RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

PANORAMA DE LA CYBERMENACE 2022

PANORAMA DE LA CYBERMENACE 2022

SOMMAIRE

1 → LES ATTAQUANTS POURSUIVENT L'AMÉLIORATION DE LEURS CAPACITÉS — 6
A → Une convergence accrue de l'outillage des attaquants — 7
B → Le ciblage d'équipements périphériques — 10
C → Des acteurs privés toujours actifs — 12

2 → LE GAIN FINANCIER, L'ESPIONNAGE ET LA DÉSTABILISATION RESTENT LES PRINCIPAUX OBJECTIFS DES ATTAQUANTS — 14
A → Les attaques à finalité lucrative demeurent courantes — 15
B → Les activités d'espionnage se maintiennent en France et dans le monde — 22
C → Une menace de déstabilisation à surveiller dans un contexte géopolitique sensible — 24

3 → LES MÊMES FAIBLESSES SONT TOUJOURS EXPLOITÉES — 26
A → L'exploitation de vulnérabilités — 27
B → L'exploitation des nouveaux usages numériques à des fins malveillantes — 31
C → Les opportunités offertes par les divulgations de données — 33

CONCLUSION — 34
BIBLIOGRAPHIE — 36

SYNTHÈSE

Malgré une année marquée par le conflit russo-ukrainien et ses effets dans le cyberespace, la menace informatique n'a pas connu d'évolution majeure, les tendances identifiées en 2021 s'étant confirmées en 2022.
Le niveau général de la menace se maintient en 2022 avec 831 intrusions avérées contre 1082 en 2021[1]. Si ce nombre est inférieur à celui de 2021, cela ne saurait être interprété comme une baisse du niveau de la menace. En effet, si une chute de l'activité liée aux rançongiciels a bien été observée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sur les opérateurs régulés publics et privés à l'exception des hôpitaux, elle n'illustre pas l'évolution générale de cette menace cyber qui se maintient à un niveau élevé en se déportant sur des entités moins bien protégées.

Les acteurs malveillants poursuivent l'amélioration constante de leurs capacités à des fins de gain financier, d'espionnage et de déstabilisation. Cette amélioration s'illustre en particulier dans le ciblage des attaquants qui cherchent à obtenir des accès discrets et pérennes aux réseaux de leurs victimes. Les acteurs malveillants tentent de compromettre des équipements périphériques qui leur offrent un accès plus furtif et persistant aux réseaux victimes.
Ce ciblage périphérique se transpose également dans le type d'entités attaquées et confirme l'intérêt des attaquants pour les prestataires, les fournisseurs, les sous-traitants, les organismes de tutelle et l'écosystème plus large de leurs cibles finales.

La convergence des outils et des techniques des différents profils d'attaquants se poursuit également en 2022 et continue de poser des difficultés de caractérisation de la menace. L'utilisation de rançongiciels par des attaquants étatiques illustre cette porosité entre différents profils d'attaquants déjà identifiée en 2021. Leur utilisation à des fins de déstabilisation dans le cadre d'opérations de sabotage s'est par ailleurs matérialisée au cours de l'année 2022 et participe à complexifier la compréhension des activités malveillantes. L'apparition d'alternatives aux codes génériques tels que Cobalt Strike entraîne également des difficultés de détection de ces nouveaux outils utilisés par plusieurs profils d'attaquants, tout en compliquant la détermination des activités associées.

Les attaques poursuivant un objectif de gain financier demeurent les plus courantes en 2022. Si une baisse de l'activité des rançongiciels a été remarquée au premier semestre 2022, une multiplication des cas d'attaques par rançongiciels est observée depuis l'été 2022, particulièrement à l'encontre des collectivités territoriales et des établissements de santé avec des impacts conséquents. Les autres activités cybercriminelles comme les arnaques,

les services de vente d'accès ou de programme malveillant à la demande et le cryptominage se sont maintenues.

L'espionnage informatique a également perduré en 2022 tant en France que dans le monde. Il constitue la catégorie de menace qui a le plus impliqué les équipes de l'ANSSI sur l'année écoulée. Comme en 2021, la majorité des cas d'espionnage informatique traités par l'agence impliquait de nouveau des modes opératoires associés en source ouverte à la Chine. Ces intrusions répétées de modes opératoires étrangers témoignent d'un effort continu pour s'introduire dans les réseaux d'entreprises stratégiques françaises.

L'invasion russe en Ukraine a également été favorable à des campagnes d'espionnage stratégique au cours de l'année 2022 et a fourni un contexte favorable à des actions de déstabilisation en Europe. Si les attaques par sabotage informatique ont été, jusqu'à présent, relativement circonscrites au théâtre du conflit, d'autres modes d'actions tels que des attaques en déni de service distribué, des défigurations de sites Internet ou des opérations informationnelles associées à des exfiltrations de données ont affecté de nombreuses victimes en Europe et en Amérique du Nord.

Les usages numériques non maîtrisés et les faiblesses dans la sécurisation des données continuent d'offrir de trop nombreuses opportunités d'actions malveillantes. Le *Cloud Computing* et l'externalisation de services auprès d'entreprises de services numériques, sans clauses de cybersécurité adaptées, représentent toujours un vecteur d'attaque indirecte d'intérêt. En dépit d'une baisse du nombre d'attaques ciblant la *supply chain* en 2022, cette tendance reste d'actualité et souligne un risque systémique. Enfin, l'exploitation de vulnérabilités disposant de correctifs est encore trop souvent observée, notamment dans le cadre des incidents traités ou rapportés à l'ANSSI et ce malgré la publication d'avis et d'alertes sur le site du CERT-FR ou de campagnes de signalement. L'ANSSI appelle à l'application prioritaire des correctifs sur les systèmes exposés sur Internet ou, à défaut, la mise en place de mesures de contournement.

Le contexte géopolitique et les évènements majeurs que sont la Coupe du monde de rugby 2023 et les Jeux olympiques et paralympiques de Paris 2024 vont fournir aux attaquants de nombreuses opportunités de nuire. L'application rigoureuse d'une politique de mise à jour, une sensibilisation régulière des utilisateurs et le développement de capacités de détection et de traitement d'incident permettent de se prémunir des menaces les plus courantes.

1. 1082 intrusions avérées ont été portées à la connaissance de l'ANSSI sur l'ensemble de l'année 2021.

1 → LES ATTAQUANTS POURSUIVENT L'AMÉLIORATION DE LEURS CAPACITÉS

A → UNE CONVERGENCE ACCRUE DE L'OUTILLAGE DES ATTAQUANTS

→ Les attaquants étatiques poursuivent l'utilisation de codes et de méthodes traditionnellement employés dans le milieu cybercriminel. C'est plus particulièrement le cas des rançongiciels qui, en 2022, ont encore été utilisés à des fins de déstabilisation par des attaquants étatiques.
En juillet 2022, l'Albanie a ainsi été la cible de plusieurs cyberattaques menées notamment à l'aide de rançongiciels et de *wipers*[2] dans le cadre d'une opération de déstabilisation [1]. Ces attaques ont entraîné l'indisponibilité temporaire de plusieurs services numériques et de sites Internet gouvernementaux albanais le 15 juillet 2022 [2].

D'autres programmes malveillants ont été associés à la fois à des activités cybercriminelles et à des activités d'espionnage. C'est notamment le cas de la porte dérobée modulaire DarkCrystal RAT, mise en vente à partir de 2018 sur des forums russophones et composée d'un *stealer*[3], d'une interface de commande et de contrôle et d'un outil d'administration [3]. Sa structure

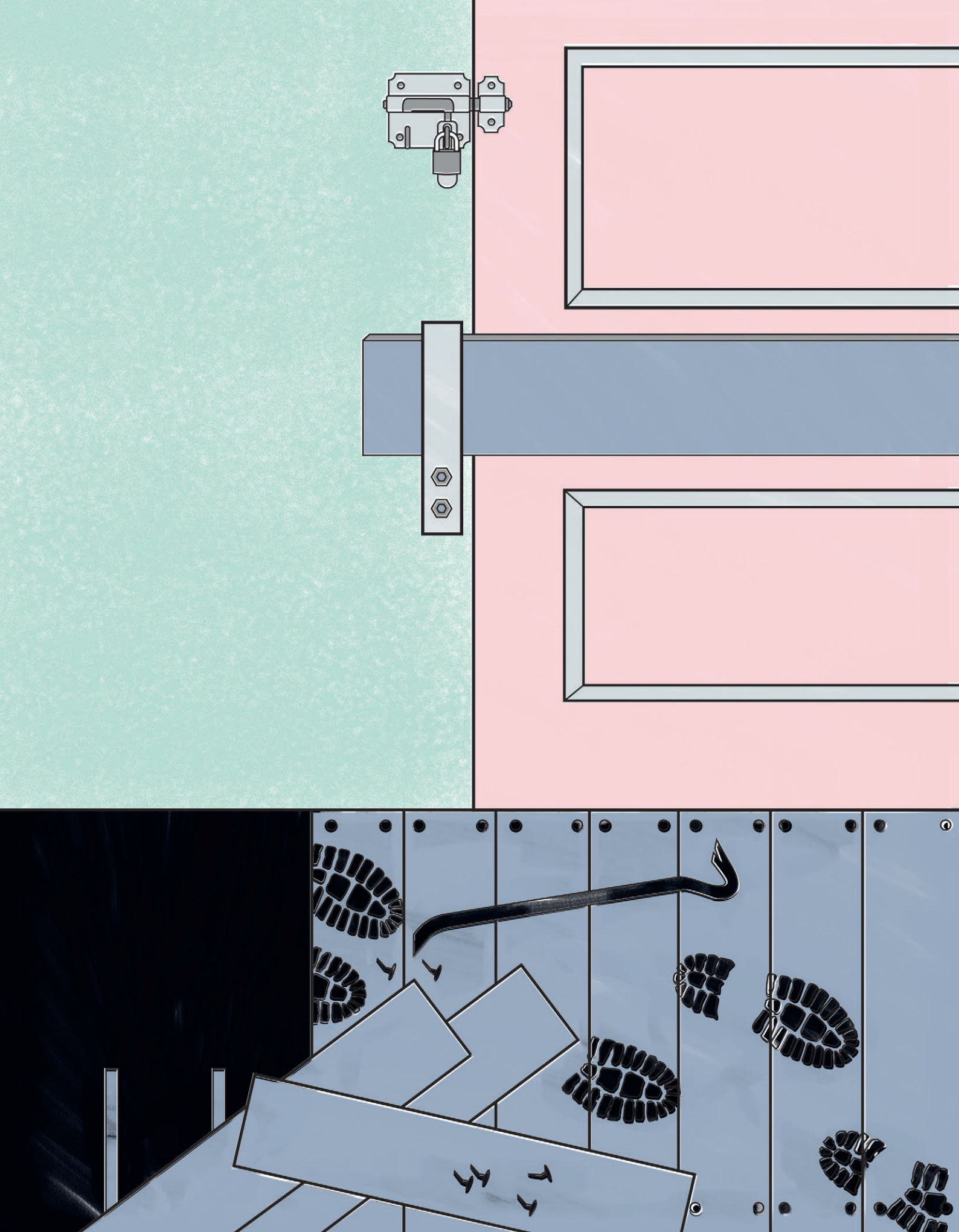
2. Programme malveillant visant à détruire les données présentes sur un système d'information.
3. Programme malveillant qui collecte différents types d'informations (identifiants et mots de passe, jeton d'authentification) avant de les transmettre à son opérateur.

modulaire permet de l'adapter aux objectifs de l'attaquant en ajoutant des modules d'enregistrement de frappe, de collectes d'identifiants enregistrés sur le navigateur Web ou encore de capture d'écran. Le faible prix de cet outil[4] et sa disponibilité en source ouverte en ont rapidement fait un outil populaire auprès de plusieurs acteurs cybercriminels. DarkCrystal RAT aurait également été utilisé par les attaquants du mode opératoire (MOA) Sandworm en juin 2022 pour compromettre des organisations ukrainiennes des secteurs des médias et des télécommunications selon le CERT-UA [4] [5].

À ce phénomène s'ajoute la proximité soupçonnée entre certains groupes cybercriminels et des États. Au cours des premiers mois du conflit russo-ukrainien, des groupes cybercriminels russophones ont réorienté leur ciblage pour s'aligner sur les intérêts russes en Ukraine et ont affiché leur soutien au gouvernement russe, à l'instar du groupe Conti [6]. À l'inverse, certains groupes ont souhaité cibler la Russie. Enfin, d'autres groupes ont pris le parti de rester neutres et de se concentrer sur des attaques purement lucratives. Ces prises de position patriotiques, spontanées ou orchestrées, participent une fois de plus à brouiller la caractérisation et l'attribution des activités malveillantes.

La réutilisation accrue d'outils disponibles en source ouverte et d'outils commerciaux comme Cobalt Strike[5], tant par des attaquants étatiques que cybercriminels, participe également aux difficultés de caractérisation de la menace. L'apparition d'alternatives à ces outils génériques complique encore la détection des activités malveillantes. Qu'ils soient commerciaux, comme Brute Ratel, ou disponibles en source ouverte, comme Mythic ou Sliver, ces outils sont de plus en plus utilisés par différents profils d'attaquants dans le cadre d'activités d'espionnage informatique ou d'activités cybercriminelles [7] [8]. Leur utilisation répond à une recherche de discrétion des attaquants.

4. 500 roubles pour un abonnement de deux mois.
5. Outil commercial utilisé à des fins de test d'intrusion.



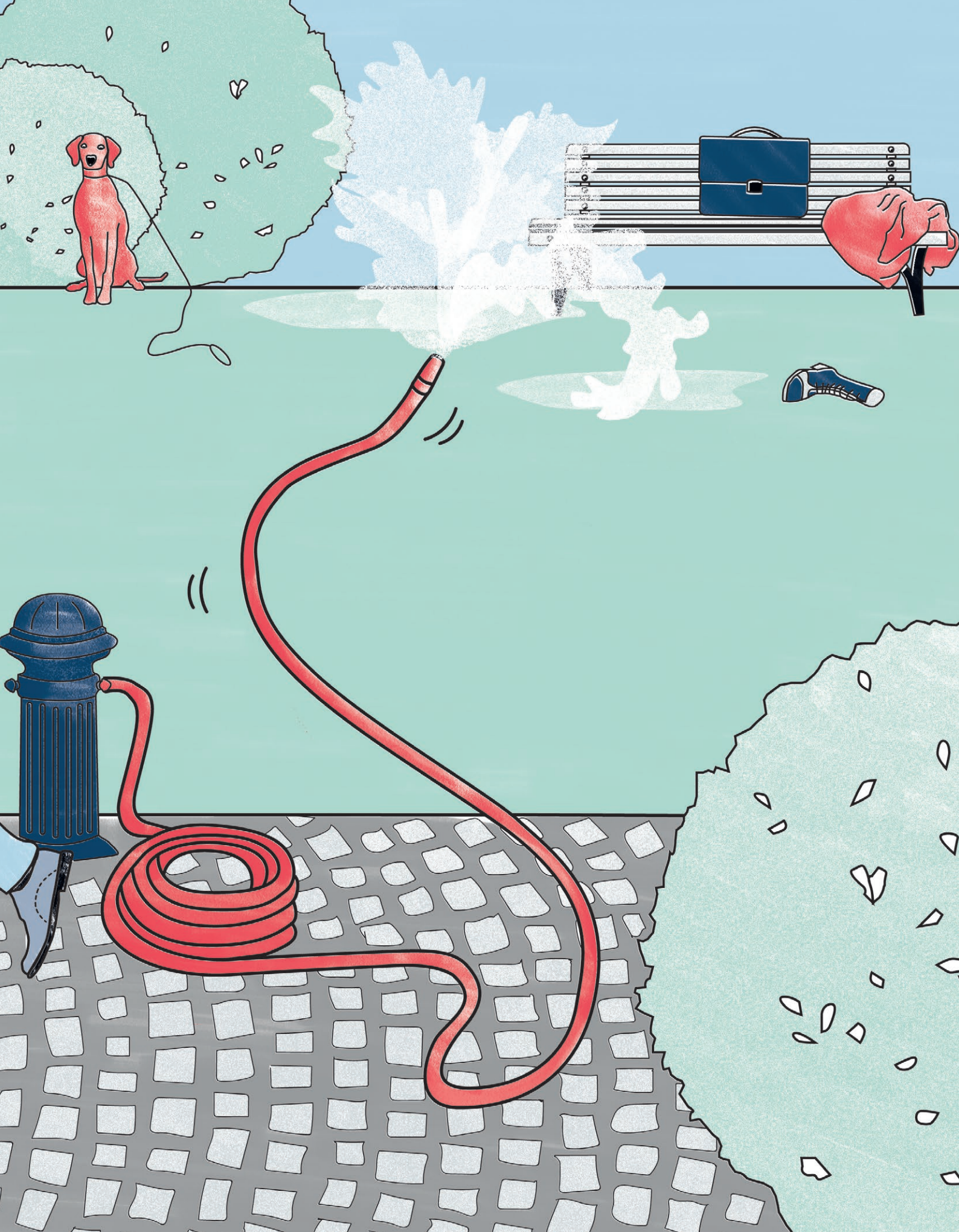
B → LE CIBLAGE D'ÉQUIPEMENTS PÉRIPHÉRIQUES

La recherche de furtivité des attaquants se traduit aussi dans le type d'équipement ciblé. La compromission d'équipements périphériques, tels que des pare-feux ou des routeurs, offre effectivement de multiples avantages. Ces équipements connectés en permanence, généralement peu supervisés par les outils grand public et professionnels, fournissent aux attaquants un accès discret et persistant aux réseaux de leurs victimes. La nature de ces équipements impose d'adapter les outils et les méthodes de collecte et d'analyse dans le cadre des opérations de remédiation.

Ces équipements peuvent également être intégrés à une infrastructure attaquante afin d'anonymiser les communications de l'acteur malveillant ou une activité de reconnaissance. Cette technique a été utilisée par les attaquants mettant en œuvre le mode opératoire (MOA) APT31 pour constituer une infrastructure de Commande et de Contrôle (C2) et de reconnaissance en compromettant des routeurs de marque Pakedge, Cyberoam et Cisco [9].

Ce type de ciblage a été observé et analysé récemment par l'ANSSI. L'agence a été informée d'activités malveillantes menées entre avril et décembre 2021 sur des équipements réseau d'une entité française disposant d'une présence internationale. Les analyses de l'ANSSI ont démontré qu'un attaquant avait compromis ces équipements et y avait installé des outils d'administration à distance (*Remote Administration Tool* – RAT). Profitant de la furtivité de sa présence sur ces équipements périphériques, l'attaquant a été en mesure d'utiliser ses accès pour se connecter à des machines du réseau interne de la victime, dont il avait été évincé un an plus tôt après la remédiation d'une précédente compromission. Il a ensuite exfiltré des informations techniques et des données métier. En ayant pris le contrôle de différents pare-feux, l'attaquant était également en mesure d'intercepter un certain type de trafic entre quelques bureaux, spécifiquement ciblés, de l'entité visée.

Des acteurs cybercriminels ont également eu recours à ces mêmes procédés. Les opérateurs du cheval de Troie Trickbot ont ainsi compromis des routeurs MikroTik et les ont intégrés à leur C2 [10].



C → DES ACTEURS PRIVÉS TOUJOURS ACTIFS

Malgré les révélations sur le programme Pegasus de NSO Group en 2021, le secteur des entreprises privées de lutte informatique offensive (LIO) reste très actif, comme en atteste le récent rachat de l'entreprise italienne RCS Lab par son concurrent Cy4Gate [11]. Les produits de RCS Lab et plus particulièrement son espiogiciel Hermit ont fait l'objet de publications par l'éditeur de sécurité Lookout [12] et le *Threat Analysis Group* de Google [13]. Hermit aurait notamment été utilisé au Kazakhstan pour cibler des équipements Android après les manifestations qui ont eu lieu au début de l'année 2022. Si aucun ciblage de la France ou de personnalités françaises à l'aide de cet espiogiciel n'est connu, le dévoiement potentiel de ce type d'outil justifie le suivi de ces entreprises et de leurs capacités.

La problématique de l'utilisation de ces logiciels espions est traitée au niveau européen par la commission d'enquête PEGA[6] du Parlement européen, qui a rendu public son rapport préliminaire le 8 novembre 2022 [14].

Parallèlement à ces acteurs offrant des solutions d'espiogiciels, des entreprises, telles que BellTrox InfoTech Services [15], fournissent des prestations moins sophistiquées mais persistantes comme de l'expertise humaine (*hacker-for-hire*). Elles mènent des activités intenses d'espionnage économique et politique au profit de clients variés qui peuvent porter atteinte au secret des affaires et à la défense nationale.

Les récentes révélations du journal *The Sunday Times* et de l'organisation non gouvernementale *The Bureau of Investigative Journalism* [16] à propos de campagnes d'espionnage de personnalités ayant critiqué l'attribution de la Coupe du monde de football 2022 au Qatar en sont une nouvelle illustration. Quatre personnalités françaises feraient partie des cibles présumées [17]. Les publications régulières sur les capacités cyber offensives privées soulignent la nécessité de renforcer les capacités de détection et d'investigation.

6. Commission d'enquête sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents créée le 10 mars 2022. Elle a pour mandat de récolter des informations sur l'utilisation par des États membres et d'autres pays de logiciels de surveillance qui violeraient les droits et les libertés inscrits dans la Charte des droits fondamentaux de l'Union européenne.

2 → LE GAIN FINANCIER, L'ESPIONNAGE ET LA DÉSTA-BILISATION RESTENT LES PRINCIPAUX OBJECTIFS DES ATTAQUANTS

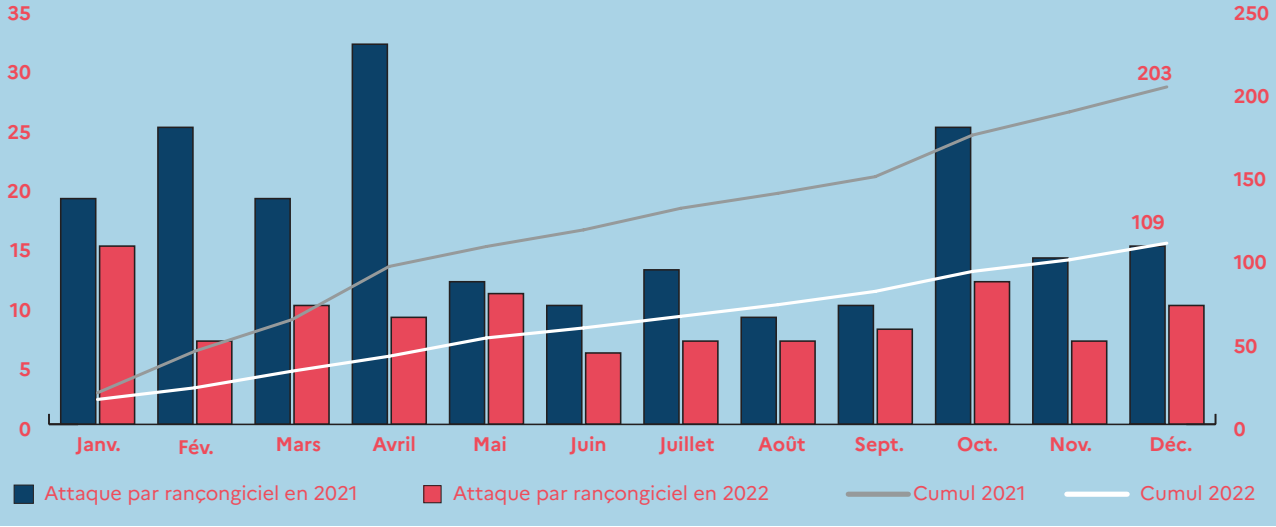
A → LES ATTAQUES À FINALITÉ LUCRATIVE DEMEURENT COURANTES

Si les attaques à finalité lucrative restent courantes, une baisse en volume de l'activité liée aux rançongiciels en France et en Europe est observée depuis le début de l'année 2022, tant au niveau de l'ANSSI que par certains partenaires étrangers et éditeurs [18]. Le nombre total de compromissions portées à la connaissance de l'ANSSI est ainsi inférieur de 46 % à celui constaté sur la même période en 2021. Cette diminution avait commencé à être observée à la fin de l'année 2021. Elle se limite toutefois aux incidents signalés à l'agence et ne reflète pas nécessairement une vision exhaustive de la situation. L'ANSSI note cependant une multiplication des attaques par rançongiciel depuis le mois de septembre qui pourrait annoncer une intensification à venir de ces activités malveillantes. Plusieurs collectivités territoriales ont ainsi été victimes de rançongiciel depuis l'été 2022 [19] [20] [21] [22] [23] [24].

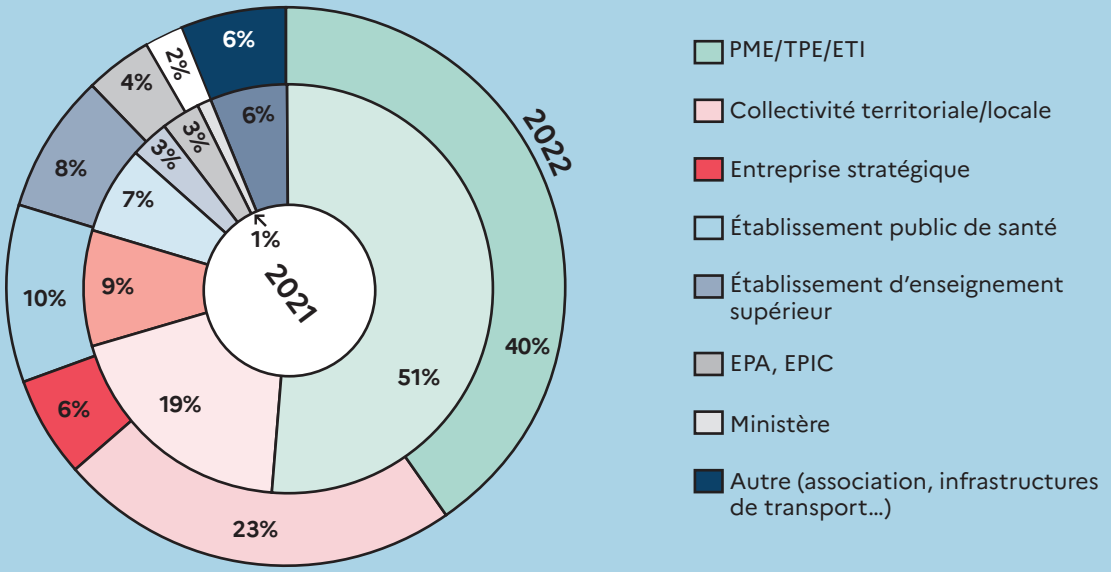
DES COLLECTIVITÉS TERRITORIALES PARTICULIÈREMENT AFFECTÉES PAR LES ATTAQUES PAR RANÇONGICIEL :

Les collectivités locales constituent la deuxième catégorie de victime la plus affectée par des attaques par rançongiciel derrière les TPE, PME et ETI. Elles représentent ainsi 23 % des incidents en lien avec des rançongiciels traités par ou rapportés à l'ANSSI en 2022. Les conséquences de ces attaques sont particulièrement importantes pour les collectivités concernées. Ces attaques parfois destructrices perturbent notamment les services de paie, le versement des prestations sociales et la gestion de l'état civil. Passé la découverte de l'attaque, le fonctionnement de ces entités continue d'être dégradé le temps de la reconstruction, affectant durablement les services à destination des administrés.

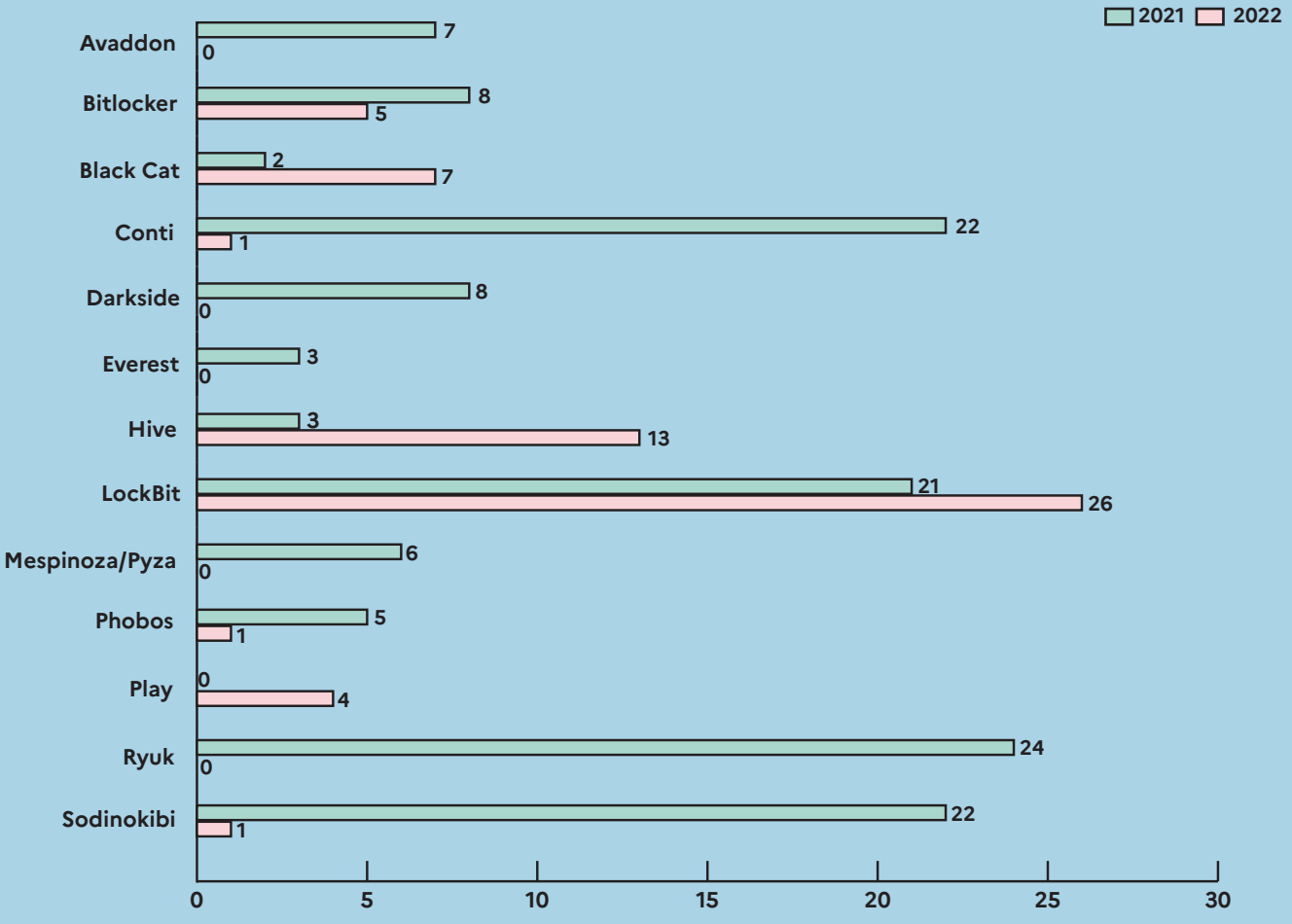
→ COMPARAISON DES SIGNALEMENTS D'ATTAQUES PAR RANÇONGICIEL EN 2021 ET 2022.



→ RÉPARTITION DES TYPES DE VICTIMES DE COMPROMISSIONS PAR RANÇONGICIEL EN 2021 ET 2022



→ COMPARATIF DES PRINCIPALES SOUCHES UTILISÉES DANS DES INCIDENTS SIGNALÉS À L'ANSSI EN 2021 ET 2022.



Plusieurs facteurs peuvent expliquer cette baisse perçue. Après l'invasion russe en Ukraine, une réorientation du ciblage des groupes cybercriminels a été remarquée. Certains groupes ont choisi de s'aligner avec les intérêts des belligérants. D'autres groupes ont modifié substantiellement leur ciblage géographique en s'attaquant notamment à l'Amérique latine [25]. L'engagement dissuasif de certains pays, comme les États-Unis [26], dans la lutte contre la cybercriminalité a pu influer sur le ciblage des acteurs cybercriminels. Le conflit russo-ukrainien a également entraîné la réorganisation de certains groupes cybercriminels russophones, à l'instar du groupe Conti, victime de divulgations de données vraisemblablement orchestrées par un membre ukrainien du groupe [27]. Cette restructuration a pu influencer le rythme opérationnel de ces groupes.

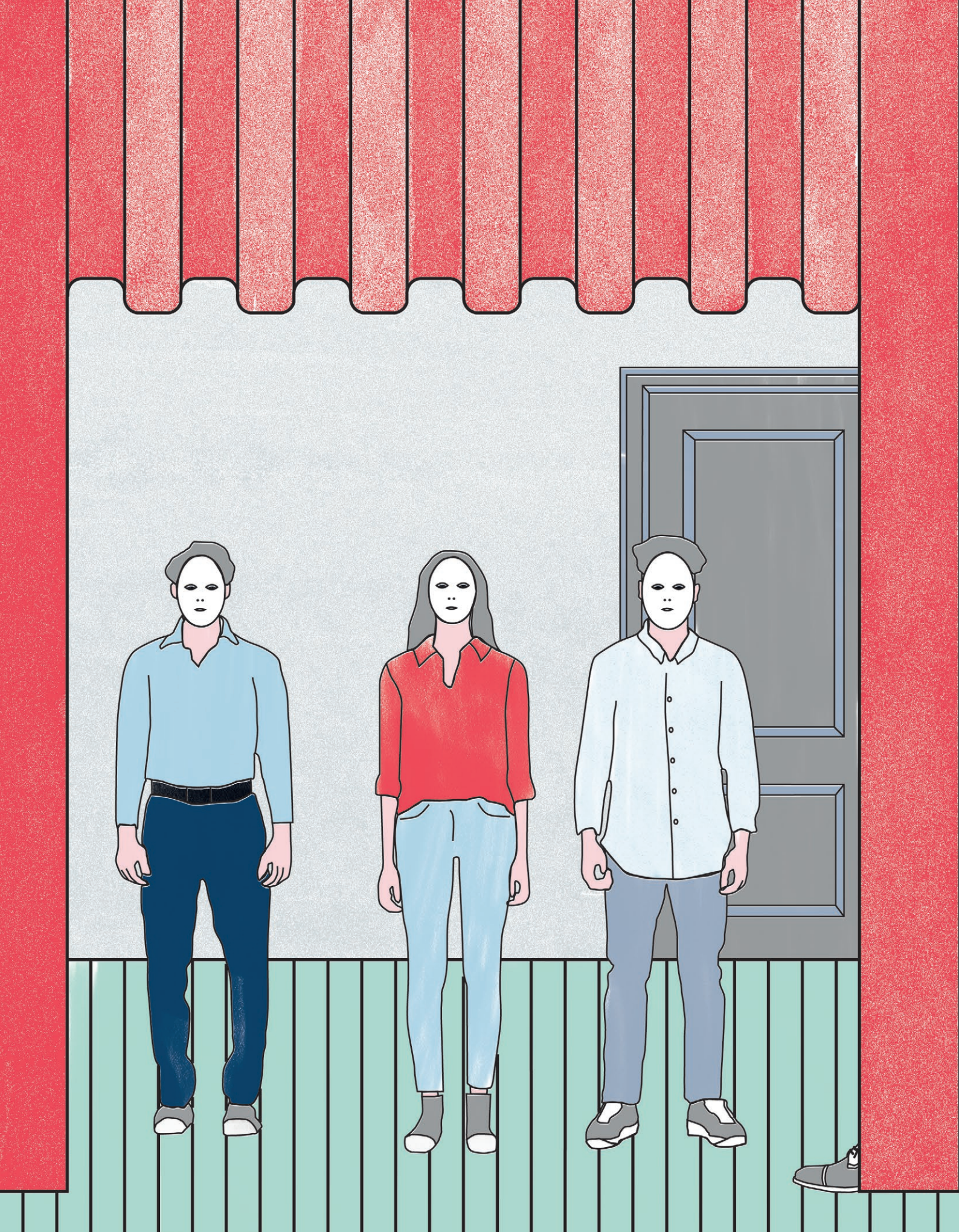
Cela étant, comme en 2021, les principales victimes françaises d'attaques par rançongiciels observées par l'agence en 2022 demeurent les TPE, PME, et ETI, suivies des collectivités territoriales et des établissements publics de santé.

En 2022, les principales souches de rançongiciel utilisées dans les incidents portés à la connaissance de l'ANSSI sont LockBit, Hive et BlackCat.
Si le nombre d'attaques par rançongiciel est en baisse sur l'année 2022, leurs conséquences demeurent très importantes, plus particulièrement dans des secteurs critiques comme la santé. Outre les conséquences financières, ce type d'évènement peut également avoir un impact sur le suivi des patients [28] et la confidentialité de leurs données de santé. Dans la nuit du 20 au 21 août 2022, le Centre Hospitalier Sud Francilien a été victime d'une attaque par rançongiciel revendiquée par le groupe Lockbit. L'indisponibilité d'une partie des données et des applications portées par le système d'information a contraint les services hospitaliers à fonctionner en mode dégradé. En outre, le 23 septembre 2022, 11 gigaoctets de données exfiltrées lors de la compromission ont été publiés sur le site web du groupe cybercriminel. Parmi les éléments divulgués figuraient notamment des données médicales et personnelles liées aux patients et au personnel hospitalier. Une situation similaire s'est répétée quelques mois plus tard au Centre Hospitalier de Versailles [29].

L'action des équipes techniques du Centre Hospitalier, assistées par l'ANSSI et par plusieurs prestataires, a permis un redémarrage des services critiques. La reconstruction sécurisée du système d'information ainsi que le retour à un fonctionnement nominal nécessiteront un travail de long terme.

Certains gouvernements ont également été victimes d'attaques par rançongiciel, notamment le Pérou et le Costa Rica en avril 2022. En mai 2022, ce dernier a déclaré l'état d'urgence après l'attaque menée à l'aide du rançongiciel Conti [30]. C'est aussi le cas du gouvernement du Monténégro, victime en août 2022 d'une attaque s'appuyant sur le rançongiciel Cuba [31]. Les conséquences sur le fonctionnement de l'administration et de certains services publics numériques étaient telles que le gouvernement, craignant une propagation vers certaines infrastructures critiques, a sollicité l'aide de la communauté internationale. Pour les assister dans leurs investigations et la remédiation de leurs services prioritaires, une équipe de l'ANSSI a été déployée sur place au mois de septembre.

L'activité cybercriminelle ne se restreint pas aux rançongiciels. D'autres types d'activités tels que la revente de



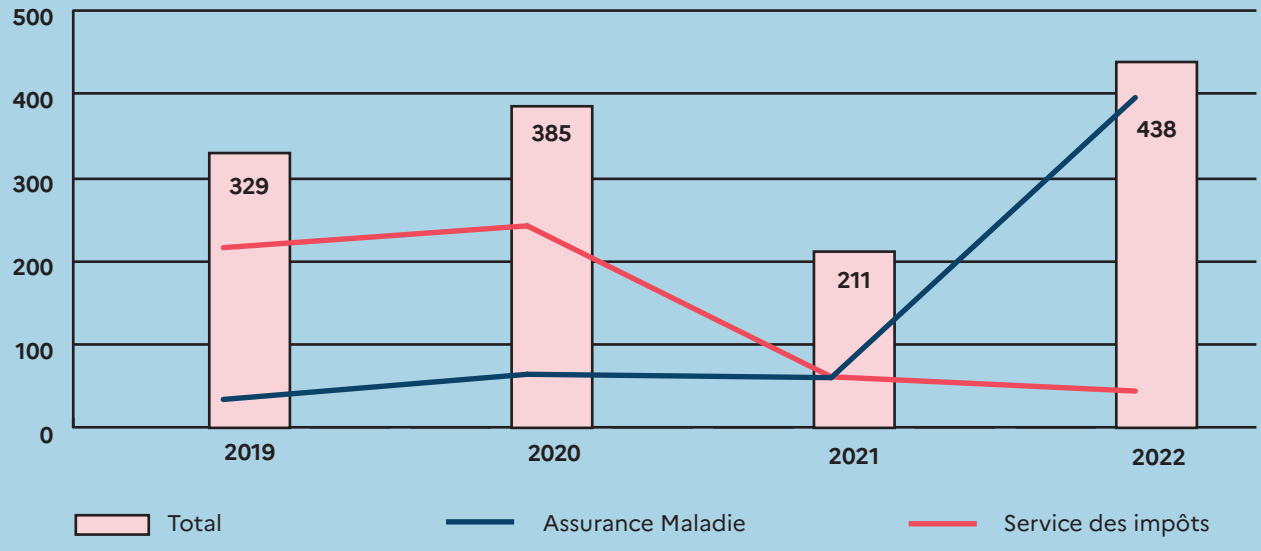
données personnelles ou bancaires et des arnaques plus classiques se sont maintenus. Un changement de thématique des campagnes d'hameçonnage a été observé. Il ressort ainsi des signalements effectués à l'ANSSI que la thématique des impôts est progressivement remplacée par celle de la santé, en usurpant notamment l'identité de l'Assurance Maladie. Les attaquants cherchent ainsi à exploiter le contexte sanitaire et l'actualité liée à la création de « Mon espace santé[7] ».

Les acteurs offrant des services d'infrastructures à des fins d'hébergement ou de distribution de services malveillants ont également maintenu leurs activités. Ces maillons essentiels de l'écosystème cybercriminel ont résisté aux opérations de démantèlement conduites par les forces de l'ordre [32]. Si certains services comme Dridex ou TrickBot semblent avoir disparu [33], d'autres à l'image de QakBot ou Emotet sont de nouveau actifs [34].

Une vigilance particulière doit être accordée aux activités de cryptominage. En effet, les cybercriminels ont adapté leurs techniques, leurs tactiques et leurs procédures (TTP) pour être moins détectables, en consommant par exemple moins de puissance de calcul (CPU) sur les machines compromises ou en dissimulant les traces de leurs activités. C'est notamment le cas du groupe TeamTNT qui a annoncé la fin de ses activités en novembre 2021 [35]. Ce mode opératoire risque toutefois d'inspirer d'autres groupes. Parfois peu visibles pour les victimes, ces activités génèrent pourtant des revenus considérables qui pourraient être réinvestis par les attaquants pour acquérir de nouvelles capacités. Les membres du groupe Kinsing se sont notamment distingués par le soin apporté à la dissimulation de leurs activités via diverses techniques d'obfuscation.
Le groupe se démarque également par l'automatisation de l'exploitation de vulnérabilités comme Log4J[8], exploitée deux jours après sa divulgation [36].

7. Espace numérique proposé par l'Assurance Maladie et le ministère de la Santé, qui a vocation à devenir le carnet de santé numérique interactif de tous les assurés.
8. Vulnérabilité découverte dans la bibliothèque de journalisation Apache Log4j.

→ ÉVOLUTION DE LA THÉMATIQUE EXPLOITÉE DANS LES COURRIELS D'HAMEÇONNAGE DEPUIS 2019



B → LES ACTIVITÉS D'ESPIONNAGE SE MAINTIENNENT EN FRANCE ET DANS LE MONDE

Comme en 2021, la menace d'espionnage informatique est celle qui a le plus impliqué les équipes de l'ANSSI en 2022. Ainsi, sur les 19 opérations de cyberdéfense et les incidents majeurs traités par l'agence en 2022, 9 impliquaient de nouveau des modes opératoires associés en source ouverte à la Chine. Ces intrusions répétées attestent d'un effort continu pour s'introduire dans les réseaux d'entités françaises stratégiques.

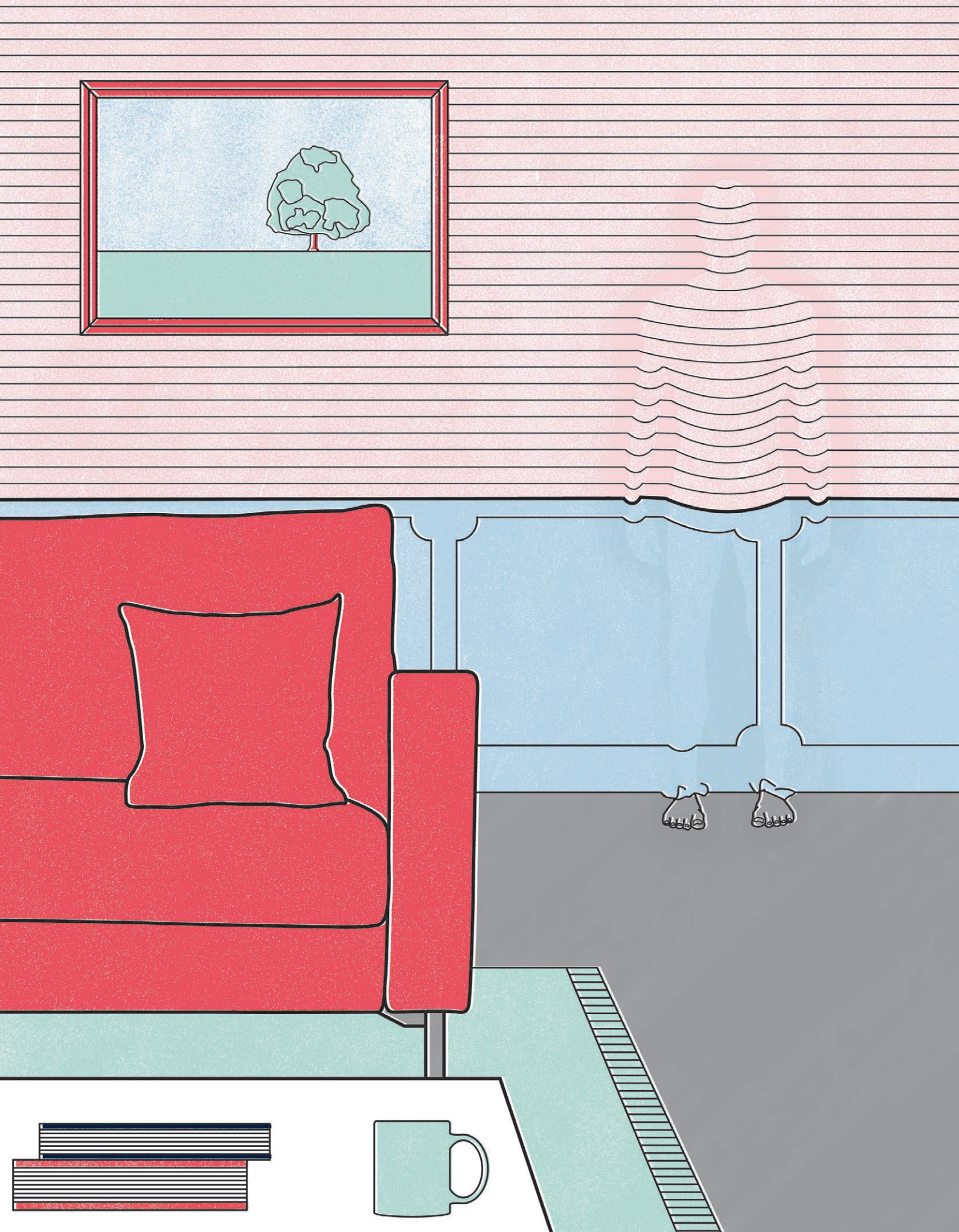
> Avertissement : l'évolution du nombre d'incidents majeurs et d'opérations de cyberdéfense ne doit pas être comprise comme une mesure de l'évolution du niveau menace. Elle est le fait des différents modes d'engagement des équipes de l'ANSSI qui s'appuie également sur un ensemble de prestataires qualifiés de réponse à incidents de sécurité pour le traitement des incidents relevant de son périmètre.

Durant le premier semestre 2022, l'ANSSI a traité la compromission en profondeur du système d'information d'un fournisseur spécialisé du secteur de la défense, dont le savoir-faire est en mesure de susciter l'intérêt d'un gouvernement étranger. Les investigations menées par l'ANSSI ont confirmé la présence d'un acteur malveillant au sein du système d'information depuis au moins mars 2021. De multiples occurrences d'exfiltration de données ont été détectées sur la même période. Des actions de remédiation ont été entreprises par la victime, en coordination avec l'ANSSI, afin de garantir l'éviction de l'attaquant et de permettre la reconstruction d'une infrastructure de confiance.

Ces différentes compromissions confirment par ailleurs une évolution plus durable du ciblage des attaquants qui ne se restreint pas à une organisation donnée. Suivant la tendance des attaques sur la chaîne d'approvisionnement (*supply chain*), les acteurs malveillants visent plus couramment les entreprises, les partenaires, les sous-traitants, les prestataires et les organisations de tutelle de leurs cibles finales dans le cadre de campagnes d'espionnage global au long cours.

Ce constat ne se limite pas à la France. Plusieurs campagnes d'espionnage ciblant par exemple la base industrielle et technologique de défense (BITD) en Russie ont été révélées par différents éditeurs de sécurité [37] [38] [39].

Le contexte de l'invasion russe en Ukraine a également été favorable à des campagnes d'espionnage stratégique contre des pays européens et des membres de l'OTAN. Plusieurs modes opératoires ont été mis en œuvre dans le cadre de telles campagnes au cours de l'année 2022 comme Gamaredon [40], APT28 [41] et Turla [42]. Ce ciblage devrait se poursuivre à la faveur d'un contexte géopolitique particulièrement tendu.



C → UNE MENACE DE DÉSTABILISATION À SURVEILLER DANS UN CONTEXTE GÉOPOLITIQUE SENSIBLE

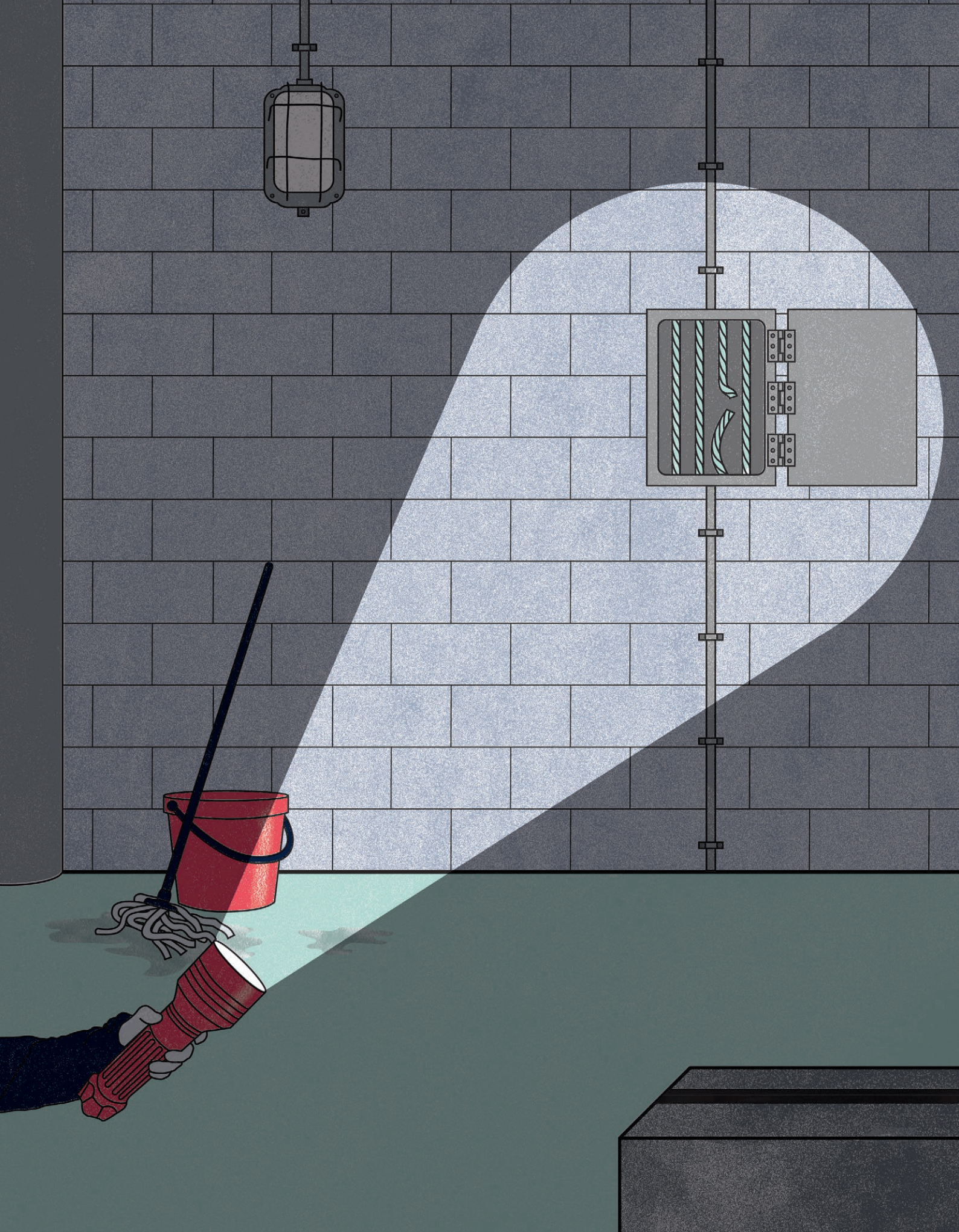
L'invasion russe de l'Ukraine a fourni un contexte propice à l'augmentation du niveau de la menace de déstabilisation en Europe. Celle-ci s'est matérialisée sous différentes formes. Des attaques par déni de service distribué, par sabotage informatique ainsi que des opérations informationnelles s'appuyant sur des compromissions de systèmes d'information ont été observées.
Si les tentatives de sabotage informatique à l'encontre d'infrastructures critiques ont été nombreuses dans ce contexte, elles ont été relativement circonscrites géographiquement à la zone de conflit ukrainien. Peu de dommages collatéraux ont été constatés, à l'exception de l'attaque subie par le réseau de communication satellitaire KA-SAT[9] qui a eu des effets de bord en dehors des frontières ukrainiennes.

Cette attaque menée dans la nuit du 23 au 24 février 2022 et attribuée à la Russie par le Service européen pour l'action extérieure le 10 mai 2022 [43] n'a pas directement ciblé le satellite, qui est demeuré pleinement fonctionnel, mais les équipements au sol. Plusieurs dizaines de milliers de modems ont été mis hors service en Europe, dont un grand nombre en France. Cette coupure de communication satellitaire a privé plusieurs milliers de citoyens français résidant en zones blanches de moyen de communication avec les services d'urgence et de secours. Des structures publiques ainsi que de nombreuses entreprises qui utilisaient ce service ont également été affectées. Le retour à un fonctionnement nominal a pu prendre jusqu'à plusieurs mois pour certains clients français.

Toutefois, les conséquences économiques du conflit, plus spécifiquement dans le secteur de l'énergie, appellent à une vigilance particulière de la part de l'ensemble des organisations du secteur, des opérateurs d'importance vitale aux sous-traitants, aux prestataires et aux fournisseurs. Des actions de reconnaissance contre un terminal de gaz naturel liquéfié aux Pays-Bas ont été imputées aux MOA Kamacite et Xenotime par l'éditeur de sécurité Dragos [44]. Au regard des attaques passées mettant en œuvre ces MOA, la menace de déstabilisation au travers d'attaques par sabotage informatique paraît crédible dans ce contexte.

Le conflit russo-ukrainien a également favorisé une recrudescence de l'hacktivisme, plus particulièrement en Europe de l'Est en soutien à la Russie comme à l'Ukraine. Ces acteurs, à l'image de KillNet [45] et de Squad303 [46] ou encore de l'IT Army of Ukraine [6] agissent par le biais d'attaques DDoS ou d'exfiltration, de défigurations de sites Internet ou de divulgations de données dans le cadre d'opérations informationnelles. Leurs cibles sont variées mais se concentrent essentiellement en Europe et en Amérique du Nord. L'impact médiatique de leurs actions est souvent disproportionné par rapport au niveau de compétences mises en œuvre et à l'impact réel sur le fonctionnement de leurs cibles. Toutefois, les conséquences de ce type d'attaques pouvant provoquer l'indisponibilité de certaines ressources ou porter atteinte à l'image d'institutions ne doivent pas être négligées.

9. Opéré par l'entreprise américaine Viasat



3 → LES MÊMES FAIBLESSES SONT TOUJOURS EXPLOITÉES

A → L'EXPLOITATION DE VULNÉRABILITÉS

De nombreux incidents observés par et rapportés à l'ANSSI au cours de l'année 2022 ont pour origine l'exploitation de vulnérabilités disposant pourtant de correctifs mis à disposition par les éditeurs et ayant fait l'objet d'avis ou de bulletins d'alerte, toujours disponibles sur le site du CERT-FR. Pour les plus critiques, ces publications ont été accompagnées de campagnes de signalement.

Ces vulnérabilités concernent des logiciels particulièrement courants et utilisés par de très nombreuses organisations publiques comme privées. Certaines de ces vulnérabilités, parmi les plus exploitées, sont corrigées depuis 2021.

Avertissement : Ce classement ne comptabilise que les évènements pour lesquels l'ANSSI ou un prestataire d'investigation a pu confirmer avec un haut degré de certitude l'exploitation d'une vulnérabilité en 2022. Le nombre réel d'évènements pour lesquels l'exploitation d'une de ces vulnérabilités a été – même fortement – supposée est considérablement plus élevé. Le classement ci-dessous est donné à titre indicatif, en considérant que les occurrences avérées d'exploitation d'une vulnérabilité constituent un échantillon proportionnellement représentatif de l'ensemble.

→ LISTE DES VULNÉRABILITÉS LES PLUS EXPLOITÉES DANS LES INCIDENTS TRAITÉS PAR OU RAPPORTÉS À L'ANSSI EN 2022.

ANSSI		
CVE	**ÉDITEUR**	**RÉFÉRENCE CERT-FR**
CVE-2021-34473	MICROSOFT EXCHANGE	CERTFR-2021-ALE-017
CVE-2021-44228	APACHE	CERTFR-2021-ALE-022
CVE-2022-26134	CONFLUENCE	CERTFR-2022-ALE-006
CVE-2022-35914	GLPI	CERTFR-2022-ALE-010
CVE-2022-27925	ZIMBRA	CERTFR-2022-AVI-736
CVE-2022-41040 CVE-2022-41082	MICROSOFT EXCHANGE	CERTFR-2022-ALE-008
CVE-2021-26855	MICROSOFT EXCHANGE	CERTFR-2021-ALE-004
CVE-2021-31207 CVE-2021-34523	MICROSOFT EXCHANGE	CERTFR-2021-ALE-017
CVE-2022-22954	VMWARE WORKSPACEONE	CERTFR-2022-AVI-318
CVE-2021-34527	MICROSOFT WINDOWS	CERTFR-2021-ALE-014

IDENTIFIANT	CVE-2021-34473	DATE DE PUBLICATION	14/07/2021
ÉDITEUR	MICROSOFT	CVSS SCORE[10]	10.0

De multiples vulnérabilités ont été découvertes dans MICROSOFT EXCHANGE. Elles permettent à un attaquant de provoquer **une exécution de code arbitraire à distance** et de prendre le contrôle du serveur de messagerie MICROSOFT EXCHANGE. La technique, dénommée *PROXYSHELL* s'appuie sur l'existence de plusieurs vulnérabilités corrigées en avril et en mai 2021 [47].

10. 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 3 mesures appelées métriques : la métrique de base, la métrique temporelle et la métrique environnementale. Le score final est compris entre 0 et 10, 10 correspondant aux vulnérabilités les plus critiques. Plus d'informations sur www.first.org/cvss.

IDENTIFIANT	CVE-2021-44228	DATE DE PUBLICATION	10/12/2021
ÉDITEUR	APACHE	CVSS SCORE	9.3

Une vulnérabilité a été découverte dans la bibliothèque de journalisation APACHE LOG4J. Cette bibliothèque est très souvent utilisée dans les projets de développement d'application JAVA/J2EE. Cette vulnérabilité permet à un attaquant de provoquer une **exécution de code arbitraire à distance** s'il a la capacité de soumettre une donnée à une application qui utilise la bibliothèque LOG4J pour journaliser l'évènement [48].

IDENTIFIANT	CVE-2022-26134	DATE DE PUBLICATION	03/06/2022
ÉDITEUR	ATLASSIAN	CVSS SCORE	7.5

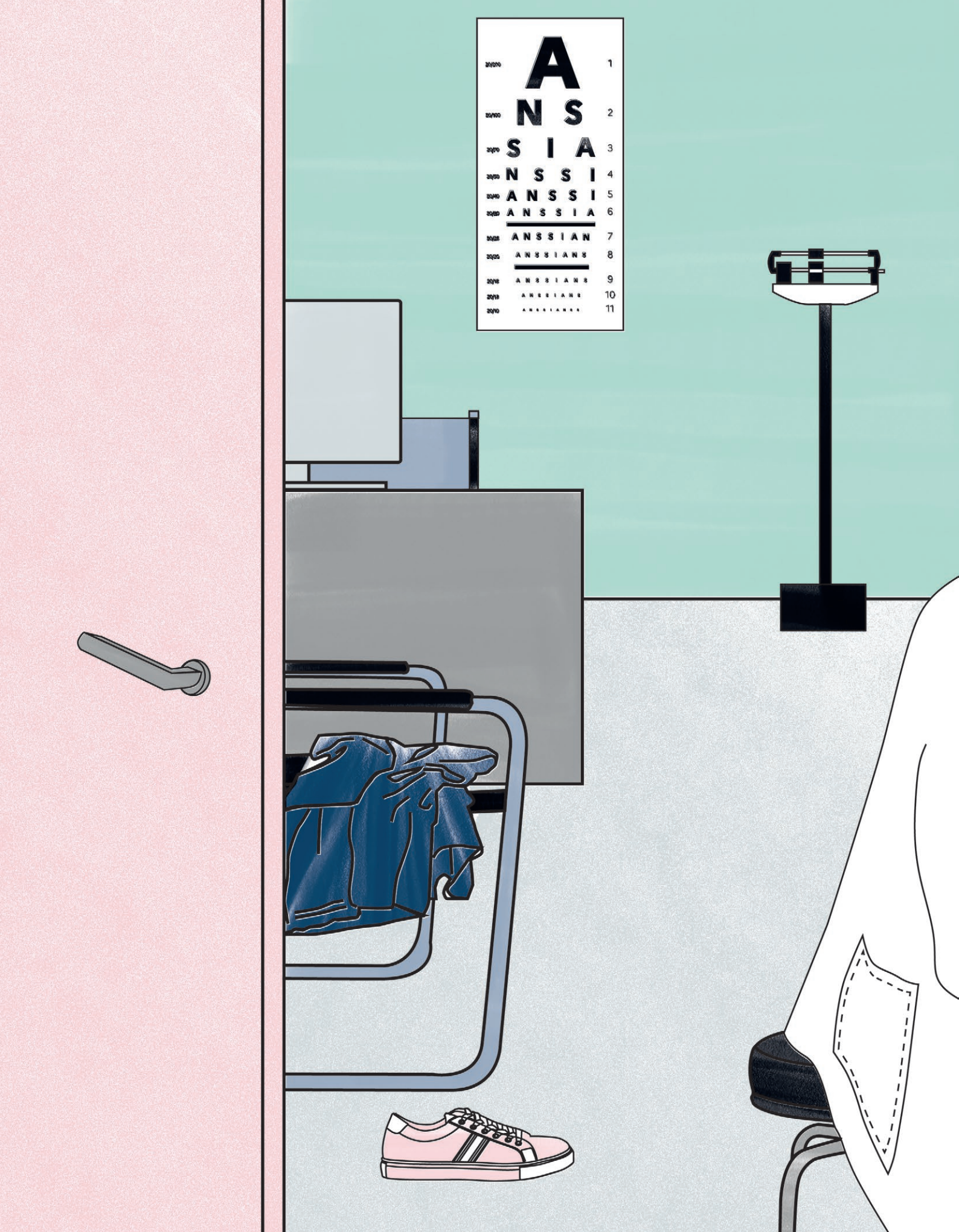
Une vulnérabilité a été découverte dans ATLASSIAN CONFLUENCE. Elle permet à un attaquant non authentifié de provoquer une **exécution de code arbitraire à distance**. Cette vulnérabilité est **exploitée par des attaquants** pour déployer différentes portes dérobées (*webshells*) afin de maintenir leur présence sur les serveurs compromis [49].

IDENTIFIANT	CVE-2022-35914	DATE DE PUBLICATION	19/09/2022
ÉDITEUR	GLPI	CVSS SCORE	9.8

De multiples vulnérabilités ont été découvertes dans la solution GLPI (GESTIONNAIRE LIBRE DE PARC INFORMATIQUE). En particulier, cette vulnérabilité permet à un attaquant de provoquer une **exécution de code arbitraire à distance** et un **contournement de la politique de sécurité**. La vulnérabilité référencée affecte une bibliothèque tierce – *HTMLAWED* – embarquée par GLPI [50].

IDENTIFIANT	CVE-2022-27925	DATE DE PUBLICATION	21/04/2022
ÉDITEUR	ZIMBRA	CVSS SCORE	7.2

De multiples vulnérabilités ont été découvertes dans ZIMBRA. La vulnérabilité référencée CVE-2022-27925 permet à un attaquant de provoquer **une atteinte à la confidentialité et à l'intégrité des données** [51].


A
N S
S I A
N S S I
A N S S I
A N S S I A
A N S S I A N
A N S S I A N S
A N S S I A N S
A N S S I A N S
A N S S I A N S

B → L'EXPLOITATION DES NOUVEAUX USAGES NUMÉRIQUES À DES FINS MALVEILLANTES

Les nouvelles technologies et les nouveaux usages qu'elles entraînent altèrent et tendent à accroître la surface d'attaque de leurs utilisateurs. Ainsi, l'ANSSI observe que le ciblage des solutions de virtualisation est devenu plus courant. Ces solutions sont particulièrement populaires pour la souplesse et la flexibilité qu'elles apportent dans la gestion des systèmes d'information. Toutefois, outre les difficultés de détection sur ces environnements, leur compromission permet aux attaquants de maintenir un accès persistant à l'ensemble des machines virtuelles gérées par l'hyperviseur[11]. En septembre 2022, les éditeurs Mandiant et VMware [52] ont indiqué que des attaquants ciblaient spécifiquement la solution de virtualisation vSphere à des fins d'espionnage pour déployer deux portes dérobées nommées « VirtualPita » et « VirtualPie ». Le ciblage des hyperviseurs est également particulièrement intéressant pour des cybercriminels opérant des rançongiciels, comme le groupe Conti [53].

Ce constat est partagé par l'ANSSI qui a traité en 2022 plusieurs incidents impliquant la compromission d'hyperviseurs VMWare. À de multiples occasions distinctes, des attaquants étatiques ont compromis un environnement vSphere en exploitant une vulnérabilité. Cet accès, atteint soit par le biais d'une console vCenter, ou en ciblant directement un ESXi, leur a permis de prendre le contrôle de l'ensemble des machines virtuelles hébergées dans l'environnement. Sans user des mêmes vulnérabilités, les acteurs cybercriminels font également preuve d'intérêt pour ces solutions. Les solutions de virtualisation étant fréquemment inclues dans l'Active Directory, les opérateurs de rançongiciels les ciblent lors du chiffrement, pour rendre rapidement indisponible un grand nombre de machines. Pour aider les victimes, l'ANSSI a mis à disposition sur le GitHub de l'agence un outil nommé DFIR4vSphere permettant de collecter des journaux et des artéfacts sur un environnement vSphere [54] à des fins d'analyse forensique.

Par ailleurs, le *Cloud Computing* et plus généralement l'externalisation de services informatiques auprès d'entreprises de services numériques (ESN) participent aussi à l'augmentation de la surface d'attaque potentielle des organisations.

Les infrastructures de *Cloud* peuvent être exploitées à des fins lucratives comme le minage de cryptomonnaies ou être intégrées à une infrastructure attaquante. Elles peuvent aussi constituer un vecteur d'intrusion efficace.

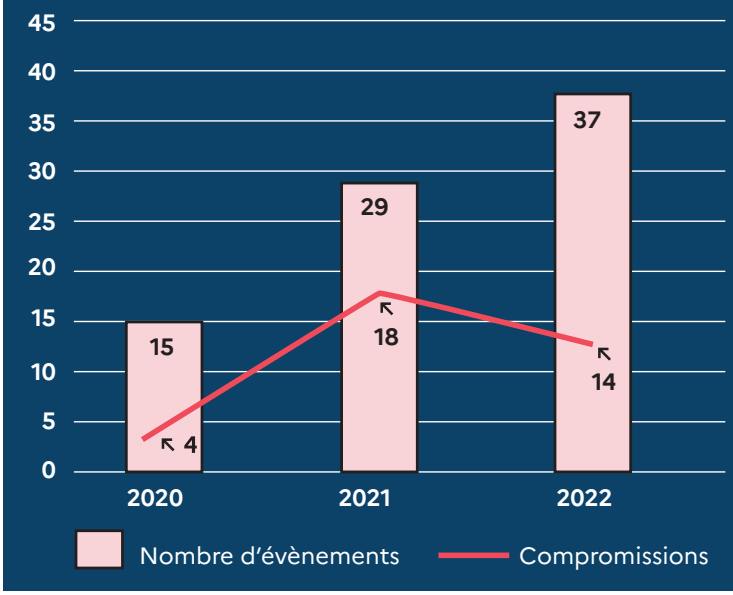
Le déploiement de solutions d'authentification unique (*Single Sign-On* - SSO) et la généralisation du *Cloud* font peser une menace croissante sur les cookies de session. Ces cookies, utilisés pour l'authentification, représentent une cible privilégiée pour plusieurs profils

d'attaquants. Ils constituent un vecteur d'intrusion ou un levier de latéralisation efficace en permettant de contourner l'authentification, y compris multifacteur. Ils sont régulièrement collectés par des cybercriminels à l'aide de *stealers* déposés sur les systèmes de leurs victimes ou lors d'opérations d'hameçonnage. Associés à des identifiants, ces cookies permettent d'accéder à des systèmes et des applications en ligne tels que des gestionnaires d'identité comme Okta, victime en mars 2022 du groupe LAPSUS$ [55]. Cette attaque avait pour origine la compromission du compte d'un ingénieur de Sitel, fournisseur de services d'Okta. Selon les dernières informations disponibles, les attaquants se seraient introduits sur le réseau de Sitel au travers de sa filiale Sykes [56]. Cette attaque illustre l'effet domino que peuvent avoir des attaques ayant pour origine la compromission d'un prestataire ou d'une filiale.

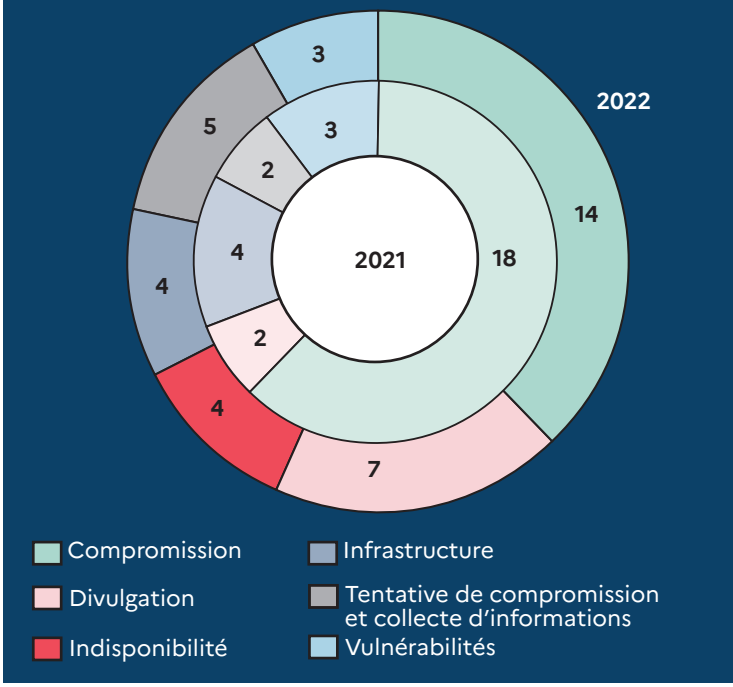
Des recommandations portant sur la politique de sécurité associée aux sessions authentifiées et le durcissement du système d'information sont disponibles sur le site du CERT-FR [57] et dans les guides publiés par l'ANSSI.

Les attaques sur la chaîne d'approvisionnement numérique ont été moins nombreuses en 2022. L'agence a également observé cette baisse. Il ressort ainsi des incidents traités par ou rapportés à l'ANSSI que les cas de compromission d'ESN ont légèrement baissé entre 2021 et 2022. Toutefois, les attaques sur la *supply chain*, qu'elles concernent un prestataire comme une ESN ou une chaîne de distribution logicielle, continuent de présenter un risque systémique, comme l'illustre le cas d'Okta évoqué précédemment ou celui de la communauté de développement Rust [7] dévoilé en mai 2022.

→ ÉVOLUTION DES ÉVÈNEMENTS TOUCHANT LES ESN DEPUIS 2020.



→ COMPARATIF DES TYPES D'INCIDENTS AFFECTANT LES ESN EN 2021 ET 2022.



11. Composant logiciel qui joue le rôle d'interface entre les machines virtuelles (VM) et le serveur hôte. L'hyperviseur contrôle l'accès aux ressources de la machine hôte et est responsable du cloisonnement entre VM. L'exploitation de vulnérabilités de l'hyperviseur peut permettre à un attaquant de compromettre l'intégralité de l'hôte et des VM qu'il héberge.

C → LES OPPORTUNITÉS OFFERTES PAR LES DIVULGATIONS DE DONNÉES

Qu'elles soient consécutives à des attaques par rançongiciel [58] ou à de la négligence [59], mises en vente par des cybercriminels [60] ou exposées dans le cadre d'opérations informationnelles associées à des revendications idéologiques ou politiques [61], les divulgations de données constituent une opportunité d'agir pour les attaquants.

Ces données peuvent être réutilisées notamment pour mener des campagnes d'hameçonnage crédible. Lorsqu'elles sont constituées d'identifiants et de mots de passe, ces informations peuvent être réutilisées directement par les attaquants. L'activation de l'authentification multifacteur permet de s'en prémunir en grande partie. À l'image des veilles sur la réputation, il convient de surveiller les divulgations de données concernant son organisation ou ses partenaires et d'appliquer les recommandations relatives à l'authentification multifacteur et aux mots de passe disponibles sur le site de l'ANSSI.

4 → CONCLUSION

→ En dépit du conflit russo-ukrainien, la menace informatique a peu évolué entre 2021 et 2022. Elle se maintient à un niveau élevé en ce qui concerne l'espionnage d'organisations publiques et privées.

L'évolution du conflit et les tensions économiques qui en résultent notamment dans le secteur de l'énergie, appellent à une vigilance de l'ensemble des organisations. Au regard de la nature des attaques informatiques menées par le passé dans le cadre de ce conflit et de l'implication des pays européens, la menace d'actions de déstabilisation et d'actions de prépositionnement est jugée crédible. Ces actions de déstabilisation peuvent prendre la forme d'attaques DDoS ou de divulgations de données orchestrées et associées à des revendications ou encore d'attaques par sabotage informatique.

La menace cybercriminelle et plus spécifiquement celle liée aux rançongiciels se maintient avec un regain d'activités remarqué en fin d'année 2022. Elle ne doit pas éluder les autres types d'activités cybercriminelles comme le cryptominage. Plus furtif qu'auparavant, il permet de générer des fonds importants qui peuvent être réinvestis par les acteurs malveillants pour acquérir de nouvelles capacités.

Si les élections présidentielles et législatives françaises de 2022 n'ont pas été l'objet d'attaque informatique d'ampleur, d'autres évènements à venir comme la Coupe du monde de rugby en 2023 et les Jeux olympiques et paralympiques de Paris 2024 représenteront des opportunités à saisir pour des attaquants aux profils variés, qu'ils soient motivés par le gain financier, l'espionnage ou la déstabilisation.

L'application rigoureuse d'une politique de mises à jour et du Guide d'hygiène informatique de l'ANSSI, une sensibilisation régulière des utilisateurs et le développement de capacités de détection et de traitement d'incident permettent de se prémunir des menaces les plus courantes.

Les récentes évolutions législatives comme la nouvelle directive *Network and Information System Security* (NIS 2) adoptée par le Parlement européen le 10 novembre 2022 et transposée en droit français d'ici septembre 2024, vont permettre de renforcer le pouvoir de supervision de l'agence en élargissant son champ d'actions à un plus grand nombre de secteurs économiques et d'acteurs publics et privés. Cette directive, qui prend en compte la problématique de la numérisation de la *supply chain,* devrait également permettre d'imposer des exigences de sécurité plus importantes aux entreprises concernées, d'induire une augmentation du niveau de maturité des organisations et ainsi de participer à réduire les risques d'attaques indirectes.

ANNEXE →
BIBLIOGRAPHIE

[1]
MINISTÈRE DES AFFAIRES ÉTRANGÈRES ET EUROPÉENNES.
8 septembre 2022.
URL : https://www.diplomatie.gouv.fr/fr/dossiers-pays/albanie/evenements/article/albanie-q-r-extrait-du-point-de-presse-08-09-22

[2]
ASSOCIATED PRESS.
Albania Cuts Diplomatic Ties with Iran over July Cyberattack. 7 septembre 2022.
URL : https://apnews.com/article/nato-technology-iran-middle-east-6be153b291f42bd549d5ecce5941c32a

[3]
BLACKBERRY.
Dirty Deeds Done Dirt Cheap: Russian RAT Offers Backdoor Bargains.
5 septembre 2022.
URL : https://blogs.blackberry.com/en/2022/05/dirty-deeds-done-dirt-cheap-russian-rat-offers-backdoor-bargains

[4]
CERT-UA.
Масована кібератака на медійні організації України з використанням шкідливої програми CrescentImp (CERT-UA#4797). 6 juin 2022.
URL : https://cert.gov.ua/article/160530

[5]
FORTINET.
Ukraine Targeted by Dark Crystal RAT (DCRat). 27 juin 2022.
URL : https://www.fortinet.com/blog/threat-research/ukraine-targeted-by-dark-crystal-rat

[6]
THE RECORD.
Russia or Ukraine: Hacking Groups Take Sides. 25 février 2022.
URL : https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/

[7]
SENTINEL ONE.
CrateDepression Rust Supply-chain Attack Infects Cloud CI Pipelines with Go Malware. 19 mai 2022.
URL : https://www.sentinelone.com/labs/cratedepression-rust-supply-chain-attack-infects-cloud-ci-pipelines-with-go-malware/

[8]
MICROSOFT SECURITY BLOG.
Looking for the 'Sliver' lining: Hunting for merging command-and-control frameworks. 24 août 2022.
URL : https://www.microsoft.com/en-us/security/blog/2022/08/24/looking-for-the-sliver-lining-hunting-for-emerging-command-and-control-frameworks/

[9]
CERT-FR.
APT31: Pakdoor, Synthèse technique.
15 décembre 2021.
URL : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-012b.pdf

[10]
MICROSFOT SECURITY BLOG.
Uncovering Trickbot's use of IoT devices in command-and-control infrastructure.
16 mars 2022.
URL : https://www.microsoft.com/en-us/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/

[11]
INTELLIGENCE ONLINE.
RCS Lab Leads new owner Cy4gate's Europen growth goals. 15 avril 2022.
URL : https://www.intelligenceonline.com/surveillance--interception/2022/04/15/rcs-lab-leads-new-owner-cy4gate-s-european-growth-goals,109768275-art

[12]
LOOKOUT.
Lookout Découverte du logiciel espion Hermit déployé au Kazakhstan.
16 juin 2022.
URL : https://fr.lookout.com/blog/hermit-spyware-discovery

[13]
GOOGLE THREAT ANALYSIS GROUP.
Spyware vendor targets users in Italy and Kazakhstan. 23 juin 2022.
URL : https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/

[14]
PEGA.
PEGA: Findings. *Parlement européen*.
14 novembre 2022.
URL : https://www.europarl.europa.eu/committees/en/pega-findings/product-details/20221114CAN67684

[15]
CITIZEN LAB.
Dark Basin Uncovering a Massive Hack-For-Hire Operation. 9 juin 2020.
URL : https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

[16]
THE BUREAU OF INVESTIGATIVE JOURNALISM.
How Qatar hacked the World Cup.
URL : https://www.thebureauinvestigates.com/stories/2022-11-05/how-qatar-hacked-the-world-cup

[17]
MEDIAPART.
Le Qatar soupçonné d'avoir ciblé Mediapart dans une opération mondiale de hacking. 6 novembre 2022.
URL : https://www.mediapart.fr/journal/international/061122/le-qatar-soupconne-d-avoir-cible-mediapart-dans-une-operation-mondiale-de-hacking

[18]
ZDNET.
Ransomware has gone down because sanctions against Russia are making life harder for attackers. 10 mai 2022.
URL : https://www.zdnet.com/article/ransomware-has-gone-down-because-sanctions-against-russia-are-making-life-harder-for-attackers/

[19]
MARIANNE.
Face à l'explosion des cyberattaques, la solution contestée du gouvernement.
27 septembre 2022.
URL : https://www.marianne.net/societe/big-brother/face-a-lexplosion-des-cyberattaques-la-solution-contestee-du-gouvernement

[20]
PARIS NORMANDIE.
Le Département de Seine-Maritime touché par une cyberattaque : les services publics « dégradés ».
10 octobre 2022.
URL : https://www.paris-normandie.fr/id349866/article/2022-10-10/le-departement-de-seine-maritime-touche-par-une-cyberattaque-les-services

[21]
VILLE DE CHAVILLE.
La Ville de Chaville victime d'une cyberattaque. 17 octobre 2022
URL : https://www.ville-chaville.fr/actualites-evenements/toute-l-actualite-77/la-ville-de-chaville-victime-dune-cyberattaque-5426. html?cHash=d24693b307b60aabf87ac7b4a08e4e4d

[22]
MIDI LIBRE.
Cyberattaque à Frontignan : les services de la mairie piratés, les hackeurs demandent une rançon. 31 octobre 2022.
URL : https://www.midilibre.fr/2022/10/31/la-mairie-de-frontignan-victime-dune-cyberattaque-et-dune-demande-de-rancon-10774268.php

[23]
20 MINUTES.
Essonne : La mairie de Brunoy visée par une attaque au rançongiciel.
2 novembre 2022.
URL : https://www.20minutes.fr/faits_divers/4008154-20221102-essonne-mairie-brunoy-visee-attaque-rancongiciel

[24]
LE MONDE.
Cyberattaque : une rançon de 10 millions de dollars réclamée au département de Seine-et-Marne. Le Monde.
17 novembre 2022.
URL : https://www.lemonde.fr/societe/article/2022/11/17/cyberattaque-une-rancon-de-10-millions-de-dollars-reclamee-au-departement-de-seine-et-marne_6150336_3224.html

[25]
CYBERSCOOP.
Latin America governments are prime targets for ransomware due to lack of resources, analysis argues. *Cyberscoop*.
16 juin 2022.
URL : https://www.cyberscoop.com/latin-america-ransomware-recorded-future/

[26]
CNN.
Cyber Command head says US has carried out a 'surge' to address ransomware attacks.
3 novembre 2021.
URL : https://edition.cnn.com/2021/11/03/politics/nakasone-ransomware-surge/index.html

[27]
BREACHQUEST.
The Conti Leaks | Insight into a Ransomware Unicorn. 9 mars 2022.
URL : https://www.breachquest.com/blog/conti-leaks-insight-into-a-ransomware-unicorn/

[28]
TIC SANTÉ.
Le coût total de la cyberattaque du CH de Dax s'est élevé à 2,3 millions d'euros (RSSI). *Tic santé*. 8 avril 2022.
URL : https://www.ticsante.com/story?ID=6141

[29]
FRANCEINFO.
L'hôpital André-Mignot du centre hospitalier de Versailles victime d'une cyberattaque. *FranceInfo*.
4 décembre 2022.
URL : https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/info-franceinfo-l-hopital-andre-mignot-du-centre-hospitalier-de-versailles-victime-d-une-cyberattaque_5522235.html

[30]
BLEEPING COMPUTER.
Costa Rica declares national emergency after Conti ransomware attacks.
8 mai 2022.
URL : https://www.bleepingcomputer.com/news/security/costa-rica-declares-national-emergency-after-conti-ransomware-attacks/

[31]
LE MONDE.
Le Monténégro, visé par une cyberattaque, appelle à l'aide internationale et accuse la Russie. *Le Monde*. 27 août 2022.
URL : https://www.lemonde.fr/international/article/2022/08/27/le-montenegro-vise-par-une-cyberattaque-appelle-a-l-aide-internationale-et-accuse-la-russie_6139205_3210.html

[32]
EUROPOL.
Internet Organised Crime Threat Assessment (IOCTA) 2021. Publications Office of the European Union, Luxembourg, 2021.
URL : https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

[33]
MALWAREBYTES LABS.
TrickBot takes down server infrastructure after months of inactivity.
MalwareBytes Labs. 28 février 2022.
URL : https://www.malwarebytes.com/blog/news/2022/02/trickbot-takes-down-server-infrastructure-after-months-of-inactivity

[34]
BLEEPING COMPUTER.
Emotet botnet starts blasting malware again after 4 month break.
Bleeping Computer. 2 novembre 2022.
URL : https://www.bleepingcomputer.com/news/security/emotet-botnet-starts-blasting-malware-again-after-4-month-break/

[35]
TREND MICRO.
Probing the Activities of Cloud-Based Cryptocurrency-Mining Groups.
Trend Micro. 29 mars 2022.
URL : https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/probing-the-activities-of-cloud-based-cryptocurrency-mining-groups

[36]
JUNIPER NETWORKS.
Log4j Attack Payloads In The Wild. *Juniper Networks*. 17 décembre 2021.
URL : https://blogs.juniper.net/en-us/security/in-the-wild-log4j-attack-payloads

[37]
THE NEW YORK TIMES.
Chinese Hackers Tried to Steal Russian Defense Data, Report Says.
The New York Times. 19 mai 2022.
URL : https://www.nytimes.com/2022/05/19/world/asia/china-hackers-russia.html

[38]
SECURITY PARROT.
Chinese hackers attack defense companies and government agencies in Russia and Eastern Europe. *Security Parrot*. 8 août 2022.
URL : https://securityparrot.com/news/chinese-hackers-attack-defense-companies-and-government-agencies-in-russia-and-eastern-europe/

[39]
POSITIVE TECHNOLOGIES.
APT31 new dropper. Target destinations: Mongolia, Russia, the U.S., and elsewhere.
Positive Technologies. 3 août 2022.
URL : https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/apt31-new-attacks/

[40]
CERT-UA.
Кібератака групи UAC-0010 (Armageddon) **на державні інституції країн Європейського Союзу** (CERT-UA#4334).
CERT-UA. 4 avril 2022.
URL : https://cert.gov.ua/article/39086

[41]
CLUSTER25 THREAT INTEL TEAM.
In the footsteps of the Fancy Bear: PowerPoint mouse-over event abused to deliver Graphite implants. *uksRise*.
23 septembre 2022.
URL : https://blog.cluster25.duskrise.com/2022/09/23/in-the-footsteps-of-the-fancy-bear-powerpoint-graphite/

[42]
GOOGLE THREAT ANALYSIS GROUP.
Update on cyber activity in Eastern Europe. 3 mai 2022.
URL : https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/

[43]
CONSEIL EUROPÉEN.
Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. 10 mai 2022.
URL : https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[44]
NL TIMES.
Russian hackers targeting Dutch gas terminal: report. 25 novembre 2022.
URL : https://nltimes.nl/2022/11/25/russian-hackers-targeting-dutch-gas-terminal-report

[45]
CBS NEWS.
U.S. airport websites knocked offline in apparent pro-Russia hacking attack. *CBS News*. 10 octobre 2022.
URL : https://www.cbsnews.com/news/airport-websites-hacked-pro-russia-ddos-attack/

[46]
THE RECORD.
'We are unstoppable': How a team of Polish programmers built a digital tool to evade Russian censorship. *The Record*. 17 mars 2022.
URL : https://therecord.media/we-are-unstoppable-how-a-team-of-polish-programmers-built-a-digital-tool-to-evade-russian-censorship/

[47]
CERT-FR.
Multiples vulnérabilités dans Microsoft Exchange. CERT-FR. 27 août 2021.
URL : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-017/

[48]
CERT-FR.
Vulnérabilité dans Apache Log4j. CERT-FR. 10 décembre 2021.
URL : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2021-ALE-022/

[49]
CERT-FR.
Vulnérabilité dans Atlassian Confluence. CERT-FR. 6 juin 2022.
URL : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-006/

[50]
CERT-FR.
Multiples vulnérabilités dans GLPI. CERT-FR. 7 octobre 2022.
URL : https://www.cert.ssi.gouv.fr/alerte/CERTFR-2022-ALE-010/

[51]
CERT-FR.
Multiples vulnérabilités dans Zimbra. CERT-FR. 31 mars 2022.
URL : https://www.cert.ssi.gouv.fr/avis/CERTFR-2022-AVI-291/

[52]
MANDIANT.
Bad VIB(E)s Part One: Investigating Novel Malware Persistence Within ESXi Hypervisors. *Mandiant*. 29 septembre 2022.
URL : https://www.mandiant.com/resources/blog/esxi-hypervisors-malware-persistence

[53]
TRELLIX.
Conti Group Targets ESXi Hypervisors With its Linux Variant. *TRELLIX*. 20 avril 2022.
URL : https://www.trellix.com/en-us/about/newsroom/stories/research/conti-group-targets-esxi-hypervisors-with-its-linux-variant.html

[54]
CERT-FR.
DFIR4vSphere : Investigation numérique sur la solution de virtualisation VMWare vSphere. CERT-FR. 22 juin 2022.
https://www.cert.ssi.gouv.fr/actualite/CERTFR-2022-ACT-027/

[55]
OKTA.
Frequently Asked Questions Regarding the January 2022 Compromise. *OKTA*. 26 avril 2022.
URL : https://support.okta.com/help/s/article/Frequently-Asked-Questions-Regarding-January-2022-Compromise?language=en_US

[56]
WIRED.
Leaked Details of the Lapsus$ Hack Make Okta's Slow Response Look More Bizarre. *WIRED*. 29 mars 2022.
URL : https://www.wired.com/story/lapsus-okta-hack-sitel-leak/

[57]
CERT-FR.
Menaces liées aux vols de cookies et contre-mesures. CERT-FR. 25 mai 2022.
URL : https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-005

[58]
RAPID7.
New Report Shows What Data Is Most at Risk to (and Prized by) Ransomware Attackers. *Rapid7*. 6 juin 2022.
URL : https://www.rapid7.com/blog/post/2022/06/16/new-report-shows-what-data-is-most-at-risk-to-and-prized-by-ransomware-attackers/

[59]
GROUP-IB.
Thousands of IDs exposed in yet another data breach in Brazil. *Group-IB*. 16 juin 2022.
URL : https://blog.group-ib.com/brazil-exposed-db

[60]
BLEEPING COMPUTER.
14 novembre 2022.
URL : https://www.bleepingcomputer.com/news/security/whoosh-confirms-data-breach-after-hackers-sell-72m-user-records/

[61]
SOCRADAR.
Hacktivist Group Black Reward Leaked Iran's Nuclear Program Secrets. *SOCRadar*. 4 novembre 2022.
URL : https://socradar.io/hacktivist-group-black-reward-leaked-iran-nuclear-program-secrets/

[62]
TREND MICRO.
Credential Stealer Targets US, Canadian Bank Customers. 17 décembre 2020.
URL : https://www.trendmicro.com/en_us/research/20/l/stealth-credential-stealer-targets-us-canadian-bank-customers.html

[63]
PROOFPOINT.
Asylum Ambuscade: State Actor Uses Compromised PRivate Ukrainian Military Emails to Target European Governments and Refugee Movement. 1er mars 2022.
URL : https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails

[64]
STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE.
25 mars 2022.
URL : https://cip.gov.ua/en/news/khto-stoyit-za-kiberatakami-na-ukrayinsku-kritichnu-informaciinu-infrastrukturu-statistika-15-22-bereznya

PANORAMA DE LA CYBERMENACE 2022 CRÉDITS

OURS

PANORAMA
DE LA
CYBERMENACE
2022

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

Direction artistique,
maquettage et illustrations
Cercle Studio (www.cerclestudio.com)

DÉPÔT LÉGAL
Janvier 2023

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

ISBN : 978-2-11-167130-0 (papier)
ISBN : 978-2-11-167131-7 (numérique)

AGENCE NATIONALE
DE LA SÉCURITÉ DES
SYSTÈMES D'INFORMATION

ANSSI – 51 boulevard de
la Tour-Maubourg
75700 PARIS 07 SP

www.ssi.gouv.fr
www.cert.ssi.gouv.fr
cert-fr@ssi.gouv.fr