMA
DEFENSE
CYBERMENACE

RÉFÉRENCES

[01] SUSPECTED COLLINS AEROSPACE HACKER ARRESTED IN UK.
24 09 2025.
https://www.bankinfosecurity.com/suspected-collins-aerospace-hacker-arrested-in-uk-a-29531

[02] NEWS, RECORDED FUTURES. RESEARCHERS WARN OF QILIN RANSOMWARE GANG AFTER GROUP HIT HUNDREDS OF ORGS THIS YEAR.
28 10 2025.
https://therecord.media/qilin-ransomware-gang-hits-hundreds-of-orgs-2025

[03]. OPÉRATION ENDGAME 2025.
23 05 2025.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-008/

[04] PRÉPARER LA REMÉDIATION.
16 01 2026.
https://messervices.cyber.gouv.fr/guides/cyberattaques-et-remediation-preparer-la-remedation

[05] ORACLE E-BUSINESS SUITE ZERO-DAY EXPLOITED IN WIDESPREAD EXTORTION CAMPAIGN.
10 09 2025.
https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation

[06] EXFILTRATION DE DONNÉES DU SECTEUR SOCIAL: RETOUR D'EXPÉRIENCE DU CERT-FR.
18 09 2024.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-009.pdf

[07] EXTORTION AND RANSOMWARE TRENDS JANUARY-MARCH 2025.
23 04 2025.
https://unit42.paloaltonetworks.com/2025-ransomware-extortion-trends/

[08] #STOPRANSOMWARE: RANSOMWARE ATTACKS ON CRITICAL INFRASTRUCTURE FUND DPRK MALICIOUS CYBER ACTIVITIES.
09 02 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a

[09] APT41: A DUAL ESPIONAGE AND CYBER CRIME OPERATION.
07 08 2019.
https://cloud.google.com/blog/topics/threat-intelligence/apt41-dual-espionage-and-cyber-crime-operation?hl=en

[10] MEET NAILAOLOCKER: A RANSOMWARE DISTRIBUTED IN EUROPE BY SHADOWPAD AND PLUGX BACKDOORS.
18 02 2025.
https://www.orangecyberdefense.com/global/blog/cert-news/meet-nailaolocker-a-ransomware-distributed-in-europe-by-shadowpad-and-plugx-backdoors

[11] NAILAOLOCKER RANSOMWARE'S "CHEESE".
18 07 2025.
https://www.fortinet.com/blog/threat-research/nailaolocker-ransomware-cheese

[12] UPDATED SHADOWPAD MALWARE LEADS TO RANSOMWARE DEPLOYMENT.
20 02 2025.
https://www.trendmicro.com/en_us/research/25/b/updated-shadowpad-malware-leads-to-ransomware-deployment.html

[13] SUPPLY CHAIN ATTACKS: MENACES SUR LES PRESTATAIRES DE SERVICE ET LES BUREAUX D'ÉTUDES.
07 10 2019.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2019-CTI-004/

[14] CHINA-LINKED ESPIONAGE TOOLS USED IN RANSOMWARE ATTACKS.
13 02 2025.
https://www.security.com/threat-intelligence/chinese-espionage-ransomware

[15] RUSSIAN FSB CYBER ACTOR STAR BLIZZARD CONTINUES WORLDWIDE SPEARPHISHING CAMPAIGNS.
07 12 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-341a

[16] THE CALLISTO GROUP.
04 2017.
https://labs.withsecure.com/content/dam/labs/docs/callisto-group.pdf

[17] FRENCH NGO REPORTERS WITHOUT BORDERS TARGETED BY CALISTO IN RECENT CAMPAIGN.
03 12 2025.
https://blog.sekoia.io/ngo-reporters-without-borders-targeted-by-calisto-in-recent-campaign/

[18] RSF CIBLÉE PAR UNE CYBERATTAQUE ATTRIBUÉE À UN GROUPE RÉPUTÉ PROCHE DES SERVICES DE RENSEIGNEMENTS RUSSES.
08 12 2025.
https://rsf.org/fr/rsf-cibl%C3%A9e-par-une-cyberattaque-attribu%C3%A9e-%C3%A0-un-groupe-r%C3%A9put%C3%A9-proche-des-services-de-renseignements

[19] AIVD AND MIVD IDENTIFY NEW RUSSIAN CYBER THREAT ACTOR.
27 05 2025.
https://www.aivd.nl/documenten/publicaties/2025/05/27/aivd-en-mivd-onderkennen-nieuwe-russische-cyberactor

[20] APT31/WUHAN XIAORUIZHI SCIENCE &TECHNOLOGY COMPANY, LTD.
https://rewardsforjustice.net/fr/rewards/apt31-wuhan-xiaoruizhi-science-technology-company-ltd/

[21] STATEMENT BY THE GOVERNMENT OF THE CZECH REPUBLIC ON THE CYBER ATTACK FROM THE PEOPLE´S REPUBLIC OF CHINA.
08 05 2025.
https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_by_the_government_of_the_czech.html

[22] UAT-5918 TARGETS CRITICAL INFRASTRUCTURE ENTITIES IN TAIWAN.
20 03 2025.
https://blog.talosintelligence.com/uat-5918-targets-critical-infra-in-taiwan/

[23] SALT TYPHOON: DATA THEFT LIKELY SIGNALS EXPANDED TARGETING.
11 06 2025.
https://s3.documentcloud.org/documents/25998809/20250611-dhs-salt-typhoon.pdf

[24] WHEN NOKIA PULLED OUT OF RUSSIA, A VAST SURVEILLANCE SYSTEM REMAINED.
28 03 2022.
https://www.nytimes.com/2022/03/28/technology/nokia-russia-surveillance-system-sorm.html

[25] DECEPTION IN DEPTH: PRC-NEXUS ESPIONAGE CAMPAIGN HIJACKS WEB TRAFFIC TO TARGET DIPLOMATS.
25 08 2025.
https://cloud.google.com/blog/topics/threat-intelligence/prc-nexus-espionage-targets-diplomats?hl=en

[26] UNC6384 WEAPONIZES ZDI-CAN-25373 VULNERABILITY TO DEPLOY PLUGX AGAINST HUNGARIAN AND BELGIAN DIPLOMATIC ENTITIES.
[En ligne] 30 10 2025.
https://arcticwolf.com/resources/blog/unc6384-weaponizes-zdi-can-25373-vulnerability-to-deploy-plugx/

[27] THE BADPILOT CAMPAIGN: SEASHELL BLIZZARD SUBGROUP CONDUCTS MULTIYEAR GLOBAL ACCESS OPERATION.
12 02 2025.
https://www.microsoft.com/en-us/security/blog/2025/02/12/the-badpilot-campaign-seashell-blizzard-subgroup-conducts-multiyear-global-access-operation/

[28] ENERGY SECTOR INCIDENT REPORT - 29 DECEMBER 2025.
29 12 2025.
https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

[29] DÉNI DE SERVICE RÉSEAU - QUALIFICATION.
28 07 2025.
https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-009/

[30] DÉNI DE SERVICE RÉSEAU - ENDIGUEMENT.
28 07 2025.
https://www.cert.ssi.gouv.fr/fiche/CERTFR-2024-RFX-010/

[31] RECOMMANDATIONS À DESTINATIONS DES ACTEURS DU SECTEUR DE L'ÉNERGIE ET DE L'EAU.
22 01 2026.
https://www.cert.ssi.gouv.fr/dur/CERTFR-2025-DUR-003/

[32] NORWAY'S SPY CHIEF BLAMES RUSSIAN HACKERS FOR DAM SABOTAGE IN APRIL.
[En ligne] 13 08 2025.
https://www.reuters.com/technology/norway-spy-chief-blames-russian-hackers-dam-sabotage-april-2025-08-13/

[33] REMOTE MONITORING AND MANAGEMENT (RMM) TOOLING INCREASINGLY AN ATTACKER'S FIRST CHOICE.
07 03 2025.
https://www.proofpoint.com/us/blog/threat-insight/remote-monitoring-and-management-rmm-tooling-increasingly-attackers-first-choice

[34] UK ARRESTS FOUR IN 'SCATTERED SPIDER' RANSOM GROUP.
10 07 2025.
https://krebsonsecurity.com/2025/07/uk-charges-four-in-scattered-spider-ransom-group/

[35] APT28 LEVERAGES MULTIPLE PHISHING TECHNIQUES TO TARGET UKRAINIAN CIVIL SOCIETY.
17 05 2023.
https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/

[36] APT28 CAMPAIGN TARGETING POLISH GOVERNMENT INSTITUTIONS.
08 05 2024.
https://cert.pl/en/posts/2024/05/apt28-campaign/

[37] FIGHTING URSA LURING TARGETS WITH CAR FOR SALE.
02 08 2024.
https://unit42.paloaltonetworks.com/fighting-ursa-car-for-sale-phishing-lure/

[38] APT28 OPERATION PHANTOM NET VOXEL.
16 09 2025.
https://blog.sekoia.io/apt28-operation-phantom-net-voxel/

[39] APT28 ATTACKS UKRAINIAN GOVERNMENT AGENCIES VIA SIGNAL USING MALWARE.
[En ligne] 01 07 2025.
https://csirt.csi.cip.gov.ua/en/posts/apt28-attacks-ukrainian-government-agencies-via-signal-using-malware

[40] APT MUDDYWATER DEPLOYS MULTI-STAGE PHISHING TO TARGET CFOS.
20 08 2025.
https://hunt.io/blog/apt-muddywater-deploys-multi-stage-phishing-to-target-cfos

[41] MAPPING THE INFRASTRUCTURE AND MALWARE ECOSYSTEM OF MUDDYWATER.
17 09 2025.
https://www.group-ib.com/blog/muddywater-infrastructure-malware/

[42] RECOMMANDATIONS DE SÉCURITÉ POUR UN SYSTÈME D'IA GÉNÉRATIVE.
29 04 2024.
https://messervices.cyber.gouv.fr/guides/recommandations-de-securite-pour-un-systeme-dia-generative

[43] SCATTERED SPIDER.
29 07 2025.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

[44] DEFENDING AGAINST SCATTERED SPIDER AND THE COM WITH CYBERCRIME INTELLIGENCE.
15 07 2024.
https://www.sans.org/blog/defending-against-scattered-spider-and-the-com-with-cybercrime-intelligence

[45] WHAT'S IN AN ASP? CREATIVE PHISHING ATTACK ON PROMINENT ACADEMICS AND CRITICS OF RUSSIA.
18 06 2025.
https://cloud.google.com/blog/topics/threat-intelligence/creative-phishing-academics-critics-of-russia?hl=en

[46] SAME SEA, NEW PHISH - RUSSIAN GOVERNMENT-LINKED SOCIAL ENGINEERING TARGETS APP-SPECIFIC PASSWORDS.
18 06 2025.
https://citizenlab.ca/research/russian-government-linked-social-engineering-targets-app-specific-passwords/

[47] STORM-2372 CONDUCTS DEVICE CODE PHISHING CAMPAIGN.
13 02 2025.
https://www.microsoft.com/en-us/security/blog/2025/02/13/storm-2372-conducts-device-code-phishing-campaign/

[48] MULTIPLE RUSSIAN THREAT ACTORS TARGETING MICROSOFT DEVICE CODE AUTHENTICATION.
13 02 2025.
https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/

[49] FAKE CAPTCHA ATTACKS DEPLOY INFOSTEALERS AND RATS IN A MULTISTAGE PAYLOAD CHAIN.
19 05 2025.
https://www.trendmicro.com/fr_fr/research/25/e/unmasking-fake-captcha-cases.html

[50] ADWARE CAMPAIGN USES FAKE CAPTCHA TO DELIVER LUMMA AND AMADEY MALWARE.
10 09 2024.
https://www.broadcom.com/support/security-center/protection-bulletin/adware-campaign-uses-fake-captcha-to-deliver-lumma-and-amadey-malware

[51] Кібератака UAC-0001 (APT28): PowerShell-команда в буфері обміну як "точка входу" (CERT-UA#11689).
25 10 2024.
https://cert.gov.ua/article/6281123

[52] COLDRIVER UPDATES ARSENAL WITH BAITSWITCH AND SIMPLEFIX.
24 09 2025.
https://www.zscaler.com/blogs/security-research/coldriver-updates-arsenal-baitswitch-and-simplefix

[53] PHANTOMCAPTCHA | MULTI-STAGE WEBSOCKET RAT TARGETS UKRAINE IN SINGLE-DAY SPEARPHISHING OPERATION.
22 10 2025.
https://www.sentinelone.com/labs/phantomcaptcha-multi-stage-websocket-rat-targets-ukraine-in-single-day-spearphishing-operation/

[54] APT39: AN IRANIAN CYBER ESPIONAGE GROUP FOCUSED ON PERSONAL INFORMATION.
29 01 2019.
https://cloud.google.com/blog/topics/threat-intelligence/apt39-iranian-cyber-espionage-group-focused-on-personal-information?hl=en

[55] PHOSPHORUS AUTOMATES INITIAL ACCESS USING PROXYSHELL.
21 03 2022.
https://thedfirreport.com/2022/03/21/phosphorus-automates-initial-access-using-proxyshell/

[56] DALBIT (M00NLIGHT): CHINESE HACKER GROUP'S APT ATTACK CAMPAIGN.
13 02 2023.
https://asec.ahnlab.com/en/47455/

[57] ICEPEONY WITH THE '996' WORK CULTURE.
16 10 2024.
https://nao-sec.org/2024/10/IcePeony-with-the-996-work-culture.html

[58] APT41 HAS ARISEN FROM THE DUST.
18 07 2024.
https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust?hl=en

[59] HOUKEN : SEEKING A PATH BY LIVING ON THE EDGE WITH ZERO DAYS.
01 07 2025.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-009.pdf

[60] GAMAREDON X TURLA COLLAB.
19 09 2025.
https://www.welivesecurity.com/en/eset-research/gamaredon-x-turla-collab/

[61] FRAUDSTERS IMPERSONATE CLOP RANSOMWARE TO EXTORT BUSINESSES.
14 03 2025.
https://www.infosecurity-magazine.com/news/fraudsters-clop-ransomware-extort/

[62] SHINYHUNTERS BEHIND SALESFORCE DATA THEFT ATTACKS AT QANTAS, ALLIANZ LIFE, AND LVMH.
30 07 2025.
https://www.bleepingcomputer.com/news/security/shinyhunters-behind-salesforce-data-theft-attacks-at-qantas-allianz-life-and-lvmh/

[63] THE RANSOMWARE CYBER THREAT LANDSCAPE H1-23.
13 07 2023.
https://www.kovrr.com/reports/the-ransomware-threat-landscape-h123

[64] TRACKING ADVERSARIES: EVILCORP, THE RANSOMHUB AFFILIATE.
02 04 2025.
https://blog.bushidotoken.net/2025/04/tracking-adversaries-evilcorp-ransomhub.html

[65] RANSOMWARE ANNUAL REPORT 2024.
13 01 2025.
https://cyberint.com/blog/research/ransomware-annual-report-2024/

[66] RANSOMWARE DEBRIS: AN ANALYSIS OF THE RANSOMHUB OPERATION.
25 04 2025.
https://www.group-ib.com/blog/ransomware-debris/

[67] BLACK BASTA RANSOMWARE LEAK: KEY FINDINGS AND INSIGHTS.
25 04 2025.
https://www.first.org/blog/20250321-black-basta-ransomware-leak

[68] INSIDE THE LOCKBIT'S ADMIN PANEL LEAK: AFFILIATES, VICTIMS AND MILLIONS IN CRYPTO.
[En ligne] 12 06 2025.
https://www.trellix.com/blogs/research/inside-the-lockbits-admin-panel-leak-affiliates-victims-and-millions-in-crypto/

[69] PANORAMA DE LA CYBERMENACE 2024.
11 03 2025.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-003.pdf

[70] STATE SECRETS FOR SALE: MORE LEAKS FROM THE CHINESE HACK-FOR-HIRE INDUSTRY.
01 07 2025.
https://spycloud.com/blog/state-secrets-for-sale-chinese-hacking/

[71] KNOWNSEC BREACH: WHAT WE KNOW SO FAR.
06 11 2025.
https://substack.com/home/post/p-178189244

[72] ILLUSTRATION DES PROBLÉMATIQUES LIÉES À L'INTÉGRATION DE LOGICIELS NON MAÎTRISÉS.
23 11 2022.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-006/

[73] MANIPULATION D'ALGORITHMES ET INSTRUMENTATLISATION D'INFLUENCEURS - ENSEIGNEMENTS DE L'ÉLECTION PRÉSIDENTIELLE EN ROUMANIE ET RISQUES POUR LA FRANCE.
02 2025.
https://www.sgdsn.gouv.fr/files/files/Publications/20250204_NP_SGDSN_VIGINUM_Rapport_public_Elections_roumanie_risques_france_VFF.pdf

[74] COMUNICAT DE PRESĂ.
04 12 2024.
https://www.presidency.ro/ro/media/comunicate-de-presa/comunicat-de-presa1733327193

[75] PRO-RUSSIAN GROUP CLAIMS HITS ON DANISH PARTY WEBSITES AS VOTERS HEAD TO POLLS.
[En ligne] 18 11 2025.
https://therecord.media/denmark-election-political-government-websites-ddos-incidents

[76] FLERE PARTIERS HJEMMESIDER RAMT AF DDOS-ANGREB.
17 11 2025.
https://samsik.dk/artikler/2025/11/flere-partiers-hjemmesider-ramt-af-ddos-angreb/.

[77] A VISUAL EXPLORATION OF EXPLOITATION IN THE WILD.
https://www.cyentia.com/wp-content/uploads/2024/07/EPSS-Exploration-Of-Exploits.pdf

[78] VULNCHECK STATE OF EXPLOITATION 2026.
21 01 2026.
https://www.vulncheck.com/blog/state-of-exploitation-2026

[79] SHADOWSERVER.
https://dashboard.shadowserver.org/statistics/combined/tree/?date_range=1&source=http_vulnerable&source=http_vulnerable6&tag=cve-2023-*&tag=cve-2024-*&geo=FR&data_set=count&scale=log

[80] SECURITY ADVISORY IVANTI CONNECT SECURE, POLICY SECURE & ZTA GATEWAYS (CVE-2025-0282, CVE-2025-0283).
08 01 2025.
https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US

[81] VULNÉRABILITÉ DANS LES PRODUITS IVANTI.
07 05 2025.
https://cert.ssi.gouv.fr/alerte/CERTFR-2025-ALE-001/

[82] SHAREPOINT UNDER SIEGE: TOOLSHELL EXPLOIT.
18 07 2025.
https://research.eye.security/sharepoint-under-siege/

[83] UNC1151 EXPLOITING ROUNDCUBE TO STEAL USER CREDENTIALS IN A SPEAR PHISHING CAMPAIGN.
05 06 2025.
https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/

[84] ESET IDENTIFIE UNE CAMPAGNE D'ESPIONNAGE DU GROUPE SEDNIT (APT28) EXPLOITANT DES FAILLES XSS DANS DES MESSAGERIES EN LIGNE.
15 05 2025.
https://www.eset.com/fr/about/newsroom/press-releases/recherche/espionnage-campagne-sednit-xss/

[85] 0DAY .ICS ATTACK IN THE WILD.
09 30 2025.
https://strikeready.com/blog/0day-ics-attack-in-the-wild/

[86] ZIMBRA VULNERABILITY TO TARGET WEBMAIL PORTALS OF NATO-ALIGNED GOVERNMENTS IN EUROPE.
03 30 2023.
https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability

[87] VMSA-2025-0004: VMWARE ESXI, WORKSTATION, AND FUSION UPDATES ADDRESS MULTIPLE VULNERABILITIES (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226).
04 03 2025.
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390

[88] YOU NAME IT, VMWARE ELEVATES IT (CVE-2025-41244).
29 09 2025.
https://blog.nviso.eu/2025/09/29/you-name-it-vmware-elevates-it-cve-2025-41244/

[89] ANOTHER BRICKSTORM: STEALTHY BACKDOOR ENABLING ESPIONAGE INTO TECH AND LEGAL SECTORS.
24 09 2025.
https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign?hl=en

[90] ÉTAT DE LA MENACE INFORMATIQUE SUR LES ÉQUIPEMENTS MOBILES.
26 11 2025.
https://cyber.gouv.fr/actualites/etat-de-la-menace-informatique-sur-les-equipements-mobiles/

[91] CYBERDICO.
https://cyber.gouv.fr/cyberdico/#S

[92] APT TODDYCAT.
21 06 2022.
Unveiling an unknown APT actor attacking high-profile entities in Europe and Asia.
https://securelist.com/toddycat/106799/

[93] SHARPPANDA: CHINESE APT GROUP TARGETS SOUTHEAST ASIAN GOVERNMENT WITH PREVIOUSLY UNKNOWN BACKDOOR.
03 06 2021.
https://research.checkpoint.com/2021/chinese-apt-group-targets-southeast-asian-government-with-previously-unknown-backdoor/

[94] SECTEUR DU CLOUD - ÉTAT DE LA MENACE INFORMATIQUE.
20 02 2025.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2025-CTI-001/

[95] MICROSOFT SHARES LATEST INTELLIGENCE ON NORTH KOREAN AND CHINESE THREAT ACTORS AT CYBERWARCON.
22 11 2024.
https://www.microsoft.com/en-us/security/blog/2024/11/22/microsoft-shares-latest-intelligence-on-north-korean-and-chinese-threat-actors-at-cyberwarcon/

[96] VULNERABILITY METRICS.
https://nvd.nist.gov/vuln-metrics/cvss

[97] ACTEURS ÉMANANT D'UN ÉTAT-NATION MIDNIGHT BLIZZARD.
25 01 2024.
https://www.microsoft.com/fr-fr/security/security-insider/midnight-blizzard

[98] SSU IDENTIFIES FSB HACKERS RESPONSIBLE FOR OVER 5,000 CYBER ATTACKS AGAINST UKRAINE (VIDEO).
04 11 2021.
https://ssu.gov.ua/en/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy

RESSOURCES

PANORAMA DE LA CYBERMENACE 2025

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

Mars 2026
Publié sous licence Ouverte/ Open Licence (Etalab — V2.0)

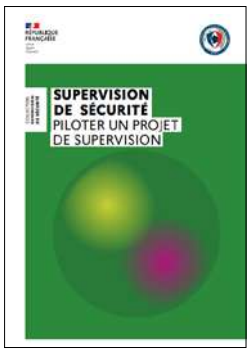
ISSN : 2970-8818

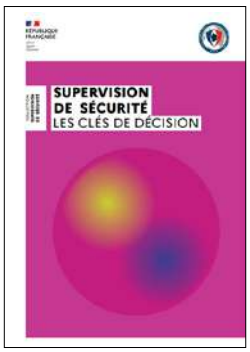
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

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

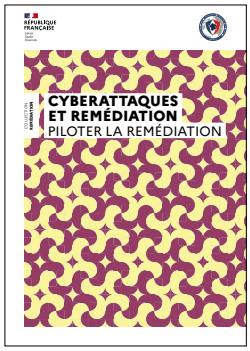
RETROUVEZ TOUS NOS GUIDES DE BONNES PRATIQUES SUR
messervices.cyber.gouv.fr

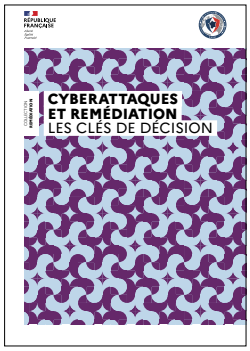
Collection Supervision de sécurité

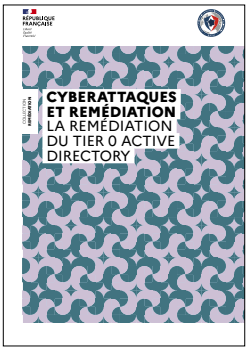




Collection Cyberattaques et remédiation







Collection Gestion de crise cyber

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*