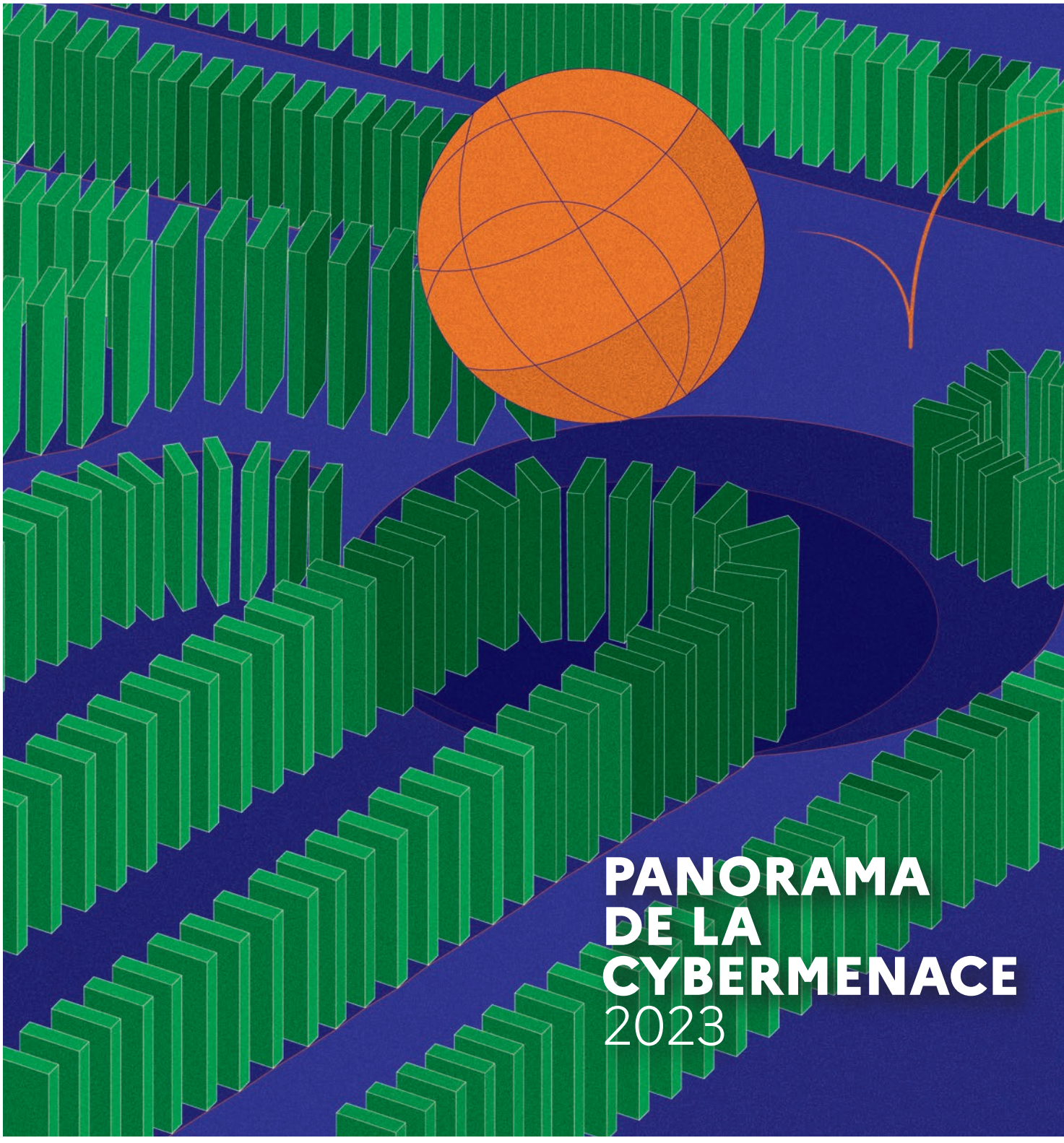
RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité



PANORAMA DE LA CYBERMENACE 2023

PANORAMA DE LA CYBERMENACE

2023

Cette troisième édition du *Panorama de la cybermenace* décrit les principales tendances constatées en 2023 par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Ce document se concentre sur les **intentions** des attaquants, leurs **capacités** et les **opportunités** exploitées pour compromettre des systèmes d'information (SI), en fournissant des exemples concrets d'incidents traités par l'ANSSI durant l'année. Le niveau de la menace informatique continue d'augmenter, dans un contexte marqué par de nouvelles tensions géopolitiques et la tenue d'événements internationaux sur le sol français. L'ANSSI estime aujourd'hui que les attaquants réputés liés à la Chine, à la Russie et à l'écosystème cybercriminel constituent les trois principales menaces tant pour les systèmes d'information français les plus critiques que pour l'écosystème national de manière systémique.

Cette année encore, l'espionnage stratégique et industriel est la menace qui a le plus mobilisé les équipes de l'ANSSI. L'agence note une augmentation significative du ciblage d'entités travaillant dans des domaines stratégiques – groupes de réflexion, instituts de recherche et base industrielle et technologique de défense (BITD) – ou qui assurent la transmission de données sensibles, comme les entreprises de télécommunications et de fourniture de services numériques (ESN). Pour ce faire, les attaquants continuent de perfectionner les techniques qui leur permettent de s'introduire sur des systèmes d'information, de s'y propager, d'exfiltrer des informations ou de se prépositionner, et d'éviter d'être détectés. En parallèle, l'ANSSI constate une augmentation du nombre d'attaques contre des téléphones portables professionnels et personnels afin d'espionner des individus ciblés. Cette tendance est notamment soutenue par la prolifération de solutions offensives commercialisées par des entreprises privées.

Les attaques informatiques à des fins d'extorsion se sont également maintenues à un niveau élevé en 2023, avec un regain du nombre d'attaques par rançongiciel contre des organisations françaises. L'écosystème cybercriminel continue de se diversifier, à la faveur de la fuite en source ouverte de codes source de rançongiciels et de la démocratisation d'outils accessibles à des acteurs aux compétences techniques limitées. La cybercriminalité représente toujours une menace importante pour le secteur public et les entités particulièrement sensibles aux interruptions de service, notamment dans les secteurs de la santé et de l'énergie. Pour lutter contre cette menace, l'ANSSI a apporté cette année son soutien à une opération internationale visant à démanteler l'infrastructure du réseau cybercriminel QakBot. Dans certains cas, les intentions lucratives des attaquants ne peuvent néanmoins pas être clairement identifiées, ce qui laisse penser que des modes opératoires cybercriminels pourraient être instrumentalisés par des acteurs étatiques pour conduire des opérations d'espionnage ou de déstabilisation.

En 2023, l'ANSSI constate un regain du nombre d'attaques destinées à promouvoir un discours politique, à entraver l'accès à des contenus en ligne ou à porter atteinte à l'image d'une organisation. En France, ces actions de déstabilisation se sont principalement matérialisées sous la forme d'attaques par déni de service distribué (DDoS) conduites par des groupes d'hacktivistes pro-russes très réactifs à l'actualité, mais dont les impacts restent limités. L'ANSSI a également eu connaissance de la compromission d'une partie du SI d'un média français qui a abouti à la divulgation d'informations exfiltrées en représailles à de précédentes publications. Dans le cadre de tensions internationales, des attaquants pourraient également être incités à s'introduire et à se maintenir sur des réseaux d'importance critique, notamment des secteurs de l'énergie, des transports et de la logistique. Si aucune opération de sabotage n'a été détectée sur le sol français, des codes destructeurs continuent d'être employés pour cibler des entités ukrainiennes. Des

activités de prépositionnement ont également été détectées contre plusieurs infrastructures critiques situées en Europe, en Amérique du Nord et en Asie.

Pour atteindre leurs objectifs, les attaquants s'appuient toujours sur de nombreuses faiblesses techniques. Parmi ces faiblesses, l'exploitation de vulnérabilités «jour-zéro»[1] et «jour-un»[2] reste une porte d'entrée de choix pour les attaquants. L'ANSSI rappelle que le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques) diffuse régulièrement sur son site des avis et des alertes de sécurité assortis de recommandations. Si certaines attaques s'avèrent particulièrement difficiles à prévenir, les attaquants profitent aussi et encore trop souvent de mauvaises pratiques d'administration, de retards dans l'application de correctifs et de l'absence de mécanismes de chiffrement. Enfin, les grands événements prévus en France en 2024, et en premier lieu les Jeux olympiques et paralympiques de Paris (JOP2024), pourraient offrir aux attaquants des opportunités supplémentaires d'agir. En vue de cet événement, l'ANSSI et l'ensemble des parties prenantes poursuivent les travaux visant à rehausser la sécurité des systèmes d'information concernés en cohérence avec la menace et à mettre en place un dispositif renforcé de détection et de réponse à incident. ←

[1] Aussi appelée «zero-day», il s'agit d'une vulnérabilité n'ayant fait l'objet d'aucune publication ni correctif de sécurité au moment de son exploitation.

[2] Aussi appelée «one-day» ou «n-day», il s'agit d'une vulnérabilité pour laquelle un correctif de sécurité est disponible, mais n'a pas été déployé par l'utilisateur, rendant l'exploitation de la vulnérabilité possible.

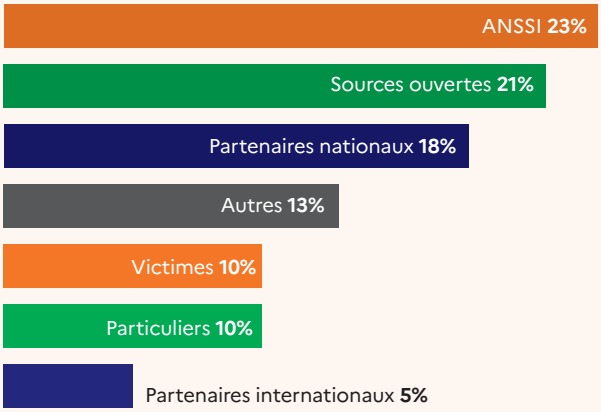
↓

Origine des événements de sécurité traités par l'ANSSI

Pour identifier les événements de sécurité affectant des entités françaises, l'ANSSI s'appuie sur de multiples sources d'informations. Ces informations proviennent avant tout de ses moyens propres (23%), qu'il s'agisse de supervision au profit des autorités publiques, de *scans*[3] ou d'investigations sur la menace. À ces capacités s'ajoute une veille réalisée en source ouverte, responsable de 21% des événements identifiés.

Parmi les événements de sécurité déclarés à l'ANSSI, 10% le sont par les victimes elles-mêmes. La gravité de ces événements tend à être nettement plus élevée que la moyenne, car ils sont souvent associés à des incidents dont les impacts sont visibles, par exemple la compromission et le chiffrement de systèmes d'information par un rançongiciel. Enfin, près de 23% des signalements reçus par l'ANSSI sont issus d'échanges avec des partenaires nationaux et internationaux, qu'ils soient privés ou institutionnels.

→ **Origine des événements de sécurité traités en 2023**



Les incidents majeurs et opérations de cyberdéfense constituent le niveau maximal d'engagement de l'agence dans le traitement d'un événement de sécurité. Ils sont réservés aux événements dont la gravité et la complexité sont significatives. Ces événements sont signalés à l'ANSSI par les victimes elles-mêmes, ou grâce au travail conjoint de l'agence et de ses partenaires nationaux et internationaux.

[3] Cf. *section 3.A.*

→ 1

ÉVOLUTION DES INTENTIONS DES ACTEURS MALVEILLANTS

A ESPIONNAGE STRATÉGIQUE ET INDUSTRIEL

→ En 2023, l'espionnage informatique est la menace qui a, à nouveau, le plus impliqué les équipes de l'ANSSI. Cette constante témoigne des moyens humains, financiers et techniques mis en œuvre par des acteurs étatiques et privés pour collecter des informations stratégiques, industrielles ou à caractère personnel sur les réseaux français. L'année a notamment été marquée par la recrudescence d'attaques réalisées au moyen de modes opératoires associés publiquement au gouvernement russe contre des organisations situées en France.

En plus des organisations publiques traditionnellement victimes d'espionnage, l'ANSSI note cette année un ciblage croissant de groupes de réflexion (*think tanks*), d'instituts de recherche et d'entreprises de la base industrielle et technologique de défense (BITD). Les attaquants visent des organisations travaillant dans des domaines stratégiques ou celles qu'ils considèrent comme proches de l'État français. Ces attaques ne se limitent pas au territoire métropolitain : en 2023, l'ANSSI a traité la compromission d'un SI situé dans un territoire ultramarin au moyen d'un mode opératoire d'attaque (MOA) associé publiquement à la Chine.

Pour mener à bien leurs campagnes, les attaquants continuent de chercher à compromettre des intermédiaires, en ciblant par exemple des sous-traitants, des prestataires ou des entreprises du secteur des télécommunications. L'ANSSI a traité en 2023 la compromission d'équipements réseau d'un opérateur, conduite au moyen d'un MOA lié à un acteur étatique, dans un but probable d'espionnage de télécommunications. D'une part, l'ANSSI a observé que des attaquants ciblent spécifiquement des protocoles d'administration faiblement sécurisés afin de compromettre des équipements réseau. D'autre part, ils profitent de l'utilisation de protocoles n'assurant pas, par défaut, le chiffrement des communications dans le but d'intercepter le trafic en clair des clients des opérateurs. Il est donc nécessaire que les opérateurs soient particulièrement attentifs à cesser l'utilisation de protocoles d'administration faibles, tandis que leurs clients ne peuvent faire l'hypothèse d'une sécurité par défaut et doivent s'assurer du chiffrement de bout en bout de leurs communications transitant, même partiellement, *via* des protocoles non sécurisés [1].

Les attaquants stratégiques visent généralement la furtivité[4] afin de pouvoir mener leurs campagnes d'espionnage ou de prépositionnement[5]. Les détecter nécessite donc une excellente coordination entre les services de l'État travaillant sur cette menace. Dans cette optique, l'État français a mis en place le Centre de coordination des crises cyber (C4) et sa déclinaison opérationnelle, appelée C4 TechOps [2]. Cette instance interministérielle, pilotée par l'ANSSI, assure l'échange d'analyses sur la menace informatique entre les experts de l'agence, de la Direction générale de la sécurité intérieure (DGSI), de la Direction générale de la sécurité extérieure (DGSE), du Commandement

[4] Cf. *section 2.A.*

[5] Cf. *section 1.C.*

de la cyberdéfense (COMCYBER) et de la Direction générale de l'armement (DGA) dans le respect des prérogatives de chaque entité [3]. Elle contribue donc directement à l'amélioration des capacités de détection, d'anticipation et d'imputation des incidents. L'ANSSI reçoit régulièrement à travers cette instance des signalements de potentielles victimes situées en France.

Si l'attention des acteurs malveillants se porte généralement sur la compromission de réseaux d'organisations, les attaquants ciblent néanmoins de plus en plus d'équipements appartenant à des individus, notamment des téléphones portables[6]. Ces actions sont principalement dirigées contre des personnalités et hauts dirigeants, mais aussi contre des équipes de cybersécurité. En 2023, des attaquants réputés liés à la Corée du Nord ont ciblé une nouvelle fois des chercheurs en sécurité informatique avec des techniques d'ingénierie sociale particulièrement avancées [4], possiblement pour collecter des informations et des outils pouvant être réutilisés dans des attaques futures.

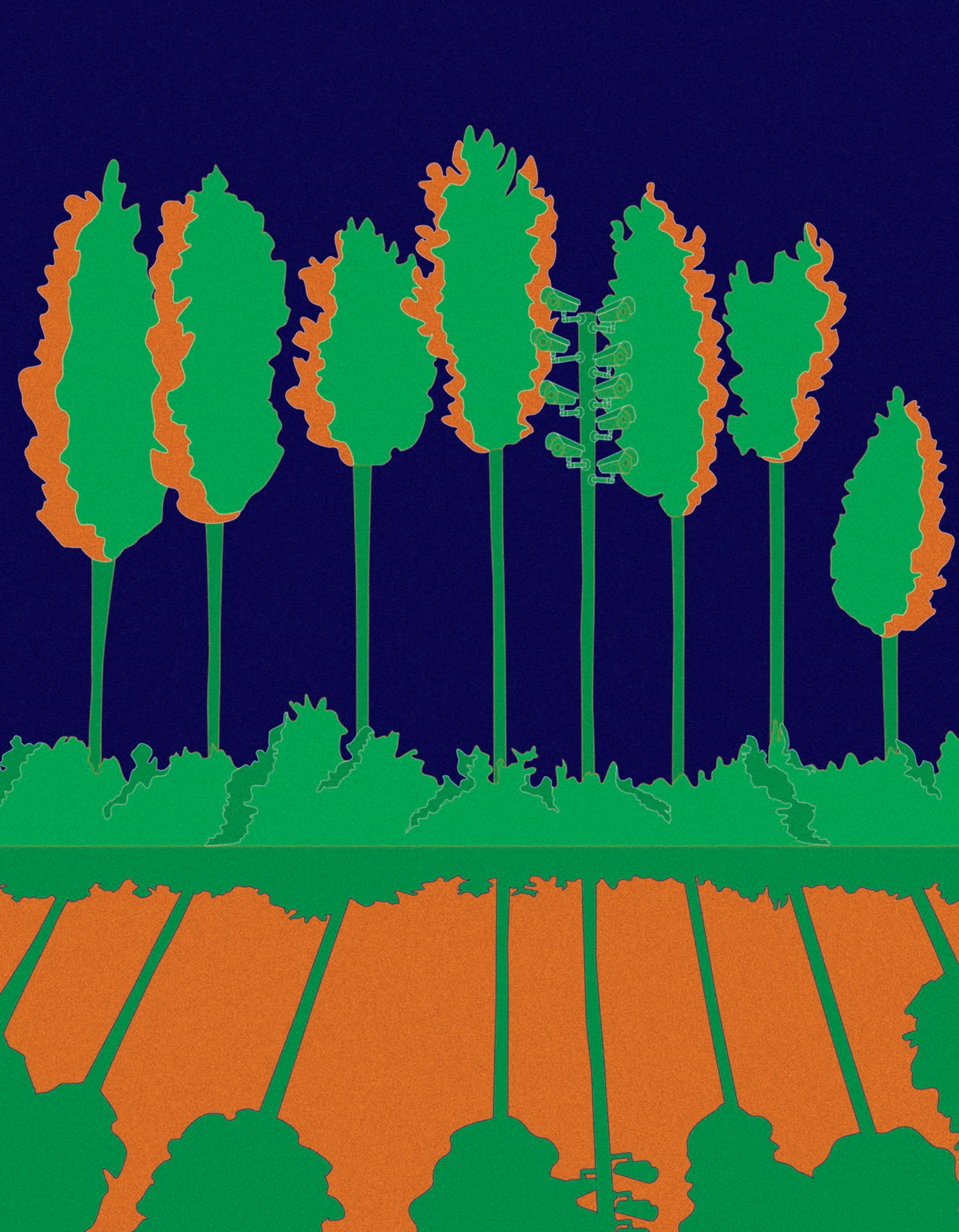
En 2023, comme les années précédentes, l'agence a traité des incidents impliquant la présence de plusieurs groupes d'attaquants sur le réseau d'une même victime (polycompromission), ainsi que le retour d'attaquants expulsés seulement quelques mois auparavant (recompromission). Ces incidents attestent de la persévérance de certains acteurs, qui continueront très probablement de cibler des entités françaises représentant un fort intérêt en termes de renseignement. Bien que leurs impacts restent difficiles à mesurer, il convient de souligner que ces campagnes pérennes et discrètes visent à recueillir des informations stratégiques ayant des conséquences importantes sur le long terme. L'ANSSI rappelle l'importance des actions de remédiation et du maintien des efforts de reconstruction et de durcissement durable des infrastructures après le traitement d'un incident. ←

[6] Cf. *section 2.C.*

Les capacités légales de détection et d'anticipation de l'ANSSI

Pour les seules menaces susceptibles de porter atteinte aux opérateurs critiques ou à la défense ou la sécurité nationale, l'ANSSI dispose de dispositifs légaux lui permettant d'améliorer la connaissance sur la menace, de détecter des victimes, voire d'entraver des activités malveillantes. La loi de programmation militaire (LPM) 2024-2030 a renforcé récemment les dispositions normatives relatives à la sécurité informatique, en modifiant le code des postes et des communications électroniques (CPCE) et le code de la défense.

Ainsi, l'article L33-14 alinéa 2 du CPCE permet à l'ANSSI de fournir des marqueurs techniques à certains opérateurs de communications électroniques (OCE) à des fins de détection de victimes potentielles parmi leurs clients. L'article L2321-2-1 du code de la défense permet quant à lui à l'agence de recueillir des données réseau ou système sur des équipements contrôlés par des attaquants auprès des OCE, des hébergeurs et des opérateurs de centre de données. Enfin, l'article L2321-2-3 du code de la défense donne à l'ANSSI la possibilité de prescrire des mesures de blocage ou de redirection de noms de domaine aux fournisseurs de résolveurs DNS, aux bureaux d'enregistrement et à l'office d'enregistrement. L'usage de ces dispositifs légaux est strictement encadré et sous le contrôle de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP).

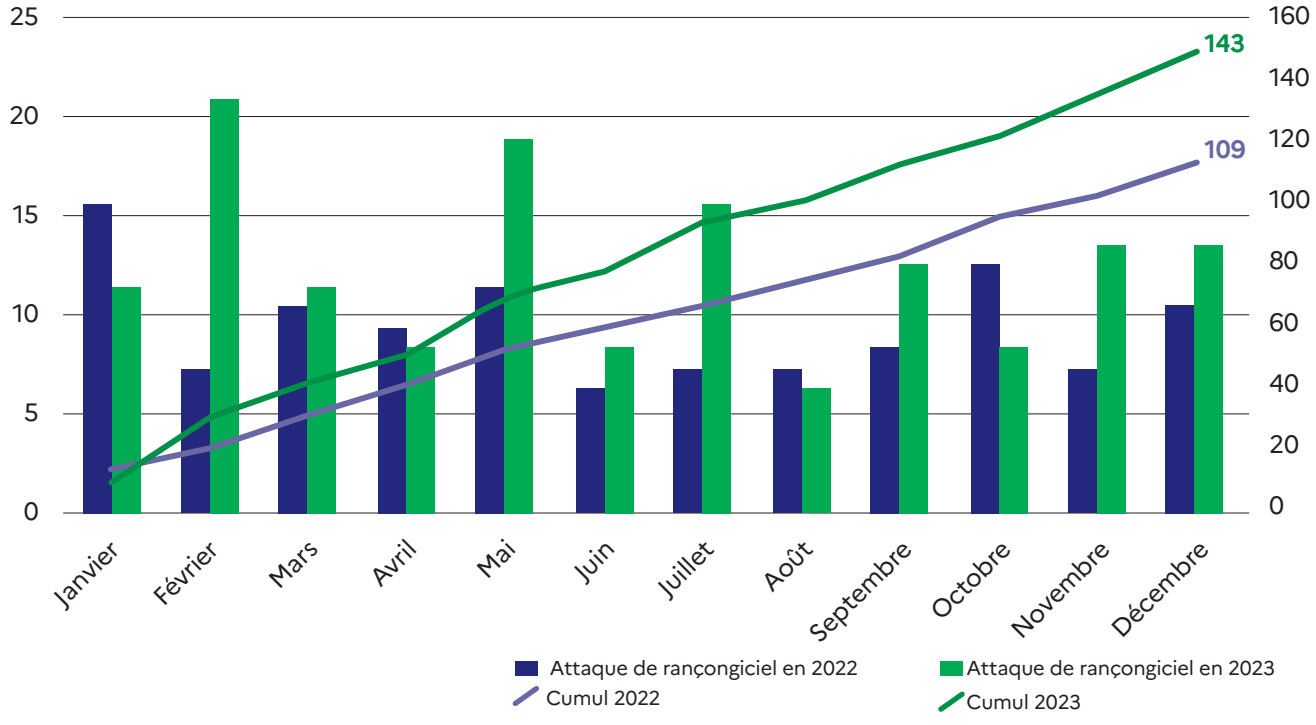


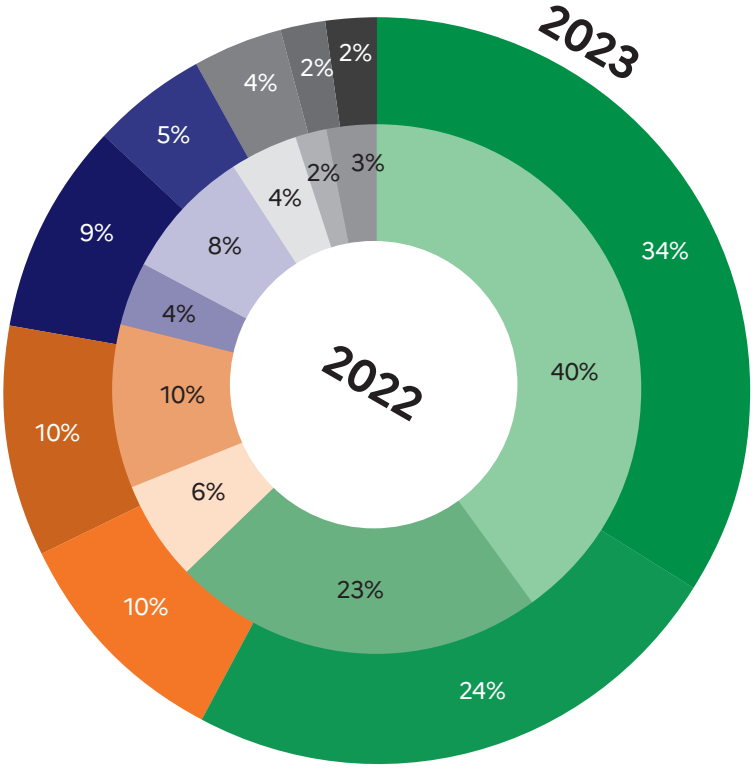
B **ATTAQUES À BUT LUCRATIF**

→ Les attaques à finalité lucrative se sont maintenues à un niveau élevé en 2023. Le nombre total d'attaques par rançongiciel portées à la connaissance de l'ANSSI est supérieur de 30% à celui constaté sur la même période en 2022. Cette recrudescence, également constatée par la section de lutte contre la cybercriminalité du parquet de Paris [5], rompt avec la diminution du nombre d'attaques par rançongiciel observée par l'agence dans son précédent Panorama de la cybermenace [6]. Cette tendance se limite toutefois aux incidents signalés à l'ANSSI ou ayant fait l'objet d'un dépôt de plainte, et ne constitue pas une vision exhaustive.

L'augmentation des attaques s'est ressentie sur l'ensemble des typologies d'entités, et les trois catégories les plus ciblées restent identiques depuis 2020 [7]. L'ANSSI constate une hausse du nombre d'incidents affectant certains secteurs, dont les associations et les collectivités territoriales et

→ Comparaison des signalements d'attaques par rançongiciel en 2022 et 2023



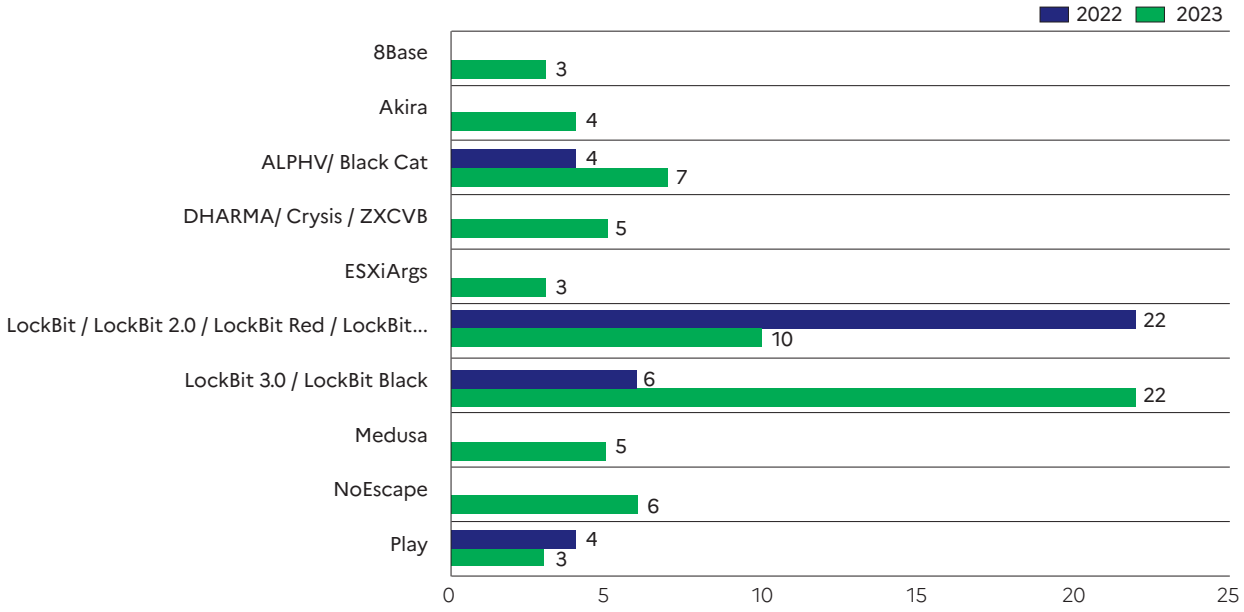


→ Répartition des victimes d'attaque par rançongiciel

- TPE/PME/ETI
- Collectivité territoriale/locale
- Entreprise stratégique
- Établissement de santé
- Association
- Établissement d'enseignement supérieur
- EPA, EPIC
- Ministère
- Autre

locales, qui ont représenté respectivement 9% et 24% des victimes d'attaque par rançongiciel en 2023. Par ailleurs, les principales souches employées pour conduire ces attaques ont connu des évolutions en 2023. L'émergence de nouvelles souches est notamment expliquée par le changement d'identité d'anciens groupes d'attaquants et par de nouveaux acteurs apparus ou s'étant réorganisés au cours de l'année (cf. *section 2.B*). L'activité importante des affiliés du rançongiciel LockBit, déjà constatée en 2022, s'est poursuivie en 2023.

→ Comparatif des principales souches de rançongiciel utilisées dans des incidents signalés à l'ANSSI en 2022 et 2023



Avertissement: le graphique ci-dessus n'inclut que les souches qui ont pu être identifiées avec certitude, et à au moins trois reprises, lors des incidents traités par l'ANSSI ou un prestataire d'investigation numérique.

Dans certains cas, il demeure difficile d'identifier avec certitude les intentions réelles des attaquants, qui peuvent se servir de méthodes et d'outils issus de l'écosystème cybercriminel pour camoufler des intentions d'espionnage ou de déstabilisation. Le rapprochement de l'outillage et des objectifs des attaquants étatiques et cybercriminels, déjà observé l'an passé, s'est accéléré depuis le début de l'invasion de l'Ukraine par la Russie (voir focus ci-contre). Il représente aujourd'hui une menace pour les entités publiques et certains secteurs critiques, ainsi qu'un défi pour les équipes de sécurité informatique.

Les acteurs malveillants n'ont pas forcément besoin d'un haut niveau de sophistication pour cibler des entités de secteurs encore trop vulnérables, comme la santé et les collectivités territoriales. Les attaques informatiques à but lucratif peuvent néanmoins avoir des impacts très importants pour la réputation et la continuité d'activité de ces structures. Pour rappel, l'ANSSI propose aux opérateurs régulés ainsi qu'à la sphère publique des services d'audit automatisé de leur système d'information. Le service *Active Directory Security*[7] (ADS) permet notamment de les accompagner dans la sécurisation des annuaires *Active Directory*, tandis que le service SILENE permet d'évaluer leur niveau d'exposition sur Internet [8]. ←

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

Le code malveillant RomCom

La porte dérobée RomCom serait utilisée à des fins lucratives depuis au moins 2022 par le groupe cybercriminel Tropical Scorpius. Ce groupe opèrerait par ailleurs le rançongiciel Cuba depuis fin 2019 [9]. Il est notamment connu pour avoir revendiqué la compromission du SI du gouvernement monténégrin en août 2022 [10]. D'octobre 2022 à juillet 2023, RomCom a été employé dans des attaques dont la victimologie laisse penser qu'elles ont été conduites à des fins d'espionnage dans le contexte de l'invasion de l'Ukraine par la Russie. De nombreuses entités ukrainiennes, européennes et américaines appartenant à des secteurs critiques publics et privés auraient été ciblées. Ces opérations d'espionnage empruntaient des tactiques, techniques et procédures (TTP) habituellement associées aux attaques cybercriminelles [11, 12].

Fin juin 2023, en amont du Sommet de l'OTAN de Vilnius, des attaques à des fins d'espionnage auraient été conduites contre des pays de l'Alliance. Les opérateurs auraient tenté de distribuer une variante de RomCom en exploitant une vulnérabilité jour-zéro[8] affectant Microsoft Office [13]. Simultanément, une attaque distribuant des codes malveillants similaires aurait ciblé une entité pour y déployer un rançongiciel à des fins lucratives, sans toutefois exploiter la même vulnérabilité. À ce stade, l'ANSSI ne peut pas affirmer qu'il s'agit d'un même groupe d'attaquants, ou au contraire de plusieurs groupes distincts. Cela illustre cependant un potentiel emploi de capacités offensives cybercriminelles au profit des intérêts stratégiques russes.

[8] CVE-2023-36684.

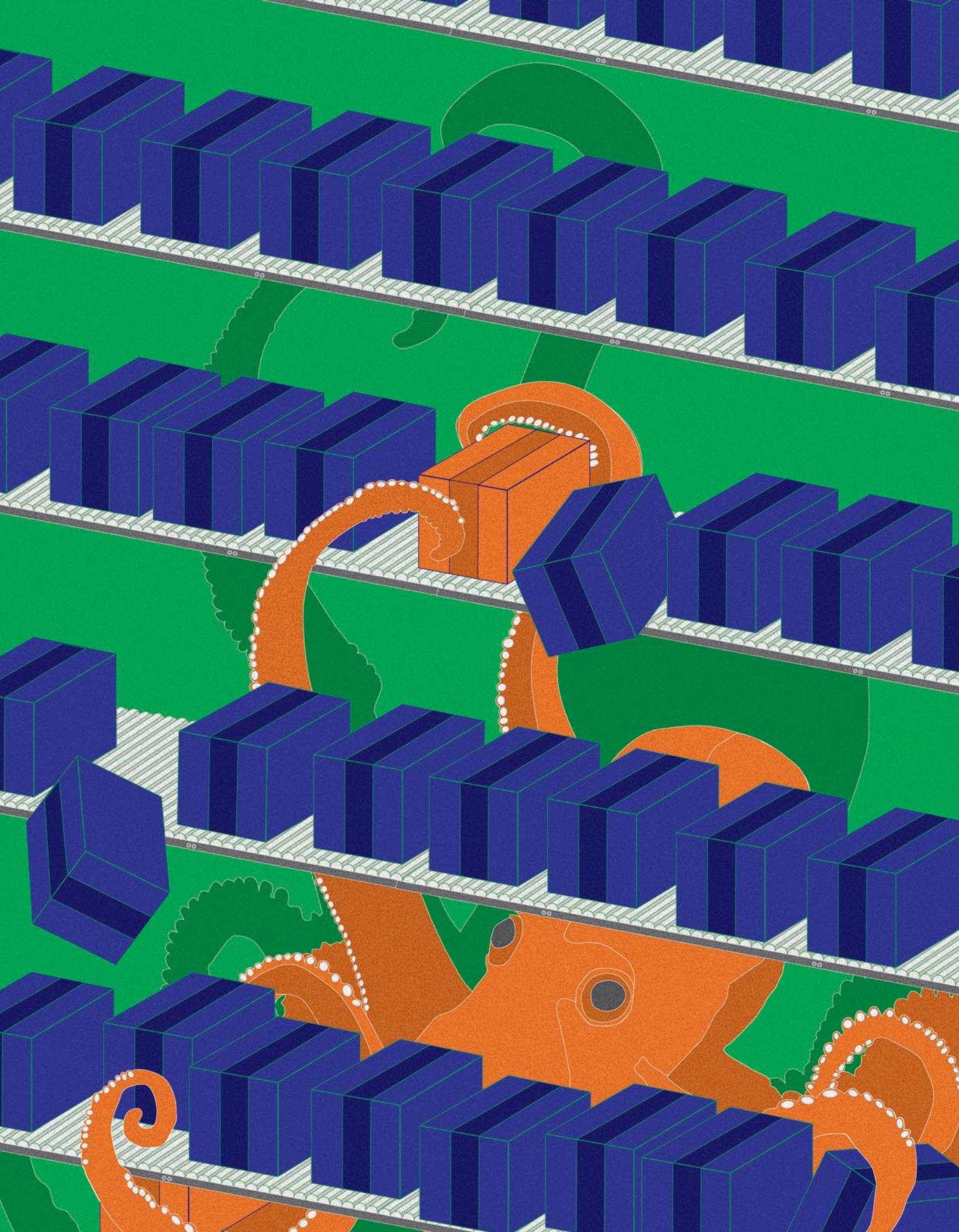
C OPÉRATIONS DE DÉSTABILISATION

→ Dans un contexte géopolitique tendu, la menace de déstabilisation a connu cette année un regain d'activité. L'ANSSI a constaté de nouvelles opérations de déstabilisation prenant la forme d'attaques par DDoS [14], de défigurations de sites Internet, de divulgations de données et de sabotage. Les opérations les plus visibles restent les attaques par DDoS [15], conduites notamment par des groupes d'hacktivistes pro-russes[9] très réactifs à l'actualité [16]. En août 2023, le groupe Anonymous Sudan a ainsi menacé la France de représailles en cas d'intervention contre le putsch au Niger [17], avant de réorienter son ciblage contre des entités israéliennes suite à l'offensive militaire dans la bande de Gaza [18].

Si les impacts des attaques par DDoS sont souvent limités, les attaquants exploitent désormais de nouvelles techniques pour contourner les dispositifs de protection existants. En septembre 2023, le groupe pro-russe NoName057(16) a revendiqué des attaques par DDoS contre les sites d'une quinzaine de CSIRT[10] européens, dont celui du CERT-FR, porté au sein de l'ANSSI.

[9] Dont Killnet, Xaknet, Bloodnet, CyberArmyofRussia_Reborn et Solntsepyok. Certains de ces groupes sont soupçonnés publiquement d'être instrumentalisés par les services de renseignement russes.

[10] *Computer Security Incident Response Team.*



La campagne a été conduite *via* le programme DDoSia, développé par le groupe [19], et ciblait spécifiquement la couche applicative des services ciblés[11], souvent non couverte par les solutions anti-DDoS. Plusieurs attaques ont été observées durant cinq jours et ont engendré une indisponibilité du site du CERT-FR durant trois heures, avant qu'un répartiteur de charge dédié ne soit déployé.

Outre les attaques par DDoS, l'ANSSI a eu connaissance de campagnes de déstabilisation reposant sur l'intrusion dans un système d'information, puis son sabotage ou la publication d'informations exfiltrées (voir focus ci-contre). Bien qu'aucune action de sabotage n'ait été observée contre des organisations en France, ce type d'attaque a été employé une nouvelle fois contre des médias [20], des entités gouvernementales [21] et des entreprises ukrainiennes de télécommunications [22, 23] en 2023. Certaines de ces opérations pourraient avoir été coordonnées avec des actions cinétiques menées par l'armée russe en Ukraine [24].

Il convient enfin de rappeler que l'évolution du contexte géopolitique pourrait encourager des acteurs malveillants à s'introduire et à se maintenir sur des réseaux critiques européens, potentiellement en vue de conduire des opérations ultérieures de sabotage. Cette année, des activités potentielles de prépositionnement ont été détectées sur les systèmes d'information et opérationnels d'entités du secteur de l'énergie en Europe, en Amérique du Nord et en Asie [25, 26]. Les secteurs de l'énergie, des transports, de la logistique et des télécommunications sont toujours considérés comme particulièrement exposés à cette menace. ←

[11] Correspondant à la couche 7 du modèle *Open Systems Interconnection* (OSI). Le code malveillant DDoSia effectue des requêtes HTTP.

Ciblage de *Charlie Hebdo*

En décembre 2022, l'hebdomadaire satirique français *Charlie Hebdo* a lancé un concours international de caricatures du guide suprême iranien. Ce concours était réalisé en soutien au mouvement de contestation déclenché par la mort en détention de Mahsa Amini, une Kurde iranienne arrêtée pour avoir enfreint le code vestimentaire du pays. Le 4 janvier 2023, *Charlie Hebdo* a publié ces caricatures dans un numéro spécial [27]. Le même jour, sa boutique en ligne a subi une défiguration et une exfiltration d'informations de la base de données clients. Les deux incidents ont été revendiqués par un acteur malveillant se présentant sous l'avatar « Holy Souls ». Cet avatar a ensuite mis en vente sur plusieurs forums cybercriminels les informations exfiltrées, qui rassemblaient les données à caractère personnel de 230 000 clients du journal [28].

D'après les autorités américaines, Holy Souls serait opéré par une société-écran nommée Emennet Pasargad ou Iliyanet [29], qui mènerait des actions d'influence et d'ingérence au service du Corps des Gardiens de la Révolution islamique et du ministère du Renseignement iranien [30]. La publication de caricatures avait déjà exposé le journal *Charlie Hebdo* à des projets d'attaques informatiques : en juin 2021, le groupe d'hacktivistes Lab Dookhtegan, qui se présente comme dissident, avait révélé sur son canal Telegram l'existence d'un plan conçu par Emennet Pasargad en 2020 pour déstabiliser le journal [31]. À l'instar de l'incident du mois de janvier 2023, ce projet aurait été mené dans une logique de représailles et d'intimidation contre *Charlie Hebdo*.

→ 2

AMÉLIORATION DES CAPACITÉS OFFENSIVES

A UNE RECHERCHE CONSTANTE DE FURTIVITÉ

Les acteurs malveillants perfectionnent constamment leurs techniques afin de réduire le risque de détection, de caractérisation et d'attribution de leurs activités. Ces évolutions concernent à la fois les infrastructures qu'ils utilisent, les méthodes d'intrusion initiale, les mécanismes de persistance et les outils employés pour conduire l'attaque.

Les attaquants s'appuient aujourd'hui sur des réseaux d'anonymisation de plus en plus complexes, qu'ils constituent en compromettant par exemple des équipements périphériques ou mutualisés (voir focus ci-contre). La recherche de furtivité se traduit également par l'emploi de capacités d'interception discrètes : cette année, l'ANSSI a traité des incidents impliquant l'emploi probable de capacités de renseignement d'origine électromagnétique (ROEM). Ces dernières auraient servi à intercepter des secrets d'authentification transitant en clair pour se connecter au réseau de la victime.

Les réseaux d'anonymisation

Un réseau d'anonymisation est un réseau de machines compromises communiquant entre elles, utilisées par un groupe d'attaquants afin de rendre ses opérations plus furtives. Ces réseaux sont utilisés aussi bien pour des actions de reconnaissance que de commande et de contrôle (C2). Un même réseau d'anonymisation est souvent exploité par de multiples acteurs, ce qui rend plus difficile la distinction et la caractérisation de ses opérateurs. Si les réseaux d'anonymisation ne sont pas spécifiques aux modes opératoires réputés chinois, des MOA comme APT31 et Ke3chang se distinguent par leur utilisation de plus en plus fréquente et à large échelle de ce dispositif [32, 33].

Pour constituer ces réseaux, les attaquants compromettent généralement des routeurs domestiques[12], des objets connectés ou d'autres équipements périphériques exposés sur Internet avec des codes malveillants spécifiques. La sécurité souvent défaillante de ces équipements facilite leur compromission. En effet :

- les opérations de maintien en condition de sécurité (MCS) sur ces équipements sont trop rares, notamment pour appliquer les mises à jour constructeur ;
- ils font rarement l'objet d'une supervision, ce qui complique la détection de la présence d'attaquants ;
- les interfaces d'administration sont trop souvent exposées sur Internet et leurs mots de passe par défaut sont rarement modifiés.

L'ANSSI constate depuis plusieurs années que des routeurs de particuliers, de petites et moyennes entreprises (PME) et de collectivités territoriales sont compromis, puis intégrés à ces réseaux d'anonymisation [34]. Leur sécurité est un enjeu collectif, puisqu'ils deviennent à leur insu des relais actifs de campagnes d'espionnage et cybercriminelles. Le futur règlement européen sur la cyberrésilience (CRA[13]) contribuera à sécuriser ce type de matériel pouvant entrer dans la composition des réseaux d'anonymisation [35, 36].

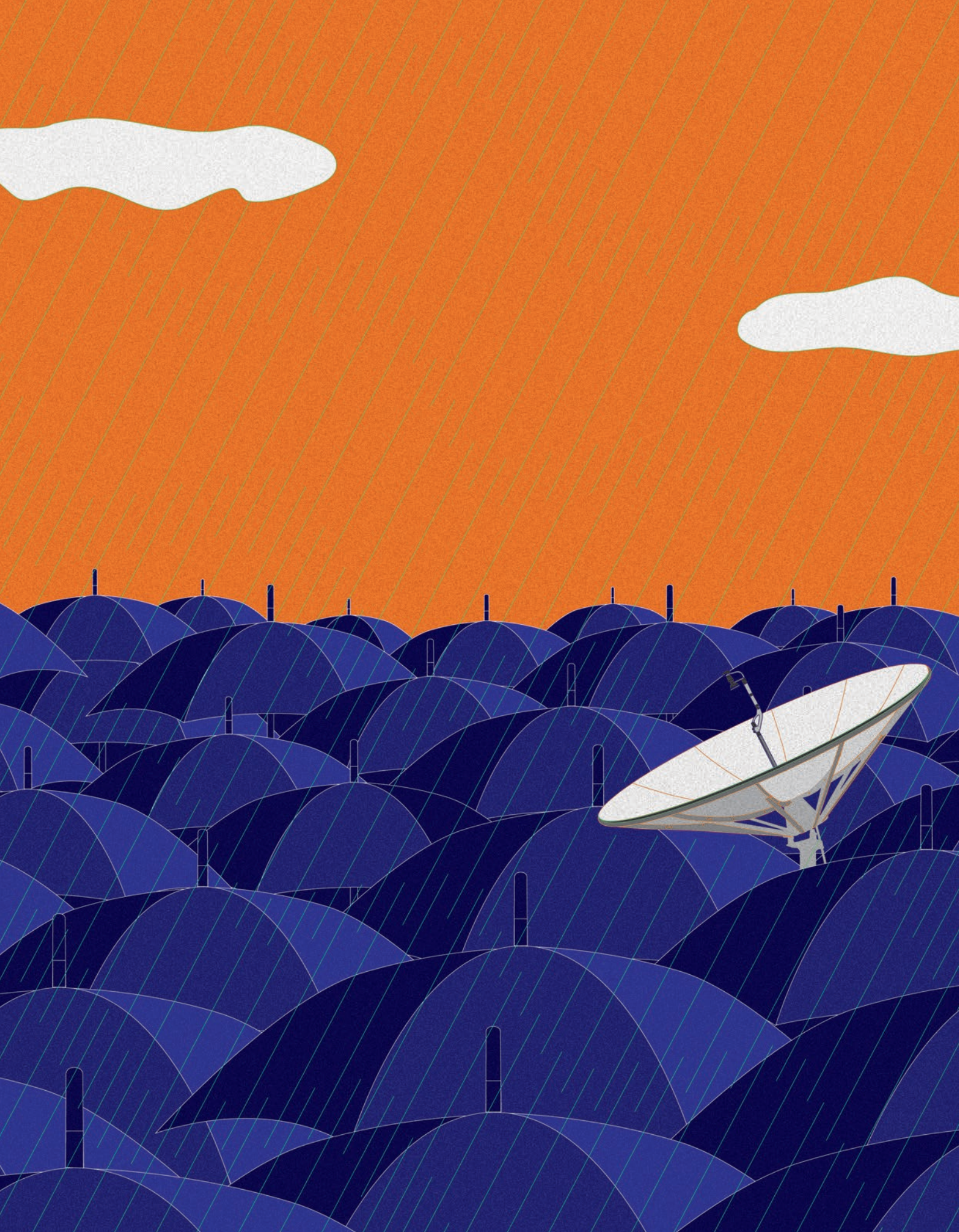
[12] Généralement appelés SOHO *(Small Office/Home Office)*.

[13] *Cyber Resilience Act*.

Après l'intrusion initiale, les attaquants accordent un soin particulier à leur furtivité sur le réseau compromis. En 2023, l'ANSSI a traité de nouveaux incidents impliquant des mécanismes de persistance sur des équipements périphériques (routeurs, passerelles de messagerie, pare-feux, etc.). Durant l'un de ces incidents, les attaquants ont ciblé un équipement de bordure non administré par la victime, réduisant ainsi fortement le risque de détection par cette dernière. Aucun code malveillant n'était déployé, les attaquants se contentant de mettre en place des filtres de redirection pour exfiltrer les courriels d'intérêt [37].

En matière d'outillage, l'ANSSI remarque un recours croissant aux techniques dites de *living-off-the-land*, qui consistent à exploiter des applications et des fonctionnalités déjà présentes sur le réseau compromis[14] plutôt que des outils spécifiques déployés par l'attaquant, afin d'éviter la levée d'alertes. Ainsi, les investigations sont rendues plus complexes par la confusion entre les activités de l'attaquant et celles des utilisateurs légitimes. Cette stratégie aurait notamment été employée par des attaquants réputés russes et chinois pour cibler des infrastructures critiques en Ukraine [24] et aux États-Unis en 2023 [38, 39]. Enfin, les attaquants tirent toujours parti de codes partagés, ce qui complexifie le suivi et l'attribution de leurs activités. Le code ShadowPad, employé depuis 2019 par différents groupes liés publiquement à la Chine [40, 41], aurait ainsi servi cette année à compromettre le réseau électrique d'un pays asiatique [42]. L'ANSSI a également observé l'utilisation de ce code malveillant dans un incident affectant une entité à portée internationale située en France. ←

[14] Par exemple des outils d'administration système légitimes.



B **DIVERSIFICATION DE L'ÉCOSYSTÈME ET DES MÉTHODES CYBERCRIMINELLES**

→ Plusieurs facteurs contribuent à la diversification des profils cybercriminels déjà observée depuis plusieurs années. La fuite de générateurs et de codes sources de rançongiciels comme LockBit, Babuk ainsi que Conti en 2021 et 2022 continue de favoriser l'émergence de groupes et d'acteurs moins expérimentés qui génèrent puis déploient leurs propres rançongiciels [43, 44]. Cette tendance est encore renforcée par la démocratisation des outils de vol d'informations (*infostealers*), notamment distribués sur des forums et au sein de groupes privés. Leur emploi croissant a facilité l'acquisition d'accès initiaux par des cybercriminels aux compétences techniques limitées [45, 46].

L'ANSSI constate par ailleurs que les attaquants s'appuient parfois sur des guides d'intrusion vendus ou diffusés sur des forums cybercriminels. Ces manuels détaillent les techniques d'attaques à mettre en œuvre pour s'introduire sur un système d'information, récolter des identifiants et élever ses privilèges [47, 48], notamment en vue de conduire des attaques par rançongiciel. En parallèle, l'ANSSI constate que la fin des activités de Conti, amorcée en mars 2022, puis le démantèlement de QakBot en août 2023, ont entraîné un éclatement et une réorganisation des activités de certains groupes et affiliés [49].

Les méthodes employées par les acteurs cybercriminels ont également connu des évolutions notables. La tendance au rançonnage reposant exclusivement sur l'exfiltration de données (sans déploiement de rançongiciel), observée depuis 2021 [7], s'est confirmée en 2023 dans le cadre de campagnes massives [50, 51]. Cette évolution entraîne des complications dans la gestion des quantités de données exfiltrées, que les groupes cybercriminels essaient de contourner en distribuant les données sur plusieurs machines *via* un protocole de transfert de données pair à pair (P2P) comme BitTorrent, ou en obligeant les individus qui souhaitent obtenir les données à entrer en contact avec les attaquants [52]. Dans le même temps, l'exploitation de plusieurs vulnérabilités jour-zéro ou jour-un par le groupe cybercriminel CL0P[15] illustre la capacité de groupes cybercriminels matures à conduire des attaques à grande échelle en ciblant des logiciels d'entreprises susceptibles d'héberger des données sensibles [53, 54]. ←

[15] Dont des vulnérabilités dans des solutions GoAnywhere MFT, Papercut, MoveIT (cf. *section 3.B*) ou encore SysAID.

Démantèlement de l'infrastructure du réseau QakBot

Le 26 août 2023, une opération internationale impliquant les autorités policières et judiciaires des États-Unis, de l'Allemagne, des Pays-Bas et de la France a permis le démantèlement de l'infrastructure de commande et de contrôle du réseau malveillant QakBot [55]. La section de lutte contre la cybercriminalité de la Juridiction nationale de lutte contre la criminalité organisée (JUNALCO) du parquet de Paris a supervisé la partie française. Actif depuis 2008, QakBot est un programme malveillant qui était principalement utilisé pour déployer des codes malveillants tiers comme des outils génériques offensifs (Cobalt Strike) et des rançongiciels (Royal, BlackBasta) sur les réseaux des victimes. Les machines infectées pouvaient être connectées entre elles sous la forme d'un réseau de machines zombies, appelé botnet.

L'ANSSI a apporté son soutien à ce démantèlement en participant à l'identification et à la notification des victimes françaises. Bien que de nouveaux implants QakBot aient été découverts en décembre 2023, les utilisateurs du botnet ont été contraints de cesser leurs activités ou de chercher des alternatives sur le marché, en investissant potentiellement dans de nouveaux codes malveillants [56, 57]. Les actions de démantèlement ont donc des conséquences directes sur le niveau de la menace, car elles perturbent significativement les activités cybercriminelles et obligent ses acteurs à se réorganiser.

Compromission d'un Centre hospitalier universitaire par le groupe BianLian

Le 21 juin 2023, le Centre hospitalier universitaire (CHU) de Rennes a détecté des actions malveillantes sur son système d'information et en a informé l'ANSSI, qui a déployé des agents sur site pour accompagner les équipes du CHU. Les investigations réalisées ont permis de mettre en évidence une compromission en profondeur du SI ainsi qu'une exfiltration de données effectuée par le groupe cybercriminel BianLian.

Suite à la compromission, le centre hospitalier a mis en place des mesures d'endiguement incluant notamment une coupure des accès à Internet, rouverts progressivement durant les mois suivants. Si l'ensemble des activités médicales réalisées par l'hôpital a été préservé, les conséquences de l'attaque ont été significatives sur l'organisation de la structure et les missions quotidiennes du personnel soignant. Cet incident illustre les impacts engendrés par la compromission du système d'information d'un hôpital, même en l'absence d'actions de chiffrement. Ce type d'incident nécessite un fort engagement et de coûteux travaux de reconstruction et de sécurisation sur le long terme. La réactivité des équipes a toutefois permis d'éviter des conséquences plus lourdes, l'attaque ayant été détectée dans sa phase initiale.

C CIBLAGE CROISSANT DE PÉRIPHÉRIQUES MOBILES À DES FINS D'ESPIONNAGE

→ L'ANSSI constate une augmentation du nombre d'incidents impliquant la compromission de téléphones portables professionnels et personnels. Le ciblage de périphériques mobiles peut requérir des moyens importants, notamment pour identifier et exploiter des vulnérabilités sur des téléphones dans des versions logicielles récentes sans action nécessaire de la cible[16]. Si ces capacités sont historiquement développées par des États possédant des capacités offensives avancées, l'essor du marché privé de la surveillance se confirme : certaines entreprises fournissent des codes malveillants très perfectionnés à des acteurs publics, mais également à des entreprises et à des particuliers aux intentions malveillantes. La prolifération d'outils offensifs commerciaux contribue de manière significative à l'augmentation générale du niveau de menace.

Cette année, de nouvelles informations ont été rendues publiques sur des codes malveillants ciblant spécifiquement des périphériques mobiles, dont BlastPass [58], Triangulation [59], Reign [60, 61] et Predator [62, 63]. Certaines de ces publications ont poussé des acteurs à cesser leurs activités, comme l'entreprise Quadream à l'origine de Reign [64]. L'écosystème continue toutefois de se réorganiser.

Ce type de capacité est employé pour cibler des cadres dirigeants d'administrations ou d'entreprises de secteurs stratégiques, mais aussi pour surveiller des opposants, des journalistes ou des défenseurs des droits humains présents sur le territoire du commanditaire ou à l'étranger [62]. Des codes malveillants ciblant des téléphones sont également déployés dans le cadre de conflits armés, à l'image d'Infamous Chisel, un code lié publiquement au mode opératoire réputé russe Sandworm, qui ciblait des périphériques Android de l'armée ukrainienne [65, 66]. Le code Pegasus, développé par la société israélienne NSO Group, serait quant à lui employé par des acteurs azerbaïdjanais pour espionner des personnalités en Arménie depuis 2022 [67, 68].

En 2023, la France a soutenu la Déclaration conjointe sur les efforts pour lutter contre la prolifération et l'utilisation abusive de logiciels espions commerciaux, adoptée dans le cadre de la 2e édition du Sommet pour la démocratie [69]. Avec le Royaume-Uni, la France est également à l'initiative de consultations pour lutter contre la prolifération d'outils offensifs commerciaux, lancées lors du Forum de Paris pour la paix, en novembre 2023 [70]. ←

[16] Communément appelées vulnérabilités « zéro-clic ».

→ 3

OPPORTUNITÉS SAISIES PAR LES ATTAQUANTS

A **DE NOMBREUSES FAIBLESSES EXPLOITÉES**

→ Pour compromettre un système d'information, les attaquants peuvent compter sur de nombreuses faiblesses, techniques comme humaines : exposition d'équipements non sécurisés sur Internet, erreurs de configuration, mauvaises pratiques d'administration ou de gestion des droits et des secrets, hameçonnage, absence de durcissement, vulnérabilités jour-zéro ou jour-un, etc. Parmi ces faiblesses, l'exploitation de vulnérabilités constitue encore aujourd'hui une porte d'entrée de choix dans nombre de systèmes. Grâce à un outillage toujours plus performant et automatisé de reconnaissance et d'exploitation, les attaquants peuvent par exemple conduire des activités d'énumération (*scan*) et obtenir de manière opportuniste des accès pour une compromission ultérieure du système d'information.

L'utilisation par les éditeurs de composants logiciels édités par des tiers reste également un sujet de préoccupation important. Qu'il s'agisse de bibliothèques largement utilisées comme log4j[17], jackson-databind[18] ou de solutions intégrées comme les systèmes d'exploitation temps-réel[19], il est très difficile de s'assurer que l'ensemble des produits qui ont recours à ces composants fera l'objet d'une mise à jour de sécurité dans un temps raisonnable, et les efforts consacrés par les CSIRT nationaux pour établir cette cartographie sont considérables.

Il convient de noter que les vulnérabilités qui affectent un tel composant ne seront pas exploitables dans tous les cas, en fonction de la manière dont le composant est utilisé au sein de chaque

[17] CVE-2021-44228 aussi dénommée Log4shell [71].

[18] CVE-2020-24616 [72], etc.

[19] CVE-2021-22156 affectant QNX, édité par BlackBerry [73].

Les activités de *scan* et de campagne d'alertes de vulnérabilité du CERT-FR

Le CERT-FR effectue une veille sur les vulnérabilités. Dans ce cadre, il qualifie la gravité des nouvelles vulnérabilités connues en fonction de leur exploitabilité, de la prévalence des produits affectés et de leur exposition sur Internet. Cette approche permet d'engager des actions de *scan* préventives afin de déterminer les entités susceptibles d'être ciblées par les attaquants. Les *scans* réalisés par le CERT-FR ont pour objectif d'identifier et de notifier les entités exposées afin qu'elles se protègent ou entament des recherches d'une éventuelle compromission [8]. En complément de cette démarche d'identification des entités, qui peut prendre du temps, d'autres leviers sont mis en œuvre. Le CERT-FR adresse notamment des communications vers ses bénéficiaires les enjoignant à prendre les mesures qui s'imposent en fonction de leur exposition à une attaque, et effectue des signalements par l'intermédiaire des opérateurs de télécommunications, conformément à l'article L33-14 alinéa 5 du CPCE.

L'exemple des actions menées suite à la découverte de la vulnérabilité ProxyLogon (CVE-2021-26855) illustre cette démarche. Le 3 mars 2021, au lendemain de la publication de l'éditeur, une alerte a été émise sur le site du CERT-FR [74]. Une campagne de signalements a été menée dès le 5 mars. Toutefois, les données du scan réalisé le 9 mars indiquaient qu'environ 70% des serveurs identifiés n'étaient pas dans une version permettant leur mise à jour avec les correctifs de sécurité proposés par Microsoft. Beaucoup d'entités ont donc eu à appliquer la dernière mise à jour cumulative avant de pouvoir appliquer les correctifs. Le CERT-FR a réitéré plusieurs communications afin d'inciter les entités à appliquer les correctifs de sécurité. Cependant, en juin 2021, 5% des serveurs observés demeuraient vulnérables. Bien que complexe, le maintien à jour des services est primordial pour l'application rapide de correctifs de sécurité.

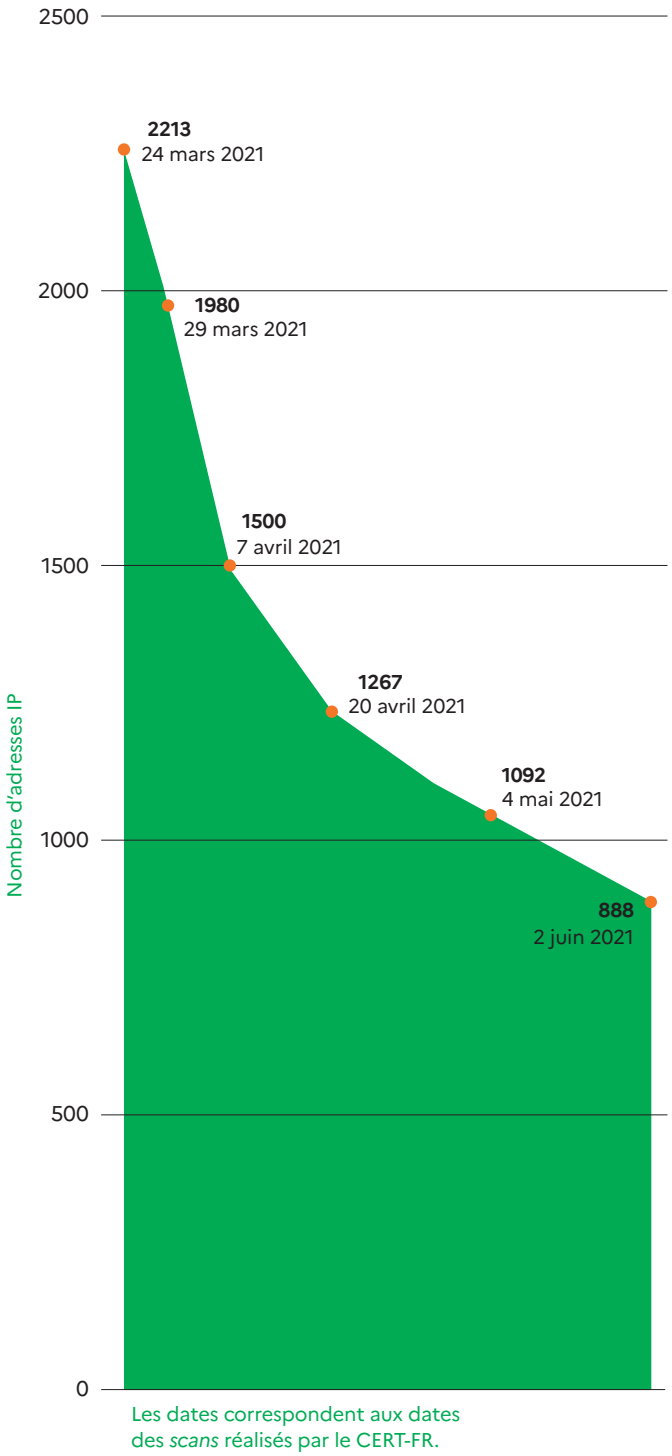
produit. Ce détail complique d'autant plus le travail d'évaluation de la gravité des vulnérabilités pour l'ensemble des acteurs (coordinateurs, utilisateurs, intégrateurs). L'utilisation des standards SBOM [75] et VEX [76] par les éditeurs permet de répondre partiellement à cette problématique. Le premier permet à un éditeur de fournir la liste des composants utilisés au sein de ses produits, tandis que le second lui permet d'informer ses clients si un produit est affecté ou non par une vulnérabilité découverte dans un de ses composants. Malheureusement, leur utilisation reste encore très limitée.

Le manque de sécurisation des environnements de développement, de test et d'intégration peut également être à l'origine d'une autre menace, celle de l'attaque par chaîne d'approvisionnement logicielle (*software supply chain attack*). Ce type d'attaque consiste en la compromission d'un logiciel par un attaquant dans le but d'y insérer un code malveillant lui permettant de prendre pied dans les systèmes d'information des utilisateurs de ce logiciel. Certains cas ont fait l'objet d'un traitement par le CERT-FR, notamment la compromission de la solution SolarWinds Orion en décembre 2020 [77] ainsi que celle de la solution 3CX Desktop App en mars 2023 [78].

L'ANSSI observe enfin que de nombreux attaquants profitent d'une trop faible maîtrise par les victimes de leurs systèmes d'information. À ce titre, la sous-traitance de tout ou partie d'un système d'information à une entreprise de services numériques ne peut être effectuée sans s'assurer du niveau de sécurité des services fournis. En effet, la responsabilité de la sécurité d'un système d'information reste à la charge de son propriétaire, en particulier pour les opérateurs stratégiques. ←

NOMBREUSES FAIBLESSES E
FAIBLESSES EXPLOITÉES **A** D

→ Adresses IP françaises vulnérables à la CVE-2021-26855



Les dates correspondent aux dates des *scans* réalisés par le CERT-FR.

B **VULNÉRABILITÉS LOGICIELLES**

Au cours de l'année 2023, l'exploitation de vulnérabilités a été à l'origine de nombreux incidents de sécurité traités par l'ANSSI. Dans une part significative des cas, des correctifs étaient pourtant disponibles pour ces vulnérabilités au moment de leur exploitation, et ces dernières avaient fait l'objet d'une publication (avis, bulletin ou alerte de sécurité) sur le site du CERT-FR [79]. Les cinq vulnérabilités les plus exploitées au cours de l'année 2023 sont présentées dans le tableau ci-dessous.

Avertissement : ce classement ne comptabilise que les événements pour lesquels l'ANSSI ou un prestataire d'investigation a pu confirmer avec un haut degré de certitude l'exploitation d'une vulnérabilité.

CVE	ÉDITEUR	CVSS SCORE [20]	RÉFÉRENCE CERT-FR
CVE-2021-21974	VMWARE	8.8	CERTFR-2023-ALE-015 CERTFR-2021-AVI-145
CVE-2023-20198	CISCO	10.0	CERTFR-2023-ALE-011 CERTFR-2023-AVI-0878
CVE-2023-3519	CITRIX	9.8	CERTFR-2023-ALE-008 CERTFR-2023-AVI-0568
CVE-2023-22518	ATLASSIAN	9.8	CERTFR-2023-AVI-0899 CERTFR-2023-ACT-048
CVE-2023-34362	PROGRESS SOFTWARE	9.8	CERTFR-2023-ALE-005

En complément, d'autres vulnérabilités rendues publiques en 2023 ont particulièrement marqué l'année en raison de leur criticité, du risque d'exploitation ou de leur impact potentiel pour les bénéficiaires de l'ANSSI.

CVE	ÉDITEUR	CVSS SCORE	RÉFÉRENCE CERT-FR
CVE-2023-23997	MICROSOFT	8.8	CERTFR-2023-ALE-002 CERTFR-2023-AVI-0231
CVE-2023-27997	FORTINET	9.8	CERTFR-2023-ALE-004 CERTFR-2023-AVI-0451
CVE-2023-35078	IVANTI	9.8	CERTFR-2023-ALE-009 CERTFR-2023-AVI-0584
CVE-2023-4966	CITRIX	9.4	CERTFR-2023-ALE-012 CERTFR-2023-AVI-0823
CVE-2023-36884	MICROSOFT	8.8	CERTFR-2023-ALE-006
CVE-2023-42117	EXIM	8.1	CERTFR-2023-ALE-010
CVE-2022-41328	FORTINET	6.7	CERTFR-2023-ALE-001 CERTFR-2023-AVI-0199
CVE-2023-37580	ZIMBRA	6.1	CERTFR-2023-ALE-007 CERTFR-2023-AVI-0546

[20] *Common Vulnerability Scoring System* (CVSS) est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables. Cette évaluation est constituée de trois mesures appelées métriques : la métrique de base, la métrique temporelle et la métrique environnementale. Le score indiqué dans ce document est celui de la métrique de base. Il est compris entre 0 et 10, 10 correspondant aux vulnérabilités les plus critiques. Plus d'information sur *www.first.org/cvss*.

Parmi les vulnérabilités précédemment décrites, la CVE-2021-21974 affectant VMWare ESXi [80] et la CVE-2023-34362 affectant la solution MOVEit Secure Managed File Transfer de l'éditeur Progress Software [53] ont donné lieu à des campagnes d'exploitation opportunistes à des fins lucratives. La première conduisait au chiffrement de données sur l'hyperviseur au moyen d'un rançongiciel baptisé « ESXiArgs », tandis que dans la seconde campagne, attribuée publiquement au groupe cybercriminel CL0P, l'attaquant menaçait les victimes de publier les données exfiltrées et les proposait à la vente. De la même manière, la vulnérabilité CVE-2023-22518 affectant le produit Confluence d'Atlassian aurait été utilisée pour le déploiement d'un rançongiciel. Dans ces exemples, les attaquants ont profité de l'exposition sur Internet d'équipements hébergeant des données sensibles, l'exploitation de la vulnérabilité étant suffisante pour accéder à ces données. Il est à noter que la campagne d'exploitation de la vulnérabilité CVE-2021-21974 a été observée en 2023 alors qu'un correctif était disponible depuis février 2021 et que des codes d'exploitation avaient été rendus publics en mai de la même année.

Comme les années précédentes, plusieurs vulnérabilités critiques publiées en 2023 concernent des équipements réseau (CVE-2023-20198, CVE-2023-27997, CVE-2023-3519, CVE-2023-4966, CVE-2022-41328), dont une partie assure également des fonctions de sécurité, notamment pour la mise en place d'un réseau privé virtuel (*Virtual Private Network*, VPN). Ces équipements sont des cibles de choix pour les attaquants, car ils offrent un accès discret et persistant au système d'information de la victime tout en permettant l'interception de trafic.

Enfin, les services de messagerie ont également été particulièrement ciblés en 2023 par des attaquants cherchant à accéder à des courriels, ou simplement à compromettre le poste de travail ou le compte d'un utilisateur. Les vulnérabilités peuvent par exemple permettre l'exécution de code dans le navigateur de la victime (CVE-2023-37580 affectant un produit Zimbra) ou encore la compromission de secrets d'authentification (comme la vulnérabilité CVE-2023-23397 affectant Microsoft Outlook). Les attaquants ciblent plus largement les équipements présents dans la chaîne de messagerie, comme les produits de sécurité pour courriels (voir focus ci-après).

IDENTIFIANT	CVE-2021-21974	DATE DE PUBLICATION	24/02/2021
ÉDITEUR	VMWARE	CVSS SCORE	8.8

Le 3 février 2023, l'ANSSI a pris connaissance d'une campagne d'attaques ciblant les hyperviseurs VMware ESXi dans le but d'y déployer un rançongiciel. Le service SLP, ayant fait l'objet de la publication de plusieurs correctifs ces dernières années (CVE-2020-3992 et CVE-2021-21974), a une nouvelle fois été visé dans le cadre de cette campagne. La première vague d'attaques consistait au chiffrement des fichiers de configuration des machines virtuelles, si bien qu'une méthode de restauration des disques de ces machines était possible. Une seconde vague initiée le 8 février 2023 employait une méthode permettant le chiffrement d'un plus grand volume de données dans les fichiers de grande taille, rendant leur restauration plus compliquée, voire impossible. La vulnérabilité CVE-2021-21974 permet à un attaquant de réaliser une exécution de code arbitraire à distance. Les systèmes ciblés auraient été des hyperviseurs ESXi en version 6.x et antérieures à 6.7 [80, 81].

IDENTIFIANT	CVE-2023-20198	DATE DE PUBLICATION	16/10/2023
ÉDITEUR	CISCO	CVSS SCORE	10.0

Entre le 16 et le 22 octobre 2023, Cisco a révélé l'existence de deux vulnérabilités affectant l'interface Web de gestion d'IOS XE (webui)[21]. Ces vulnérabilités permettent à un attaquant non authentifié de créer un utilisateur disposant de privilèges élevés. Activement exploitées par des attaquants, elles donnaient donc accès à l'ensemble des commandes et à la possibilité de modifier la configuration de l'équipement vulnérable, ce qui correspond à en prendre le contrôle complet. Tous les équipements exposant l'interface de gestion Web d'IOS XE ont dû être considérés comme compromis, l'application seule des correctifs n'étant pas suffisante pour expulser l'attaquant [82, 83].

[21] CVE-2023-20198 et CVE-2023-20273.

IDENTIFIANT	CVE-2023-3519	DATE DE PUBLICATION	19/07/2023
ÉDITEUR	CITRIX	CVSS SCORE	9.8

De multiples vulnérabilités ont été découvertes en juillet dans les produits Citrix NetScaler ADC et NetScaler Gateway. La plus critique permet à un attaquant non authentifié d'exécuter du code arbitraire à distance si l'équipement est configuré en tant que passerelle [22] ou en tant que serveur virtuel AAA [23]. Les clients ont été invités à migrer vers une version supportée et à jour des correctifs de sécurité. Le 20 juillet 2023, la CISA a documenté une méthode de recherche des signes d'une compromission de l'équipement [84, 85, 86].

IDENTIFIANT	CVE-2023-22518	DATE DE PUBLICATION	31/10/2023
ÉDITEUR	ATLASSIAN	CVSS SCORE	9.8

En octobre, une vulnérabilité a été découverte dans l'outil de travail collaboratif Confluence (versions Data Center et Server) développé par l'éditeur Atlassian. L'exploitation de cette vulnérabilité permet à un attaquant de porter atteinte à l'intégrité des données stockées dans l'outil. L'éditeur a notamment rapporté des incidents relatifs à cette vulnérabilité conduisant au déploiement d'un rançongiciel [87, 88].

IDENTIFIANT	CVE-2023-34362	DATE DE PUBLICATION	21/04/2022
ÉDITEUR	PROGRESS SOFTWARE	CVSS SCORE	9.8

Le 31 mai 2023, une vulnérabilité a été découverte au sein de la solution de transfert de fichiers MOVEit développée par l'éditeur Progress Software. Une injection SQL permet à un attaquant non identifié d'accéder, d'extraire ou de modifier la base de données de l'application. Selon le moteur de base de données utilisé (MySQL, Microsoft SQL Server ou Azure SQL), la structure et le contenu de la base de données peuvent être supprimés par un attaquant. L'exploitation de la vulnérabilité peut également permettre l'exfiltration de données *via* le déploiement de *webshells*. L'exploitation massive de cette vulnérabilité a été revendiquée en juin 2023 par le groupe cybercriminel CL0P. Plus de 80 noms de potentielles victimes ont été publiés par les attaquants à des fins d'extorsion [53].

IDENTIFIANT	CVE-2023-23997	DATE DE PUBLICATION	14/03/2023
ÉDITEUR	MICROSOFT	CVSS SCORE	8.8

En mars, Microsoft a indiqué l'existence d'une vulnérabilité affectant diverses versions du produit Outlook pour Windows. La vulnérabilité, activement exploitée dans le cadre d'attaques ciblées, permet à un attaquant de récupérer le condensat *NetNTLMv2* [24] sans intervention de l'utilisateur légitime [89, 90]. Un correctif a également été publié en mai pour une seconde vulnérabilité (CVE-2023-29324) qui permet de continuer à exploiter la vulnérabilité CVE-2023-23397 si le correctif de sécurité de mars 2023 pour les serveurs Microsoft Exchange n'a pas été appliqué [37].

[22] *Gateway : VPN virtual server, ICA Proxy, CVPN, RDP Proxy.*

[23] *AAA virtual server.*

[24] *New Technology LAN Manager*

IDENTIFIANT	CVE-2023-27997	DATE DE PUBLICATION	13/06/2023
ÉDITEUR	FORTINET	CVSS SCORE	9.8

Une vulnérabilité rendue publique en juin permet à un attaquant non authentifié d'exécuter du code arbitraire à distance sur des produits Fortinet proposant une fonctionnalité de *VPN SSL*. Cette vulnérabilité n'est exploitable que si cette fonctionnalité *VPN SSL* est activée. L'application seule des correctifs n'étant pas suffisante, le CERT-FR recommande dans son alerte d'effectuer une analyse des systèmes à partir des marqueurs de compromission fournis par Fortinet et d'appliquer les mesures de durcissement préconisées par l'éditeur [91, 92].

IDENTIFIANT	CVE-2023-35078	DATE DE PUBLICATION	25/07/2023
ÉDITEUR	IVANTI	CVSS SCORE	9.8

Une vulnérabilité affectant le produit Endpoint Manager Mobile (EPMM) a été découverte en juillet 2023. Elle permet à un attaquant d'obtenir un accès non authentifié à des chemins d'API spécifiques afin de récupérer des informations à caractère personnel d'utilisateurs. Un attaquant peut également, par le biais de cette vulnérabilité, modifier la configuration du produit EPMM et créer un compte administrateur.

Quatre jours plus tard, Ivanti a dévoilé une seconde vulnérabilité (CVE-2023-35081) qui permet à un attaquant ayant les droits administrateur d'effectuer une écriture arbitraire de fichier sur le serveur, conduisant *in fine* à une exécution de code arbitraire à distance. Cette vulnérabilité était activement exploitée dans le cadre d'attaques ciblées, en combinaison avec la vulnérabilité CVE-2023-35078 pour contourner l'authentification administrateur. Le 1er août 2023, la CISA, conjointement avec l'agence de sécurité des systèmes d'information norvégienne (NCSC-NO), a publié un avis concernant les vulnérabilités CVE-2023-35078 et CVE-2023-35081. La première aurait été exploitée depuis au moins avril 2023 [93, 94, 95]. ←

↓

Vulnérabilité dans la solution Barracuda Email Security Gateway

Le 23 mai 2023, l'entreprise américaine Barracuda Networks a annoncé qu'un de ses produits de sécurité pour courriels faisait l'objet d'une faille de sécurité critique (CVE-2023-2868). Ces équipements, chargés de filtrer et d'analyser les courriels, pouvaient être compromis lors de l'analyse de pièces jointes malveillantes. Des fichiers conçus pour exploiter cette vulnérabilité permettaient l'exécution de codes arbitraires sans restriction, dont l'installation de portes dérobées. La compromission de tels équipements peut suffire pour obtenir un accès à l'ensemble des courriels de la victime.

Selon l'éditeur de sécurité Mandiant [96, 97], cette vulnérabilité serait exploitée depuis au moins octobre 2022 par des attaquants menant des opérations d'espionnage pour le compte du gouvernement chinois. Les attaquants auraient réservé un soin particulier à la furtivité de l'exploitation de cette vulnérabilité jour-zéro, en rédigeant notamment des courriels destinés à être bloqués en aval de l'équipement vulnérable par le filtre anti-spam. Ainsi, le courriel malveillant et sa pièce jointe étaient analysés par la solution Barracuda sans que le destinataire n'en soit informé. Les attaquants auraient tenté de compromettre exclusivement des réseaux jugés d'intérêt[25], en ciblant prioritairement des équipements appartenant à des entités gouvernementales.

De nombreux équipements exposés ont fait l'objet de campagnes d'exploitation de vulnérabilités, publiques ou non, au cours de ces dernières années. La découverte et la mise en œuvre de ces vulnérabilités suggèrent que les groupes d'attaquants allouent des ressources importantes à la compromission d'équipements exposés et ne disposant généralement pas de supervision de sécurité.

[25] Seuls 5% des équipements déployés auraient été compromis, soit plusieurs milliers d'équipements.

C ORGANISATION DE GRANDS ÉVÉNEMENTS

→ Les grands événements offrent aux attaquants des opportunités supplémentaires d'agir. Ils nécessitent en effet la mise en place de nombreux systèmes d'information – souvent interconnectés et parfois créés pour l'occasion – par une multitude d'acteurs aux niveaux de sécurité hétérogènes. Les attaquants peuvent profiter de cette surface d'exposition étendue pour surveiller ou extorquer les organisateurs et les participants. Ils sont également susceptibles d'exploiter la couverture médiatique pour ternir l'image du pays hôte, voire perturber le déroulement de l'événement. Outre les campagnes d'espionnage menées en amont du sommet de l'OTAN à Vilnius, mentionnées précédemment, des attaquants auraient par exemple conduit des attaques par DDoS et une potentielle opération de divulgation de données exfiltrées lors de ce même événement [98, 99].

Des attaques de ce type pourraient notamment viser les Jeux olympiques et paralympiques de Paris 2024. La Coupe du monde de rugby, organisée en France en 2023, a constitué à ce titre un événement préfigurateur pour l'organisation de grands événements sur le territoire national [100]. L'ANSSI n'a pas remarqué d'évolution significative de la menace en amont ou durant la compétition, et aucune attaque informatique d'ampleur n'a été détectée. L'événement a par ailleurs permis de tester un dispositif renforcé de détection, d'alerte et de réponse à incident en amont des JOP2024.←

↓

Le rôle de l'ANSSI durant les Jeux olympiques et paralympiques 2024

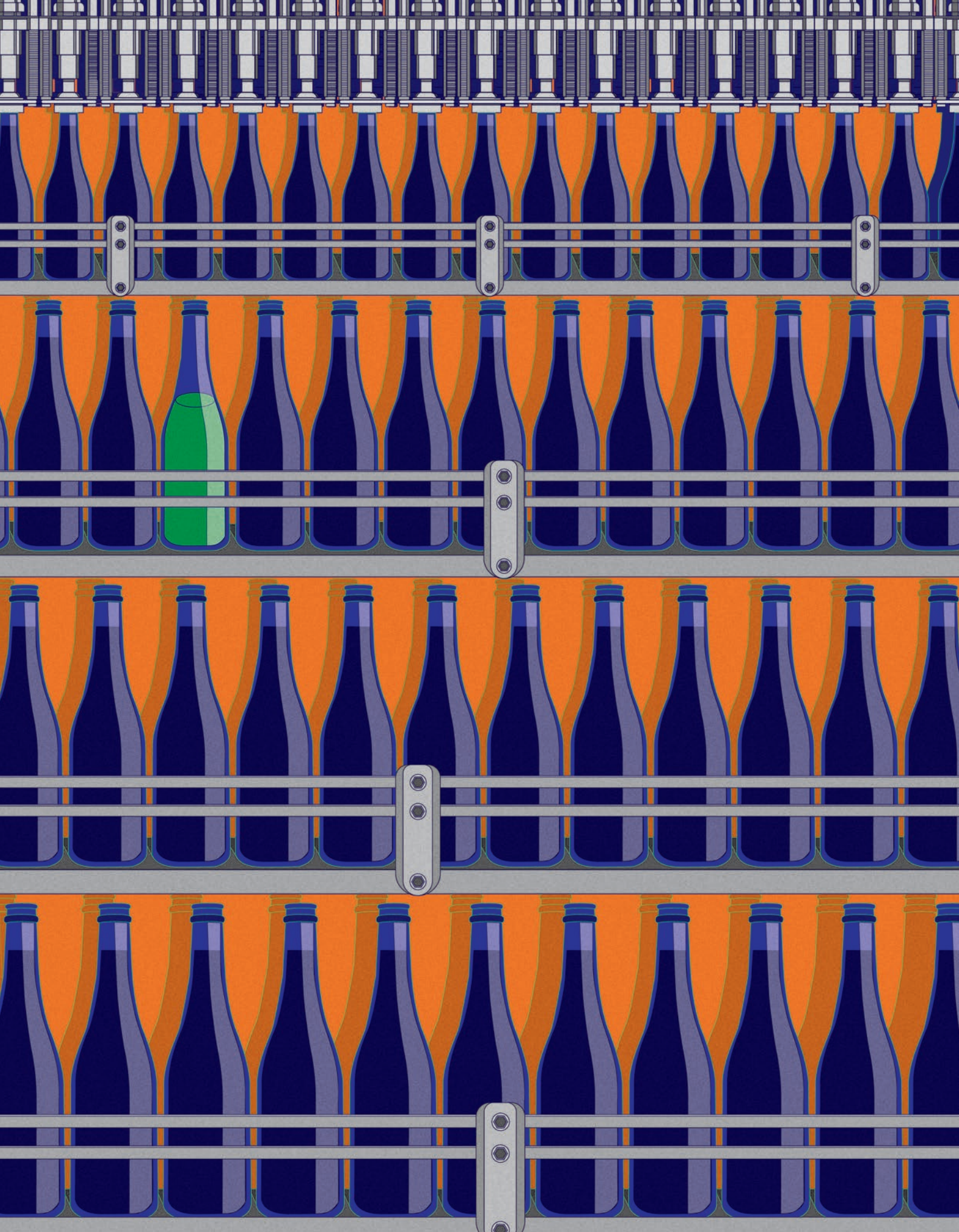
Le pilotage de la stratégie de prévention des cyberattaques en vue des JOP2024 a été confié à l'ANSSI par la Première ministre. Le dispositif mis en place par l'ANSSI, en étroite collaboration avec les différentes structures impliquées dans l'organisation des Jeux – dont en particulier la Délégation interministérielle aux Jeux olympiques et paralympiques (DIJOP), le ministère de l'Intérieur et des Outre-mer (MIOM) et le comité d'organisation des Jeux olympiques et paralympiques (Paris 2024) – s'articule selon cinq axes principaux :

- parfaire la connaissance des menaces pesant sur les Jeux ;
- sécuriser les systèmes d'information critiques ;
- protéger les données sensibles ;
- sensibiliser l'écosystème des Jeux ;
- se préparer à intervenir en cas d'attaque affectant les Jeux.

Les actions de sécurisation visent à accompagner les entités impliquées de manière adaptée à leur besoin. Elles consistent en la réalisation d'audits et d'un accompagnement technique pour les entités critiques, en un programme spécifique pour les entités sensibles, et à l'accès à des outils et des services, notamment pour l'évaluation du niveau de sécurité et la gestion de crise.

Un plan de sensibilisation est également mis en œuvre au bénéfice de plusieurs centaines d'acteurs de l'écosystème des Jeux. Il permet notamment d'informer sur la menace à l'encontre des grands événements sportifs et de diffuser des bonnes pratiques de cybersécurité. Dans cette optique, le CERT-FR a publié en août 2023 une première évaluation de la menace informatique contre les grands événements sportifs, assortie de recommandations [100].

Enfin, l'agence a défini, en coopération avec les différents services de l'État impliqués dans la préparation des JOP2024, un dispositif renforcé de veille, d'alerte et de traitement des incidents de sécurité informatique. Il comprend notamment une posture spécifique destinée à supporter une activité opérationnelle accrue. Plusieurs exercices de crise ont été organisés en 2023 pour se préparer collectivement à réagir en cas d'attaque informatique lors des Jeux.



CONCLUSION

→ Au cours de l'année 2023, l'ANSSI a pu constater des évolutions notables dans la structure et les méthodes des attaquants informatiques. Les opérations d'espionnage stratégique et industriel se maintiennent à un niveau élevé, et se concentrent de plus en plus sur des individus et des structures non gouvernementales qui créent, hébergent ou transmettent des données sensibles. Pour atteindre leurs objectifs, les acteurs de la menace perfectionnent leurs techniques afin d'éviter d'être détectés et suivis, voire identifiés. La menace d'attaques à but lucratif se maintient également à un niveau élevé, alimentée par des acteurs aux profils de plus en plus divers. L'écosystème cybercriminel profite aujourd'hui d'outils et de méthodes diffusés largement pour cibler des secteurs particulièrement vulnérables, avec des conséquences parfois graves pour la continuité d'activité et la protection des données à caractère personnel.

Dans un climat international tendu, les activités de déstabilisation ont connu cette année un regain. Les attaques par DDoS, dont l'impact est limité, restent les plus courantes. La menace d'opérations de plus grande envergure contre des secteurs d'importance critique à l'échelle de l'Union européenne, comme la divulgation coordonnée d'informations exfiltrées et le sabotage, ne peut néanmoins pas être exclue. Malgré les efforts de sécurisation engagés dans certains secteurs, les attaquants continuent de tirer profit des mêmes faiblesses pour s'introduire sur les réseaux, en exploitant notamment des vulnérabilités non corrigées et une trop faible maîtrise de leurs SI par les victimes. Ces tendances contribuent à l'augmentation générale du niveau de la menace informatique.

Le cadre réglementaire sur lequel s'appuie l'ANSSI connaît aussi des évolutions. Publiée le 27 décembre 2022 au Journal officiel de l'Union européenne, la directive *Network and Information System Security*, dite NIS 2, rentrera en vigueur en France au plus tard en 2024. Pour l'ANSSI, l'enjeu sera de déployer un dispositif efficace et pérenne permettant l'intégration de plusieurs milliers de nouvelles entités régulées au périmètre de l'agence, tout en adaptant les services et les outils mis à leur disposition. Cette transposition en droit national devra également s'articuler avec d'autres dispositifs comme les législations européennes REC [26] et DORA [27].

La structure et les méthodes des attaquants connaîtront inévitablement des évolutions en 2024, à l'heure où la France se prépare à accueillir les Jeux olympiques et paralympiques. Pour appréhender au mieux ces défis, l'ANSSI appelle à une prise en compte de la sécurité dès la conception des projets, à la mise en œuvre d'un réseau et de postes d'administration dédiés, au durcissement des systèmes d'information, notamment *via* l'utilisation régulière des services d'audit automatisés de l'ANSSI [28], et au développement de capacités de détection. L'agence recommande par ailleurs l'application rigoureuse des politiques de maintien en condition de sécurité des parcs informatiques, la mise en place d'une stratégie de sauvegarde des SI, ainsi que l'élaboration de plans de continuité et de reprise d'activité (PCA/PRA). L'ANSSI et le CERT-FR continueront de partager sur leurs sites des évaluations de la menace et des ressources utiles pour se protéger contre les menaces et les vulnérabilités les plus courantes. ←

[26] Directive (UE) 2022/2557 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience des entités critiques.

[27] Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier.

[28] Disponibles pour les opérateurs régulés ainsi que pour la sphère publique, ces services permettent d'évaluer la sécurité des annuaires *Active Directory* et de cartographier l'exposition sur Internet.

ANNEXES
BIBLIOGRAPHIE

[1]
CERT-FR
État de la menace ciblant le secteur des télécommunications.
18 décembre 2023.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-010/

[2]
SÉNAT
Pour une coordination de la cyberdéfense plus offensive dans la loi de programmation militaire 2024-2030.
24 mai 2023.
https://www.senat.fr/rap/r22-638/r22-6384.html

[3]
DGSI
La DGSI au cœur de l'organisation française de cyberdéfense.
23 juin 2021.
https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/nos-missions/cyberdefense/la-dgsi-au-coeur-de-lorganisation-francaise-de

[4]
GOOGLE
Active North Korean campaign targeting security researchers.
31 octobre 2023.
https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/

[5]
ZDNET
Les attaques par rançongiciel repartent à la hausse en France.
19 décembre 2023.
https://www.zdnet.fr/actualites/exclusif-les-attaques-par-rancongiciel-repartent-a-la-hausse-en-france-39963068.htm

[6]
ANSSI
Panorama de la cybermenace 2022.
24 janvier 2023.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-001/

[7]
CERT-FR
Panorama de la menace informatique 2021.
9 mars 2022.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-002/

[8]
CERT-FR
Scans et services.
https://www.cert.ssi.gouv.fr/scans

[9]
PALO ALTO
Novel News on Cuba Ransomware: Greetings From Tropical Scorpius.
9 août 2022.
https://unit42.paloaltonetworks.com/cuba-ransomware-tropical-scorpius/

[10]
TREND MICRO
Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals.
30 mai 2023.
https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html

[11]
MICROSOFT
Storm-0978 attacks reveal financial and espionage motives.
11 juillet 2023.
https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

[12]
CERT-UA
Attaque informatique contre des utilisateurs du système DELTA utilisant le code malveillant RomCom/FateGrab/StealDeal.
18 décembre 2022.
https://cert.gov.ua/article/3349703

[13]
BLACKBERRY
RomCom Threat Actor Suspected of Targeting Ukraine's NATO Membership Talks at the NATO Summit.
8 juillet 2023.
https://blogs.blackberry.com/en/2023/07/romcom-targets-ukraine-nato-membership-talks-at-nato-summit

[14]
ANSSI
Les dénis de service distribués (DDOS).
5 septembre 2023.
https://cyber.gouv.fr/publications/les-denis-de-service-distribues-ddos

[15]
ANSSI
Comprendre et anticiper les attaques DDoS.
20 mars 2015.
https://cyber.gouv.fr/publications/comprendre-et-anticiper-les-attaques-ddos

[16]
MANDIANT
Hacktivists Collaborate with GRU-sponsored APT28.
23 septembre 2022.
https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

[17]
LE PARISIEN
Niger : les hackers d'Anonymous Sudan menacent la France de représailles en cas d'intervention militaire.
1er août 2023.
https://www.leparisien.fr/high-tech/niger-les-hackers-danonymous-sudan-menacent-la-france-de-represailles-en-cas-dintervention-militaire-01-08-2023-P3YNIDEVEFEDFDXLUUN65WMSTQ.php

[18]
POLITICO
How hackers piled onto the Israeli-Hamas conflict. 15 octobre 2023.
https://www.politico.eu/article/israel-hamas-war-hackers-cyberattacks/

[19]
SEKOIA
Following NoName057(16) DDoSia Project's Targets.
23 juin 2023.
https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/

[20]
CERT-UA
Attaque informatique contre les systèmes d'information d'Ukrinform.
27 janvier 2023.
https://cert.gov.ua/article/3718487

[21]
CERT-UA
WinRAR comme « cyber-arme ». Attaque informatique destructrice d'UAC-0165 (problament Sandworm) contre le secteur public ukrainien avec RoarBat.
29 avril 2023.
https://cert.gov.ua/article/4501891

[22]
CERT-UA
Particularités des attaques informatiques destructrices contre des fournisseurs de services ukrainiens.
15 octobre 2023.
https://cert.gov.ua/article/6123309

[23]
REUTERS
Russian hackers were inside Ukraine telecoms giant for months.
5 janvier 2024.
https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

[24]
MANDIANT
Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology.
9 novembre 2023.
https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

[25]
SEKTORCERT
The attack against Danish, critical infrastructure.
novembre 2023.
https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

[26]
CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
The cyber threat to Canada's oil and gas sector.
21 juin 2023.
https://www.cyber.gc.ca/en/guidance/cyber-threat-canadas-oil-and-gas-sector

[27]
FRANCE INFO
Iran : « La cariture est une arme politique utilisée par les mollahs donc on l'a utilisée contre eux » dans *Charlie Hebdo*, explique Riss.
3 janvier 2023.
https://www.francetvinfo.fr/economie/medias/charlie-hebdo/iran-la-caricature-est-une-arme-politique-utilisee-par-les-mollahs-donc-on-l-a-utilisee-contre-eux-dans-charlie-hebdo-explique-riss_5577969.html

[28]
MICROSOFT
Iran responsible for *Charlie Hebdo* attacks.
3 février 2023.
https://blogs.microsoft.com/on-the-issues/2023/02/03/dtac-charlie-hebdo-hack-iran-neptunium/

[29]
FBI
Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad.
26 janvier 2022.
https://www.ic3.gov/Media/News/2022/220126.pdf

[30]
DÉPARTEMENT AMÉRICAIN DU TRÉSOR
Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election.
18 novembre 2021.
https://home.treasury.gov/news/press-releases/jy0494

[31]
LAB DOOKHTEGAN
https://t.me/lab_dookhtegan

[32]
CERT-FR
Campagne d'attaque du mode opératoire APT31 : description, contre-mesures et code.
15 décembre 2021.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-012/

[33]
BUNDESAMT FÜR VERFASSUNGSSCHUTZ
Cyber-Brief Nr. 02/2023.
31 août 2023.
https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-02-bfv-cyber-brief.pdf

[34]
CERT-FR
Synthèse de la menace ciblant les collectivités territoriales.
23 octobre 2023.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-008.pdf

[35]
COMMISSION EUROPÉENNE
Proposition de législation sur la cyberrésilience. 15 septembre 2022.
https://digital-strategy.ec.europa.eu/fr/library/cyber-resilience-act

[36]
CONSEIL EUROPÉEN
Législation sur la cyberrésilience : accord du Conseil et du Parlement sur les exigences en matière de sécurité pour les produits numériques.
30 novembre 2023.
https://www.consilium.europa.eu/en/press/press-releases/2023/11/30/cyber-resilience-act-council-and-parliament-strike-a-deal-on-security-requirements-for-digital-products/

[37]
CERT-FR
Campagnes d'attaques du mode opératoire APT28 depuis 2021.
26 octobre 2023.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-009.pdf

[38]
CISA
People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection.
24 mai 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

[39]
MICROSOFT
Volt Typhoon targets US critical infrastructure with living-off-the-land techniques.
24 mai 2023.
https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[40]
SENTINELONE
ShadowPad. A Masterpiece of Privately Sold Malware in Chinese Espionage.
19 août 2021.
https://www.sentinelone.com/labs/shadowpad-a-masterpiece-of-privately-sold-malware-in-chinese-espionage/

[41]
SECUREWORKS
ShadowPad Malware Analysis.
15 février 2022.
https://www.secureworks.com/research/shadowpad-malware-analysis

[42]
SYMANTEC
Redfly: Espionage Actors Continue to Target Critical Infrastructure.
12 septembre 2023.
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/critical-infrastructure-attacks

[43]
TALOS
Code leaks are causing an influx of new ransomware actors.
7 août 2023.
https://blog.talosintelligence.com/code-leaks-new-ransomware-actors/

[44]
BANKINFOSECURITY
Why Criminals Keep Reusing Leaked Ransomware Builders.
30 août 2023.
https://www.bankinfosecurity.com/blogs/criminals-keep-reusing-leaked-ransomware-builders-p-3503

[45]
SEKOIA
Overview of the Russian-speaking infostealer ecosystem: the distribution.
11 avril 2023.
https://blog.sekoia.io/overview-of-the-russian-speaking-infostealer-ecosystem-the-distribution/

[46]
SEKOIA
Overview of the Russian-speaking infostealer ecosystem: the logs.
11 mai 2023.
https://blog.sekoia.io/overview-of-the-russian-speaking-infostealer-ecosystem-the-logs/

[47]
ANALYST1
The Ransomware Diaries: Volume 2.
25 avril 2023.
https://analyst1.com/wp-content/uploads/2023/04/Ransomware-diaries-vol2-v2.pdf

[48]
BLEEPING COMPUTER
Angry Conti ransomware affiliate leaks gang's attack playbook.
5 août 2021.
https://www.bleepingcomputer.com/news/security/angry-conti-ransomware-affiliate-leaks-gangs-attack-playbook/

[49]
CERT-FR
FIN12 : Un groupe cybercriminel aux multiples rançongiciels.
18 septembre 2023.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-007.pdf

[50]
NCC GROUP
NCC Group Monthly Threat Pulse – June 2023.
20 juillet 2023.
https://www.nccgroup.com/ae/newsroom/ncc-group-monthly-threat-pulse-june-2023/

[51]
LOGPOINT
Emerging Threat: BianLian Ransomware's Shapeshift to Encryption-less Extortion.
22 juin 2023.
https://www.logpoint.com/en/blog/emerging-threat/bianlian-ransomware/

[52]
UNIT 42
CL0P Seeds ^_- Gotta Catch Em All!
29 septembre 2023.
https://unit42.paloaltonetworks.com/cl0p-group-distributes-ransomware-data-with-torrents/

[53]
CERT-FR
Synthèse sur l'exploitation d'une vulnérabilité dans MOVEit Transfer.
5 juillet 2023.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-ALE-005.pdf

[54]
MICROSOFT
Microsoft has discovered exploitation of a 0-day vulnerability in the SysAid IT support software.
9 novembre 2023.
https://twitter.com/MsftSecIntel/status/1722444141081076219

[55]
CERT-FR
Démantèlement du botnet Qakbot.
18 septembre 2023.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-006/

[56]
MICROSOFT
Microsoft has identified new Qakbot phishing campaigns.
16 décembre 2023.
https://twitter.com/MsftSecIntel/status/1735856754427047985

[57]
COFENSE
Are DarkGate and PikaBot the new QakBot? 2
0 novembre 2023.
https://cofense.com/blog/are-darkgate-and-pikabot-the-new-qakbot/

[58]
THE CITIZEN LAB
BLASTPASS. NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild.
7 septembre 2023.
https://citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild/

[59]
KASPERSKY
Operation Triangulation.
1er juin 2023.
https://securelist.com/trng-2023/

[60]
THE CITIZEN LAB
Sweet QuaDreams. A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers.
11 avril 2023.
https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/

[61]
MICROSOFT
DEV-0196: QuaDream's "KingsPawn" malware used to target civil society in Europe, North America, the Middle East, and Southeast Asia.
11 avril 2023.
https://www.microsoft.com/en-us/security/blog/2023/04/11/dev-0196-quadreams-kingspawn-malware-used-to-target-civil-society-in-europe-north-america-the-middle-east-and-southeast-asia/

[62] AMNESTY
Dans les mailles de Predator. La menace mondiale d'un logiciel espion « réglementé par l'Union européenne ».
9 octobre 2023.
https://www.amnesty.org/fr/documents/act10/7246/2023/fr/

[63]
EUROPEAN INVESTIGATIVE COLLABORATIONS
Predator Files. Octobre 2023.
https://eic.network/projects/predator-files.html

[64]
CALCALIST
Offensive cyber company QuaDream shutting down amidst spyware accusations.
16 avril 2023.
https://www.calcalistech.com/ctechnews/article/hy78kiym2

[65]
NCSC-UK
Infamous Chisel Malware Analysis Report.
31 août 2023.
https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/infamous-chisel/NCSC-MAR-Infamous-Chisel.pdf

[66]
CISA
Infamous Chisel Malware Analysis Report.
31 août 2023.
https://www.cisa.gov/news-events/analysis-reports/ar23-243a

[67]
ACCESS NOW
Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict.
25 mai 2023.
https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/

[68]
THE CITIZEN LAB
Armenia-Azerbaijan Conflict. Pegasus infections – Technical Brief.
25 mai 2023.
https://citizenlab.ca/2023/05/cr1-armenia-pegasus

[69]
FRANCE DIPLOMATIE
Cyber sécurité – Lutte contre la prolifération de la vente de logiciels espions.
31 mars 2023.
https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/securite-desarmement-et-non-proliferation/actualites-et-evenements-lies-a-la-securite-au-desarmement-et-a-la-non/2023/article/cyber-securite-lutte-contre-la-proliferation-de-la-vente-de-logiciels-espions

[70]
LE MONDE
Cybersécurité : la France à l'initiative d'un nouveau texte sur les logiciels commerciaux « offensifs ».
10 novembre 2023.
https://www.lemonde.fr/pixels/article/2023/11/10/cybersecurite-la-france-a-l-initiative-d-un-nouveau-texte-sur-les-logiciels-commerciaux-offensifs_6199348_4408996.html

[71]
CERT-FR
Vulnérabilité dans Apache Log4j.
10 décembre 2021.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/

[72]
CERT-FR
Bulletin d'actualité CERTFR-2021-ACT-053.
20 décembre 2021.
https://www.cert.ssi.gouv.fr/actualite/CERTFR-2021-ACT-053/

[73]
CERT-FR
Multiples vulnérabilités dans des systèmes d'exploitation temps réel.
18 août 2021.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-639/

[74]
CERT-FR
Multiples vulnérabilités dans Microsoft Exchange Server.
3 mars 2021.
https://cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-004/

[75]
CISA
Software Bill of Material (SBOM).
https://www.cisa.gov/sbom

[76]
CISA
Vulnerability Exploitability eXchange (VEX) - Use Cases.
Avril 2022.
https://www.cisa.gov/sites/default/files/2023-01/VEX_Use_Cases_Aprill2022.pdf

[77]
CERT-FR
Présence d'un code malveillant dans SolarWinds Orion.
14 décembre 2022.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-026/

[78]
CERT-FR
Compromission de l'application 3CX Desktop App.
31 mars 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-003/

[79]
CERT-FR
https://www.cert.ssi.gouv.fr

[80]
CERT-FR
Multiples vulnérabilités dans les produits VMWare.
24 février 2021.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-145/

[81]
CERT-FR
Campagne d'exploitation d'une vulnérabilité affectant VMware ESXi.
3 février 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/

[82]
CERT-FR
Multiples vulnérabilités dans Cisco IOS XE.
17 octobre 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-011/

[83]
CERT-FR
Multiples vulnérabilités dans Cisco IOS XE.
23 octobre 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0878/

[84]
CERT-FR
Vulnérabilité dans Citrix NetScaler ADC et NetScaler Gateway.
19 juillet 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-008/

[85]
CERT-FR
Multiples vulnérabilités dans Citrix NetScaler ADC et NetScaler Gateway.
19 juillet 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0568/

[86]
CISA
Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells.
20 juillet 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-201a

[87]
CERT-FR
Vulnérabilité dans Atlassian Confluence Data Center et Server.
31 octobre 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0899/

[88]
CERT-FR
Bulletin d'actualité CERTFR-2023-ACT-048.
6 novembre 2023.
https://www.cert.ssi.gouv.fr/actualite/CERTFR-2023-ACT-048/

[89]
CERT-FR
Vulnérabilité dans Microsoft Outlook.
15 mars 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-002/

[90]
CERT-FR
Multiples vulnérabilités dans Microsoft Office.
15 mars 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0231/

[91]
CERT-FR
Vulnérabilité dans les produits Fortinet.
13 juin 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-004/

[92]
CERT-FR
Multiples vulnérabilités dans les produits Fortinet.
13 juin 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0451/

[93]
CERT-FR
Multiples vulnérabilités dans Ivanti Endpoint Manager Mobile.
26 juillet 2023.
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-009/

[94]
CERT-FR
Vulnérabilité dans Ivanti Endpoint Manager Mobile.
25 juillet 2023.
https://www.cert.ssi.gouv.fr/avis/CERTFR-2023-AVI-0584/

[95]
CISA
Threat Actors Exploiting Ivanti EPMM Vulnerabilities.
1er août 2023.
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-213a

[96]
MANDIANT
Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Exploited Globally by Aggressive and Skilled Actor, Suspected Links to China.
15 juin 2023.
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

[97]
MANDIANT
Diving Deep into UNC4841 Operations Following Barracuda ESG Zero-Day Remediation (CVE-2023-2868).
29 août 2023.
https://www.mandiant.com/resources/blog/unc4841-post-barracuda-zero-day-remediation

[98]
LRT
Hackers stream anti-NATO broadcasts in Lithuania after cyber attacks.
10 juillet 2023.
https://www.lrt.lt/en/news-in-english/19/2031082/hackers-stream-anti-nato-broadcasts-in-lithuania-after-cyber-attacks

[99]
LRT
NATO summit leak linked to cyber attack on Lithuanian government – official.
20 juillet 2023.
https://www.lrt.lt/en/news-in-english/19/2039842/nato-summit-leak-linked-to-cyber-attack-on-lithuanian-government-official

[100]
CERT-FR
Grands évènements sportifs – Évaluation de la menace 2023. 30 août 2023.
https://www.cert.ssi.gouv.fr/cti/CERTFR-2023-CTI-005/

ANNEXES
RESSOURCES

PANORAMA DE LA CYBERMENACE

RESSOURCES

→**Collection Gestion de crise cyber**

Face à une menace informatique toujours croissante et en mutation, l'amélioration de la résilience numérique par l'entraînement à la gestion de crise cyber n'est plus seulement une opportunité, mais bien une nécessité pour toutes les organisations. L'ANSSI met à leur disposition la collection « Gestion de crise cyber », destinée à les accompagner dans la préparation et la gestion de crise cyber. Cette collection vise à apporter une expertise transverse sur l'ensemble des aspects de la gestion de crise cyber, et se compose ainsi de trois tomes : Organiser un exercice de gestion de crise cyber, Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique et Anticiper et gérer sa communication de crise cyber.

→**Collection Cyberattaques et remédiation**

Les dégâts financiers et matériels que peut occasionner une attaque informatique sont considérables. Si un incident majeur est partiellement ou mal remédié, ses effets peuvent s'étendre dans la durée. Ce fort potentiel de déstabilisation exige, à la fois des organisations cibles et des prestataires de cybersécurité, un savoir-faire dans l'endiguement de ces cyberattaques, dans la reprise de contrôle du système d'information compromis et dans le rétablissement d'un état de fonctionnement suffisant. La remédiation est l'étape clé pour y parvenir. L'ANSSI a donc élaboré un corpus s'articulant en trois volets (stratégique, opérationnel et technique) afin de partager son expérience de la mise en œuvre et du pilotage de la remédiation.

PANORAMA DE LA CYBERMENACE 2023

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

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

DÉPÔT LÉGAL

Février 2024
Publié sous licence Ouverte/
Open Licence (Etalab — VXX)

ISSN : 2970-4413

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI
51 boulevard de la Tour-Maubourg
75700 PARIS 07 SP
www.cyber.gouv.fr
www.cert.ssi.gouv.fr
cert-fr@ssi.gouv.fr