InterCERT FRANCE

RAPPORT D'INCIDENTOLOGIE

Analyse d'un an de réponse aux incidents cyber

TLP:CLEAR

2026

TABLE DES MATIÈRES

TLP:CLEAR

COMITÉ DE PILOTAGE

BINETRUY Thibaud
Head of CSIRT SUEZ – Président InterCERT France

BILLON Benjamin
Responsable des partenariats opérationnels secteur privé
CERT- FR

C. Sophie
Analyste CTI
CERT-Sysdream

COSTA Haude
Directrice InterCERT France

D. Julien
Analyste CTI
CERT UBISOFT

FOUCAULT Pierre
Responsable Anticipation
CERT Bouygues Telecom

PINCEAUX Tristan
Head of CERT Almond CWATCH

RENAULT Benoit
Responsable Technique InterCERT France

ROCHETEAU Alban
Responsable CyberDefense et CyberFraude du Groupe COVEA

Le comité de pilotage remercie chaleureusement Wavestone pour la qualité de son accompagnement dans la conduite de cette étude.

ÉDITO

L'année 2025 marque un véritable tournant : elle confirme l'ancrage durable des cyberattaques, utilisées non seulement comme instruments d'action opérationnelle, mais aussi comme armes hybrides au service d'enjeux géopolitiques. Alors que la complexité croissante de la scène internationale se reflète pleinement dans le cyberespace, nous ne pouvons plus laisser le terme « cyber résilience » demeurer un simple mot-clé. Il doit devenir la ligne directrice et la doctrine d'action de l'ensemble des entreprises françaises.

Le rôle de l'InterCERT France, la communauté des CERT français, est-on ne peut plus clair dans cette période d'incertitude : il doit permettre à ses membres de communiquer, d'apprendre, et de partager les leçons tirées des expériences terrain. Cette coopération nationale, entre institutions, grands groupes et cabinets spécialisés a pour objectif de tirer chacun de ses membres vers le haut, afin que tous aient les outils et les informations nécessaires pour faire face aux menaces d'aujourd'hui et de demain.

L'objectif premier de l'InterCERT France est d'accompagner l'ensemble des CERT membres dans leur développement. C'est pourquoi, ces dernières années, nous avons mis en place :

- Une plateforme d'échange en ligne, sur laquelle nos membres partagent des informations de manière quotidienne ;
- Des évènements durant toute l'année, comme l'InterCERT Day, permettant à quiconque de se familiariser avec nos activités ;
- Des programmes d'incubation, permettant aux équipes émergentes d'intégrer l'association et de monter en compétence en se faisant accompagner par nos experts.

Aujourd'hui, l'association compte parmi elle plus de130 membres. Nous sommes fiers de pouvoir porter la voix des CERT français, et fiers de pouvoir donner à la communauté de la cybersécurité et de l'IT un point de vue unique en France et en Europe, constitué de retours, de réflexions et d'une vision construite autour du quotidien de ceux présents en première ligne.

Ce rapport présente les enseignements issus des incidents déclarés par 66 membres d'InterCERT France. Il propose une analyse statistique approfondie des événements recensés par les équipes de gestion d'incident de l'association, selon une approche distincte de celle d'autres rapports d'incidentologie tels que celui de l'ANSSI. Sa rédaction a été pensée pour être accessible à la fois aux opérationnels et aux décideurs.

Thibaud Binetruy, Président d'InterCERT France

MÉTODOLOGIE

OBJECTIF DU RAPPORT

« A travers une analyse statistique des incidents recensés par des membres de l'InterCERT France en 2025, la seconde édition de ce rapport vise à présenter les tendances observées sur l'état de la menace cyber en France et sur la manière dont les CERT y répondent. Il met également en avant les éventuelles évolutions, 2 ans après le précédent rapport. »

DÉMARCHE

La collecte de ces données, effectuée sur la période d'octobre 2025 au 27 février 2026, ainsi que la production des différents graphiques présents dans cette étude ont été rendues possible grâce à l'utilisation de l'outil "Le Sphinx", logiciel de collecte, traitement et analyse de données.

Ce questionnaire, mêlant 86 questions ouvertes et fermées, a été soumis à 129 CERT membres. Il est adapté du questionnaire du précédent rapport pour le compléter et le rendre plus exploitable pour nos analyses statistiques.
66 d'entre eux ont répondu, permettant de comptabiliser un total de 366 questionnaires.

Il est essentiel de souligner l'implication et la coopération des membres de l'InterCERT France qui ont, par leur réactivité, contribué à la représentativité de l'échantillon, une condition sine qua none à la conduite d'une telle analyse.

Ce questionnaire a été conçu pour couvrir de manière exhaustive les thématiques suivantes :

- La catégorisation de l'entreprise impactée et du CERT qui est intervenu
- La nature des incidents
- Les impacts techniques et métiers
- Les capacités d'investigation
- Les capacités de remédiation et la reconstruction

Grâce à la forte mobilisation et implication des membres de l'association, nous avons encore cette année eu accès à un échantillon de données fourni et donc exploitable, nous permettant de faire des analyses plus représentatives de la réalité.

En effet, les réponses au questionnaire nous ont permis recueillir des informations nous permettant d'analyser un total de **366 incidents** sur l'année 2025, provenant de **66 CERT français** internes, externes ou institutionnels.

Répartition des participants en fonction de leur type de CERT

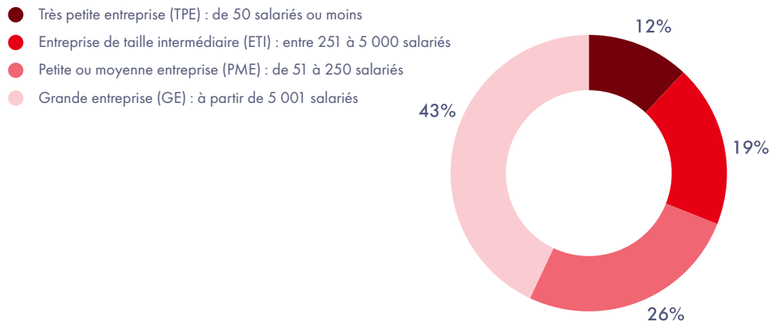
N.B : Afin de simplifier les résultats de l'étude et d'assurer la continuité des critères de mesure utilisés lors du précédent rapport, les CERT institutionnels seront considérés comme des CERT internes dans ce rapport.

PRÉSENTATION GLOBALE DES INCIDENTS

L'étude est portée cette année sur l'analyse de 366 incidents documentés par les CERT participants, en hausse de 154 incidents par rapport à 2024 malgré un nombre de répondants équivalent. Cette hausse ne reflète pas nécessairement une menace cyber plus importante en France, mais plutôt un taux de réponse plus élevé de la part des participants. Nos analyses statistiques, portant sur un échantillon plus grand que l'année du précédent rapport, sont de fait plus représentatifs de la réalité terrain..

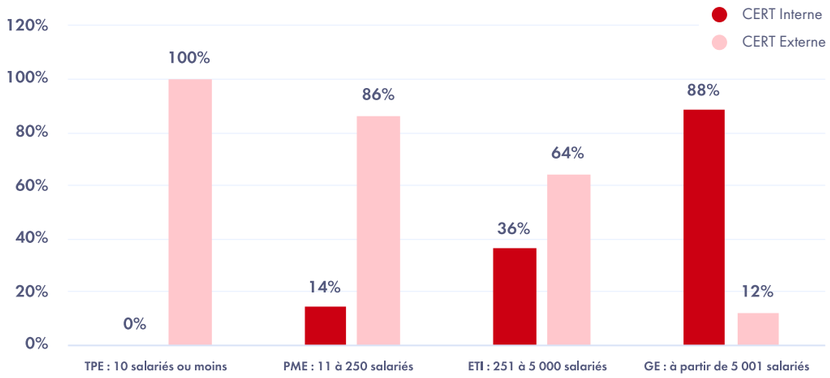
Ces incidents de sécurité visent principalement les grandes entreprises.

Répartition des incidents en fonction de la taille de l'entreprise affectée



Les plus grandes entreprises ont plus de ressources internes pour répondre en autonomie aux nombreux incidents de sécurité dont elles sont victimes. Toutefois, elles font appel à des CERT externes pour traiter les incidents les plus impactant ou complexes.

Répartition des types de CERT appelés en fonction de la taille de l'entreprise affectée



Répartition des incidents en fonction du secteur d'activité de l'entreprise affectée

Les 3 secteurs les plus touchés sont les secteurs de la santé et des actions sociales, l'industrie manufacturière et l'administration publique. Ces 3 secteurs ont vu leur nombre d'incidents recensés augmenter de l'année 2024 à 2025 : **de 13 à 80** pour le secteur de la santé et de l'action sociale **(+515%)**, **de 41 à 55** pour l'industrie manufacturière **(+34%)**, et **de 22 à 32** pour l'administration publique **(+45%)**.

BIAIS POTENTIELS

Il faut garder à l'esprit que les analyses statistiques que nous présentons dans ce rapport se basent sur un échantillon déclaratif qui nous a volontairement été communiqué par des membres de l'association. Il existe, par nature, des biais statistiques potentiels liés à cette démarche, en particulier lorsque nous réalisons des focus sur des sous-échantillons.

Par exemple, l'augmentation du nombre d'incidents rapportés dans les secteurs de la santé et de l'action publique doit être interprétée avec prudence : 74 % des signalements proviennent en réalité d'une seule et même entité, ce qui influe fortement sur la lecture globale des données. Cela témoigne d'un taux de complétion accru de la part de certains participants plutôt que d'une tendance globale sur ces secteurs d'activité.

Informations non-renseignées

Nous avons exclu de nos analyses statistiques les données non-renseignées. Ces absences de données peuvent être expliquées par un remplissage partiel du questionnaire plutôt que par une incapacité des CERT à communiquer ces informations. Il n'était donc pas forcément pertinent de prendre compte ces données dans nos analyses. La taille des échantillons sera spécifiée dans les analyses qui ne prennent pas en compte l'ensemble des réponses.

PANORAMA DES PHÉNOMÈNES CYBERCRIMINELS

TLP:CLEAR

VUE D'ENSEMBLE

Nous présentons ci après une analyse contextualisée des résultats, visant à mettre en évidence les principales tendances en matière de typologies d'attaques, en fonction du type d'organisations concernées et du type de CERT impliqué.

CIBLAGE GLOBAL

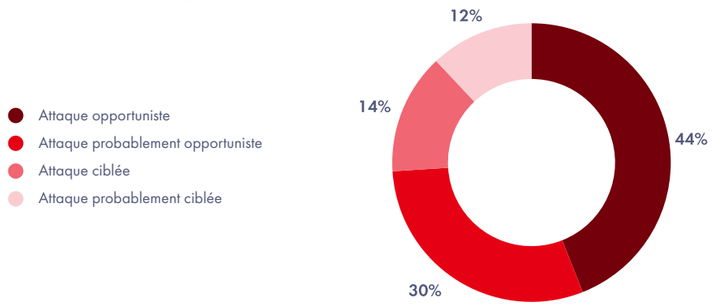
Une attaque opportuniste correspond à une opération menée à grande échelle, exploitant des vulnérabilités connues sans cibler une organisation en particulier. Souvent automatisées, massivement diffusées et faiblement personnalisées, elles reposent sur des campagnes larges cherchant à toucher un maximum de cibles potentielles.

À l'inverse, les attaques ciblées visent spécifiquement une organisation identifiée. Elles s'accompagnent généralement d'une phase préalable de reconnaissance et font l'objet d'une adaptation destinée à maximiser l'impact sur la victime.

Les attaques opportunistes demeurent largement majoritaires : les attaques ciblées ne représentent que 17 % de l'échantillon. Il convient toutefois de souligner que, dans un cas sur trois, le degré de ciblage n'a pas pu être déterminé, le plus souvent en raison d'un manque de données exploitables fournies par les CERT.

Répartition des types de ciblages dans l'ensemble du jeu de données.

Taille de l'échantillon : 247



MOTIVATION GLOBALE

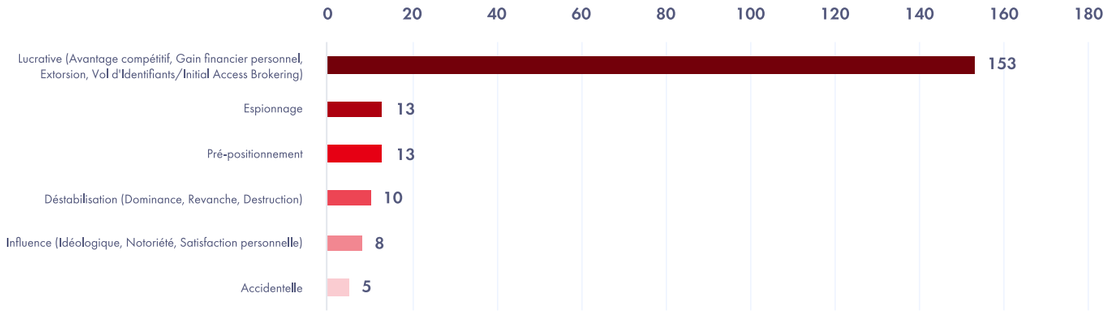
Les attaquants recherchent avant tout un gain financier.

Il est en revanche très compliqué de déterminer la motivation réelle des attaquants, qui reste inconnue dans plus d'1 attaque sur 3. C'est le cas en particulier pour les attaques non-lucratives, dont l'analyse relève plus d'enjeux géopolitiques que de l'activité d'un CERT privé.

TLP:CLEAR

Répartition des motivations sur l'ensemble des incidents.

Taille de l'échantillon : 202



NATURE GLOBALE DES ATTAQUES

Près d'une attaque sur trois vise à exfiltrer les données de l'entité attaquée.

On retrouve aussi 8% et 9% des cas d'exfiltration de données qui mènent respectivement à des usurpations d'identité et des compromissions de boîtes mail. Les attaques de ces natures sont en hausse de 40% et par rapport à 2024.

Répartition des combinaisons de nature des attaques.

Taille de l'échantillon : 530 combinaisons

	Exfiltration de données	Consultation des données	Chiffrement de données	Effacement de données	Altération de données	Indisponibilité des données	Intrusion sur le SI	Cryptominage	Défiguration	Usurpation d'identité	Compromission de boite mail
Exfiltration de données	100%	40%	30%	9%	6%	10%	40%	1%	2%	8%	9%
Consultation des données	63%	100%	33%	14%	10%	16%	60%	3%	1%	14%	13%
Chiffrement de données	56%	39%	100%	19%	3%	31%	56%	0%	0%	2%	2%
Effacement de données	59%	59%	65%	100%	18%	41%	59%	0%	0%	0%	6%
Altération de données	44%	44%	13%	19%	100%	13%	50%	0%	13%	25%	6%
Indisponibilité des données	30%	30%	49%	19%	5%	100%	46%	0%	0%	3%	3%
Intrusion sur le SI	42%	40%	32%	10%	8%	16%	100%	3%	1%	7%	9%
Cryptominage	13%	25%	0%	0%	0%	0%	38%	100%	0%	0%	0%
Défiguration	33%	17%	0%	0%	33%	0%	17%	0%	100%	17%	0%
Usurpation d'identité	21%	24%	2%	0%	10%	2%	17%	0%	2%	100%	31%
Compromission de boite mail	16%	15%	2%	2%	2%	2%	15%	0%	0%	21%	100%

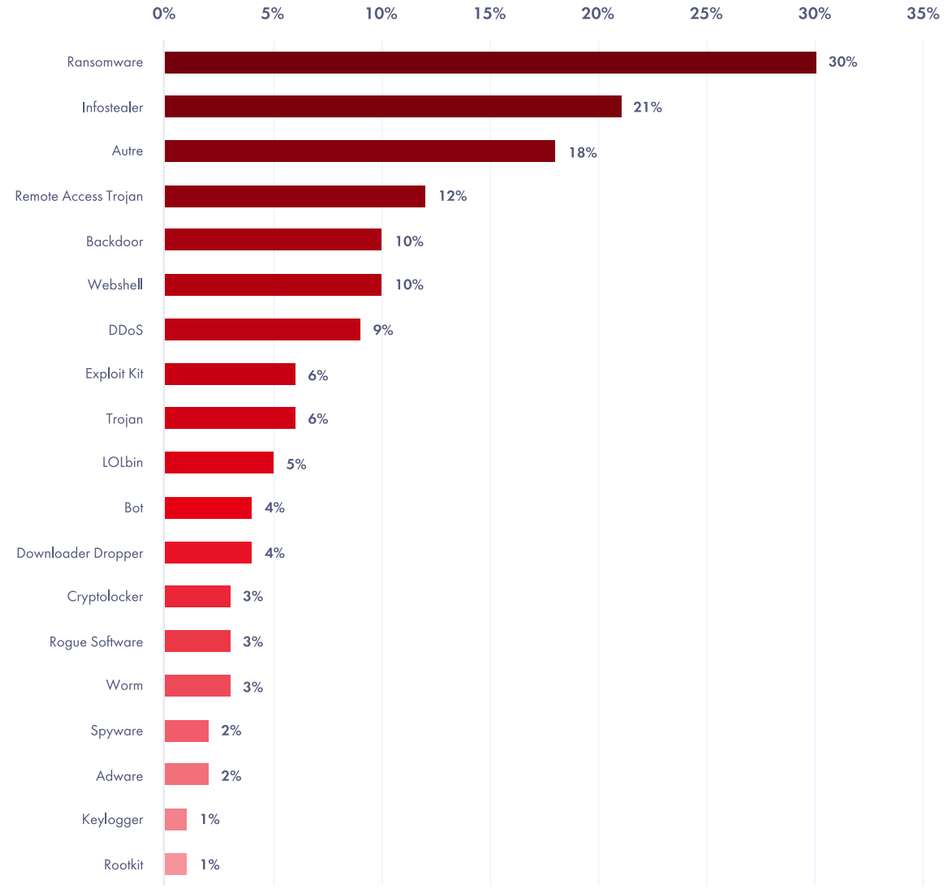
Les attaques ont le plus souvent plusieurs natures. Par exemple, l'infiltration sur le SI est très rarement une fin en soi, et s'accompagne souvent d'une exfiltration de données. Nous visualiserons plus loin dans le rapport les combinaisons de natures les plus recensées.

OUTILS

Près d'une attaque outillée sur trois utilise un type de rançongiciel.

Répartition des outil utilisés lors des attaques.

Taille de l'échantillon : 270



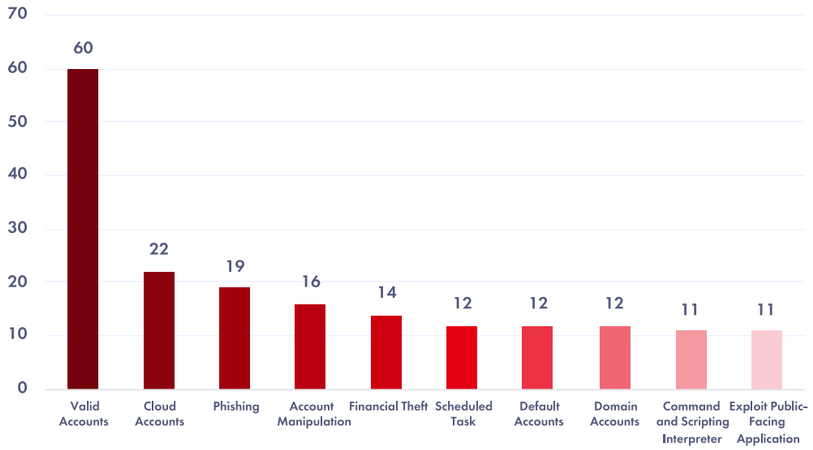
La menace des rançongiciels persiste depuis plusieurs années. On remarque que la majorité des attaques ne sont pas menées avec de nouveaux types d'outils sophistiqués ou émergeants, mais plutôt avec des outils dont l'efficacité a été prouvée durant de nombreuses années.

TECHNIQUES UTILISÉES

Le graphe ci-dessous met en évidence une prédominance des techniques de récupération de comptes parmi les techniques les plus observées dans les incidents recensés, illustrant une tendance de plus en plus présente : l'exploitation de comptes légitimes pour l'infiltration dans les entités cibles en amont d'attaques causant des dégâts importants, aussi mis en avant par la fréquence élevée d'exfiltrations de données. Ce graphe, ainsi que le nombre important d'exfiltrations de données recensées, met en avant le rôle central qu'ont les récupérations de comptes légitimes dans les attaques en 2025.

Répartition des 10 techniques les plus utilisées (format MITRE ATT&CK).

Taille de l'échantillon : 189 combinaisons



Ce chiffre demeure stable par rapport à l'année 2024 et confirme la forte dépendance des organisations à l'égard des solutions Microsoft. Les systèmes d'exploitation de l'éditeur restent en effet des cibles privilégiées pour les attaquants, qui continuent de concentrer leurs efforts sur l'exploitation des vulnérabilités propres à cet écosystème.

GRANDES TENDANCES

Cette section vient compléter la Vue d'Ensemble en apportant des éléments permettant de comparer les menaces rencontrées par les répondants selon la taille de leur entité et leur secteur d'activité.

Elle présente les informations disponibles concernant les types d'organisations ciblées, les motivations attribuées aux attaquants, ainsi que les moyens techniques qu'ils ont employés pour mener leurs actions. L'objectif est de proposer une lecture différenciée des phénomènes observés, en tenant compte des spécificités propres à chaque catégorie d'acteurs.

CIBLAGE

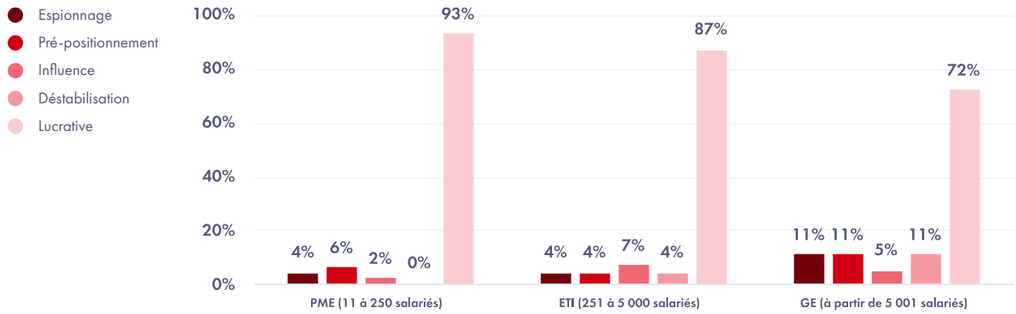
Même si la majorité des attaques sont opportunistes, on peut observer une légère augmentation de la part d'attaques ciblées chez les PMEs et les Grandes Entreprises. De plus, les natures des attaques changent selon le type de ciblage.

MOTIVATIONS

Malgré une majorité importante (72%) d'attaques lucratives, les Grandes Entreprises sont presque deux fois plus ciblées par les attaques liées à l'espionnage, l'influence et la déstabilisation que le reste des entreprises de tailles inférieures.

Distribution de la motivation en fonction de la taille de l'entreprise.

Taille de l'échantillon : 197



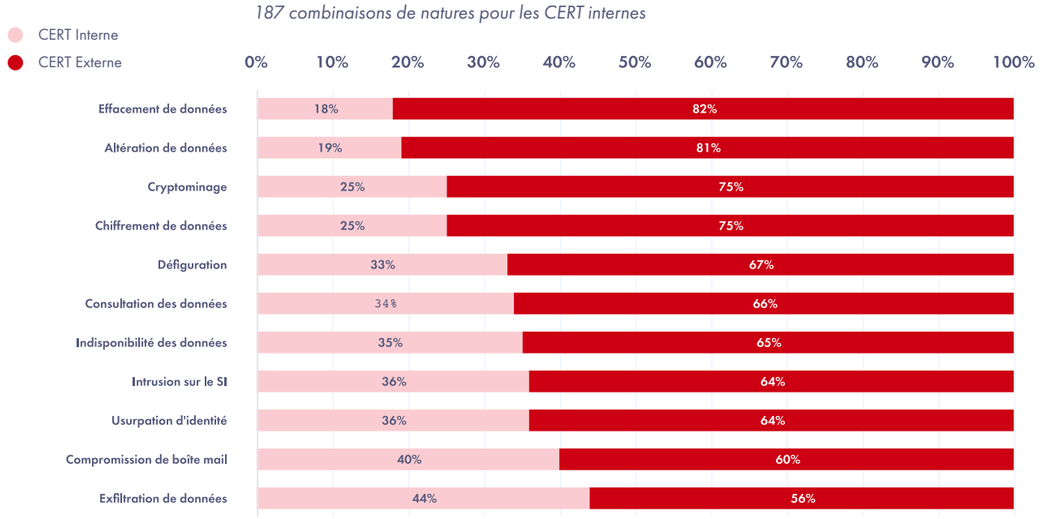
NATURE DES INCIDENTS

Le rapport entre le nombre d'interventions effectuées par des CERT internes et celui des CERT externes n'a pas évolué entre 2024 et 2025.

Les CERT externes sont très majoritairement sollicités pour intervenir sur les attaques d'effacement ou de chiffrement de données. Cette situation peut s'expliquer par le fait que les entités disposant de capacités de défense internes plus structurées parviennent généralement à détecter et à bloquer ces attaques en amont, avant qu'elles ne soient exécutées.

Répartition des types de CERT intervenus en fonction de la nature des attaques.

Taille de l'échantillon : 343 combinaisons de natures pour les CERT externes, 187 combinaisons de natures pour les CERT internes



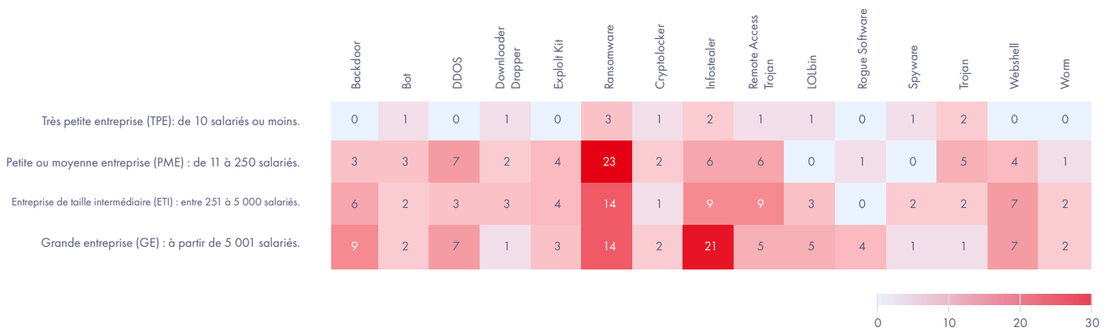
OUTILS

Les rançongiciel touchent en proportion plus les PMEs que les entreprises d'autres tailles, nous y reviendrons dans un focus dédié aux attaques par rançongiciel.

On peut voir que toutes les tailles d'entreprises subissent un nombre d'attaques par « infostealer », proportionnel au nombre d'incidents les touchant.

Répartition des types des outils utilisés en fonction de la taille de l'entreprise affectée.

Taille de l'échantillon : 238



Ce graphique met en lumière la répartition inégale des outils utilisés en fonction des secteurs d'activité de l'entreprise.

En particulier, les attaques par déni de service (« DDoS »), qui visent à rendre indisponible des services IT, ont impacté particulièrement les administrations publiques. Les motivations de ces attaques n'ont pas pu être identifiées.

L'industrie manufacturière est la principale victime des attaques opportunistes par « Webshell », qui ont eu pour impact de ralentir ou arrêter les chaînes de production.

Répartition des outil utilisés en fonction de la nature des attaques.

Taille de l'échantillon : 173 combinaisons

IMPACTS, DURÉE, RECONSTRUCTION

Nous observons des disparités dans la répartition des impacts métier en fonction de la taille des entreprises, ce qui nous permet de dégager les tendances suivantes :

- Les grandes entreprises, qui ont plus de clients, sont les principales victimes de fuite de données. Ces dernières étant mieux structurées pour répondre aux enjeux du RGPD notamment avec le rôle de DPO, elles ont une meilleure visibilité, de meilleures capacités de détection et de notification des fuites données les affectant.
- Elles sont cependant moins victimes des mails de « phishing » provenant de boites mail compromises ou de pertes de données métier. Nous pouvons justifier cette tendance par la maturité supérieure de leurs mécanismes de sécurité et de détection des environnements mail ainsi que de la forte résilience de leurs données métier, accompagné d'efforts importants de sensibilisation en interne.

On observe aussi un nombre important d'arrêts des opérations et de fuites de données chez les PMEs, qui sont souvent prises pour cible lors d'attaques visant à compromettre d'autres entités utilisant leurs services (attaque par « supply chain »). Du fait de leur gabari, elles permettent potentiellement aussi aux attaquants d'extorquer des sommes importantes, tout en évitant de se confronter à des défenses plus sophistiquées, déployées par les grandes entreprises.

Répartition des types d'impacts métiers en fonction de la taille de l'entreprise affectée.

Taille de l'échantillon : 402 combinaisons

Le nombre important d'incidents touchant les comptes administrateur, utilisateur ou de messagerie chez les Grandes Entreprises peut être expliqué par la quantité importante de ces actifs et la complexité des règles à appliquer (ex : règles relatives à la gestion des droits), nécessaires dans les organisations de ce gabari. Il est donc nécessaire que ces entités aient un système ainsi qu'une gouvernance de gestion d'identité robuste.

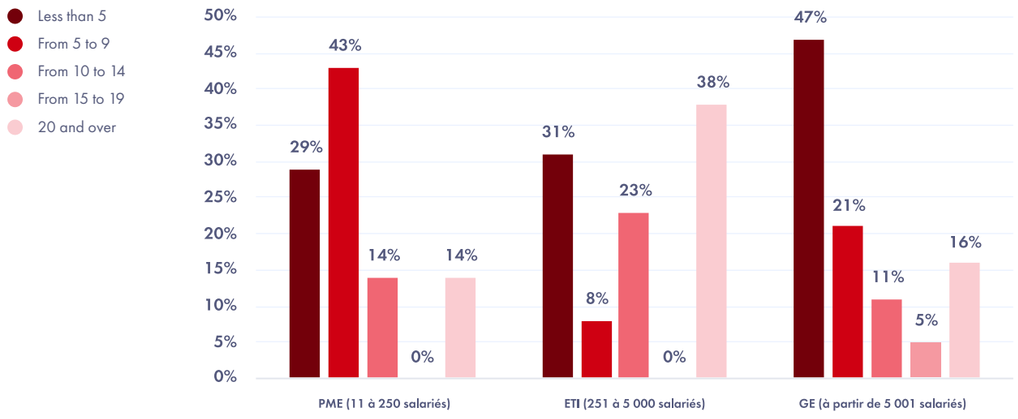
Répartition des actifs touchés en fonction de la taille de l'entreprise affectée.

Taille de l'échantillon : 512 combinaisons

Les ETIs subissent en proportion plus d'attaques qui leur impose un temps de reconstruction élevé, qui dure plus de 16 jours. Cela met en avant des processus de reconstruction moins matures que chez les grandes entreprises, avec des ressources humaines et techniques plus limitées.

Répartition de la durée de la reconstruction en fonction de la taille de l'entreprise affectée.

Taille de l'échantillon : 39 incidents



Les CERT externes interviennent globalement dans des incidents avec une durée de détection plus longue, indiquant que ces derniers interviennent lorsque les impacts de l'incidents ont déjà été observés.

TLP:CLEAR

ANALYSES CROISÉES

Cette partie du rapport se focalise sur l'analyse de l'intersection d'aspects présents dans les incidents recensés que nous avons jugé important. Ces croisements permettent de mieux exposer les détails techniques des incidents rencontrés par nos participants.

On constate une forte proportion de fuites de données associées à l'utilisation d'outils conçus pour infiltrer les systèmes d'informations des victimes en profondeur (backdoor, RATs). Ces incidents révèlent que les fuites de données ne découlent pas uniquement de l'utilisation d'outils conçus spécialisés dans l'exfiltration de données (infostealer) mais aussi d'outils permettant aux attaquants d'avoir un accès persistent et étendu. Les attaquants n'utilisent plus ces accès uniquement pour compromettre les opérations des victimes, mais aussi pour faire fuiter leurs données.

Répartition des impacts métiers en fonction des outils observés.

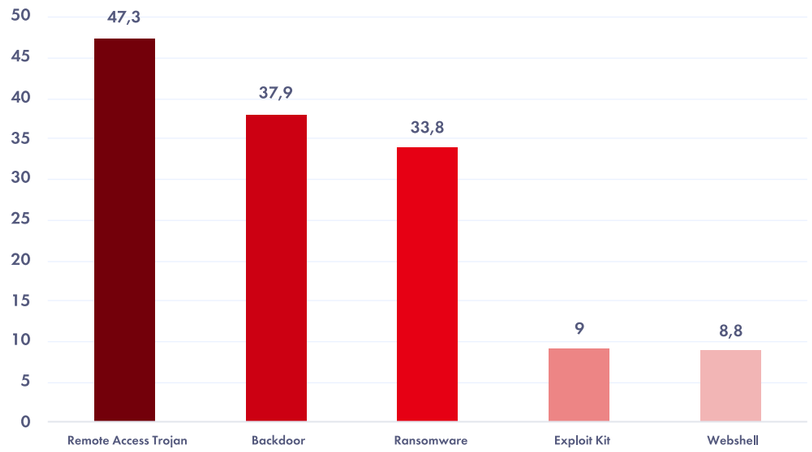
Taille de l'échantillon : 341

On observe que les outils utilisés dans les attaques menant aux temps de reconstructions les plus longs ne causent directement pas de dégâts mais permettent de récupérer des accès étendus aux infrastructures de la victime. Grace à ces accès persistants, les attaquants ont le temps de mettre au point des attaques causant des dégâts très importants sur leur système d'information.

TLP:CLEAR

Moyennes du nombre de jours de reconstruction en fonction des outils utilisés.

Taille de l'échantillon : 42



Une fois l'accès persistant à distance établi, ce sont les rançongiciels qui sont majoritairement utilisés pour déclencher les attaques.

Répartition des outils utilisés en parallèle des « backdoors » et des « Remote Access Trojans ».

Taille de l'échantillon : 54 combinaisons

ZOOM RANÇONGICIEL

Les attaques par rançongiciel (« ransomware » en Anglais) sont des attaques visant à rendre l'accès au système d'information de l'entité ciblée impossible, en y chiffrant toutes les données. À la suite du chiffrement, les attaquants contactent les responsables de l'entité victime, en leur demandant une rançon en échange de la clé de déchiffrement.

Comme nous le verrons dans cette partie, les exécutions de rançongiciels ne se limitent plus simplement aux chiffrements de données : nous observons de plus en plus d'exfiltrations de données, utilisées à des fins de chantage.

Le gouvernement déconseille fortement de payer les rançons : l'exécution d'un rançongiciel découle très souvent d'accès persistants récupérés par les attaquants. Il est donc possible que ces derniers puissent réitérer leur attaque. De plus, payer la rançon encouragerait et financerait les attaquants. Il est recommandé de déposer une plainte dans les 72h suivant la détection d'une attaque, à un commissariat de police ou sur la plateforme 17Cyber.

Le nombre d'attaques par rançongiciel recensé par l'OFAC en 2025 est de 266, en nette baisse depuis 2024 (-37%) et 2023 (-89%). Malgré cette baisse importante d'année en année, montrant que les entreprises françaises sont devenues plus matures sur la prévention et la détection de ce type d'attaques, cette menace n'en demeure pas moins persistante et évolutive. Elle exige une vigilance et une surveillance continue afin de pouvoir adapter les mesures défensives aux nouvelles techniques utilisées.

Familles de rançongiciels utilisées

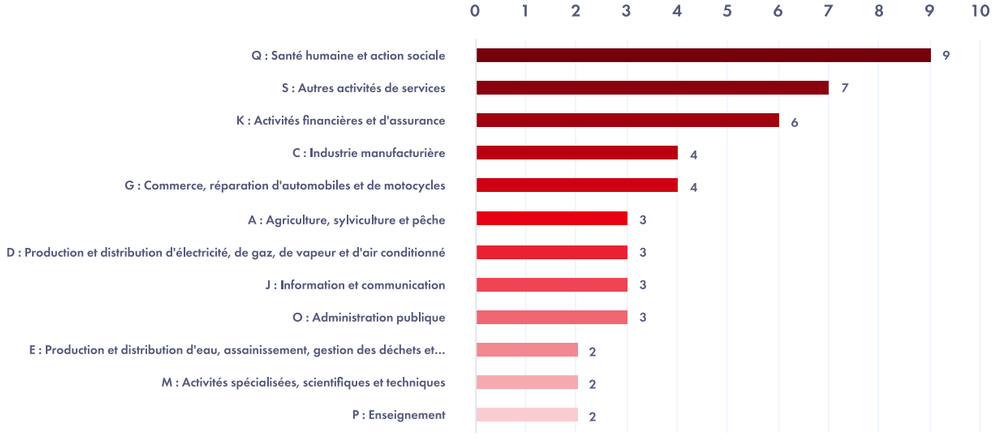
Selon le rapport de l'OFAC ainsi que le Panorama de la Cybermenace de l'ANSSI, les souches de rançongiciels les plus utilisés en 2025 sont les rançongiciels des familles « Qilin », « LockBit » et « Akira ». « Qilin » et « Akira » sont des franchises de Ransomware as a Service (RaaS) actives depuis 2022 et 2023 respectivement, et qui ont réussi, en 2025, à maintenir une clientèle fidèle et active. La franchise Qilin revendique notamment le 10 octobre 2025 une attaque par rançongiciel visant l'académie d'Amiens touchant 80% des lycées publics des Hauts-de-France ainsi que le vol de plus d'un To de données. L'ANSSI recense plus de 700 revendications d'utilisations de rançongiciels via Qilin en 2025.

PÉRIMÈTRE

Le secteur le plus touché cette année par les rançongiciels est le secteur de la santé, avec une multiplication par deux des incidents par rapport à 2024. Cette hausse est corroborée avec le Panorama de la Cybermenace 2025 de l'ANSSI, qui relève aussi une hausse significative du nombre de d'établissements de la santé touchés par les rançongiciels par rapport à 2024.

Répartition secteurs touchés par des exécutions de rançongiciels.

Taille de l'échantillon : 48

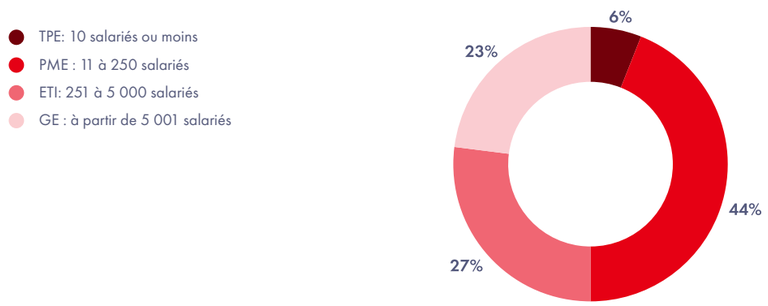


Comme en 2024, les PMEs ont été les entreprises les plus touchées par les attaques avec rançongiciel, malgré un nombre d'incidents recensés inférieur aux plus grandes entreprises. Cette tendance est aussi présente dans le rapport de l'OFAC de 2026. Cela montre un intérêt particulier des attaquants utilisant ces méthodes à attaquer ce type d'entreprise, ou une plus faible capacité à contrer le déploiement de ces derniers.

Les entreprises de cette taille sont des cibles de choix pour les attaquants utilisant les rançongiciels, suggérant que ces attaques offrent un meilleur rapport coût bénéfice que celles ciblant les grandes entreprises.

Répartition des entreprises touchées par des exécutions de rançongiciels en fonction de leur taille.

Taille de l'échantillon : 53



Les recommandations suivantes sont peu coûteuses, faciles à mettre en place, et permettent aux entreprises de se protéger contre la majorité des attaques par rançongiciel :

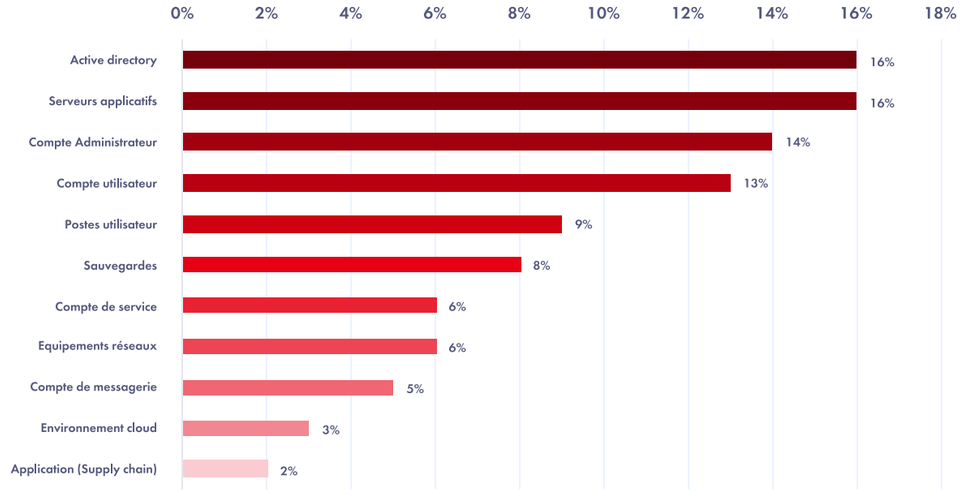
1. **Gestion d'actifs :**
   - Avoir un inventaire à jour des actifs possédés
   - Avoir une liste des actifs exposés en ligne
2. **Gestion de comptes :**
   - Maximiser la couverture de l'authentification multi facteur
   - Mettre en place la politique du moindre privilège sur tous les comptes
   - Imposer des mots de passes robustes
3. **Montée en compétence du personnel :**
   - Sensibiliser son personnel par le biais d'acteurs externes (exemple : ANSSI, services de renseignements pour les entités à intérêt sensible...)

Les outils les plus utilisés dans les attaques menant à l'exécution d'un rançongiciel sont soit des outils permettant à l'attaquant de récupérer ou de garder un accès dans l'environnement de la victime (« RATs », « backdoor », « infostealer »), soit des outils permettant l'exécution de la charge utile (« cryptolocker », « LOLBin », « downloader dropper »).

Les rançongiciels touchent en proportion similaire les actifs les plus critiques d'une organisation : « Active Directories », serveurs applicatifs et comptes administrateurs. Les attaquants cherchant le plus souvent à entraver les activités de l'entreprise victime afin de pouvoir extorquer des sommes intéressantes, ces actifs sont de facto des cibles prioritaires pour les attaquants.

Répartition des actifs touchés lors d'exécutions de rançongiciels.

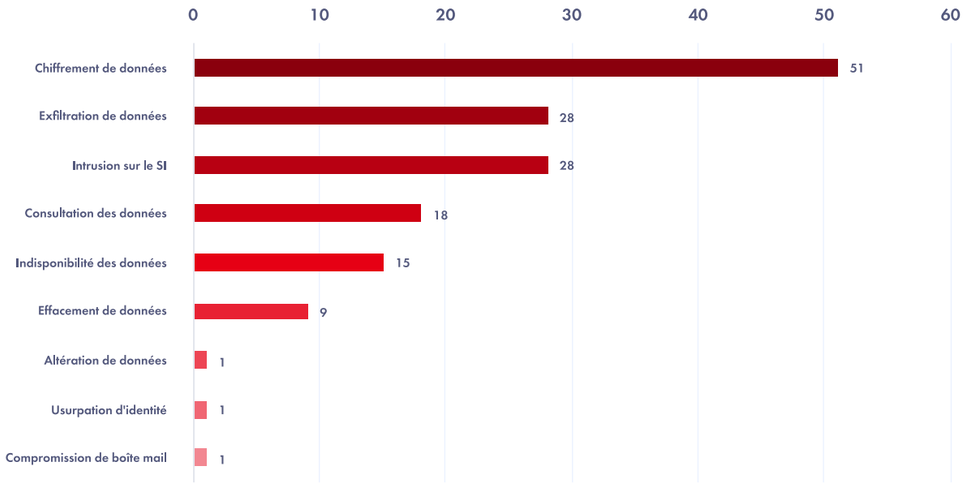
Taille de l'échantillon : 173 combinaisons



On peut observer deux leviers utilisés par les attaquants pour la négociation de leur rançon : le principal levier, utilisé depuis des années, est le chiffrement du SI, qui arrête de manière partielle ou totale les activités de l'entreprise touchée. Le deuxième cas, émergeant, est le chantage à la fuite de données.

Répartition des natures d'attaques lors d'exécutions de rançongiciels.

Taille de l'échantillon : 52 incidents

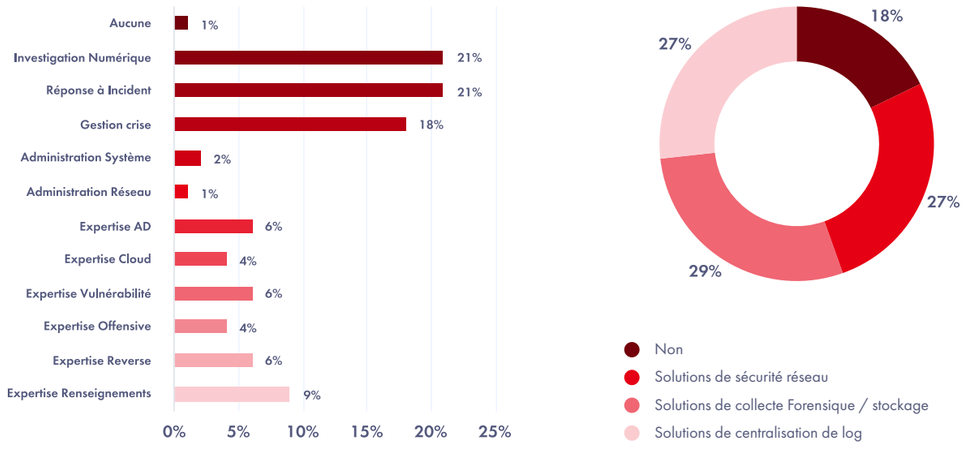


On remarque que les entreprises souffrent principalement d'un manque de compétences et de ressources matérielles pour faire de l'investigation numérique lorsqu'une attaque par rançongiciel est déployée. Pour répondre efficacement à ces crises, les entreprises font 3 fois sur 4 font appels à des CERT externes, qui sont spécialistes dans le domaine.

Les CERT externes s'appuient majoritairement sur les compétences en administration réseau et système de l'entité impactée pour remédier à la crise. Ils analysent en priorité les logs réseau et système pour mener leurs investigations.

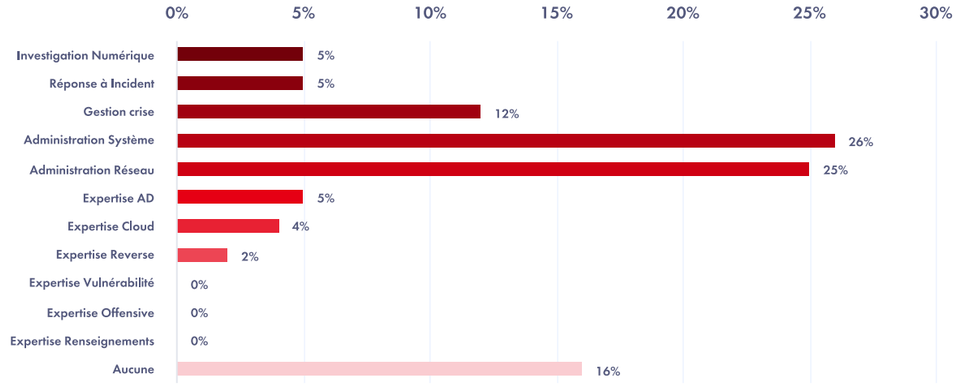
Répartition des compétences manquantes et des ressources manquantes lors d'exécutions de rançongiciels.

Taille de l'échantillon : 134 et 49



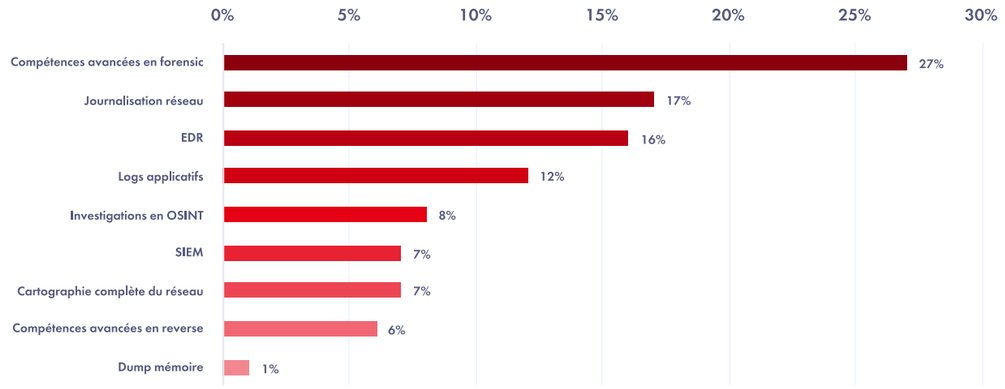
Répartition des compétences jugées comme ayant fait la différence lors d'exécutions de rançongiciels.

Taille de l'échantillon : 57 combinaisons



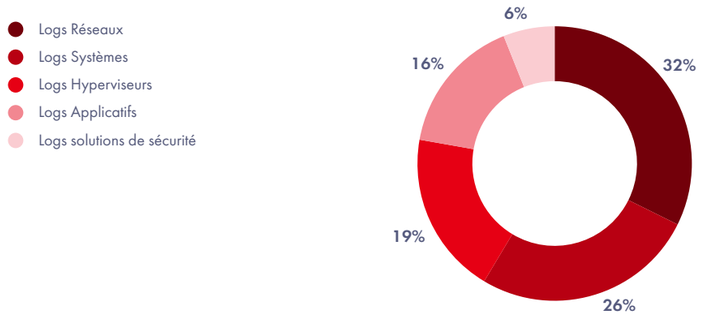
Répartition des éléments jugés utiles lors d'exécutions de rançongiciels.

Taille de l'échantillon : 101 combinaisons



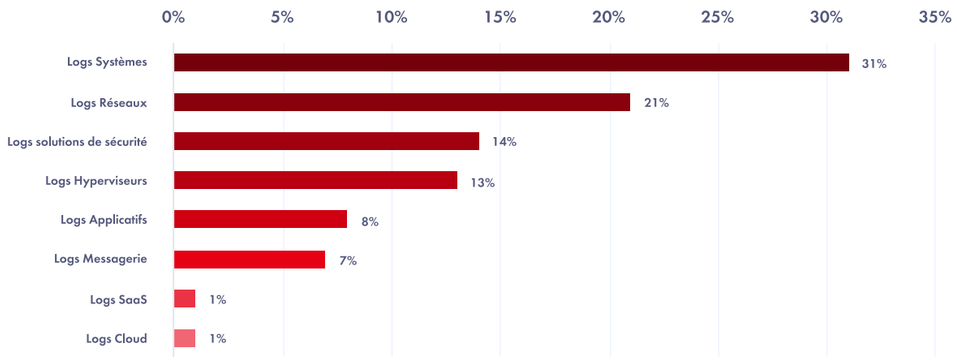
Répartition des logs manquants lors d'exécutions de rançongiciels.

Taille de l'échantillon : 31



Répartition des logs jugés comme utiles lors d'exécutions de rançongiciel.

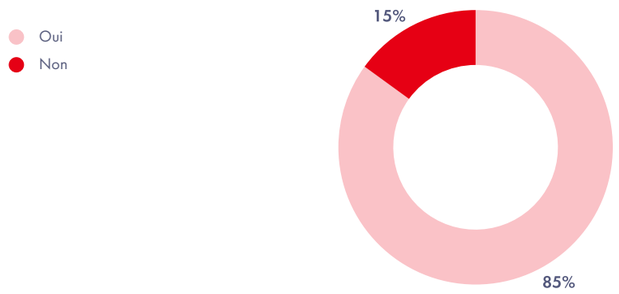
Taille de l'échantillon : 29 incidents



Les attaques par rançongiciel nécessitent dans 85% des cas une reconstruction partielle ou totale du SI de la victime, chiffre équivalent au chiffre de 2024 (86% de reconstruction sur 64 incidents). Ces attaques sont à la fois courantes et entraînent des conséquences importantes sur les entreprises affectées.

Taux de reconstruction lors d'exécutions de rançongiciel.

Taille de l'échantillon : 46



ZOOM AUTRES PHÉNOMÈNES

Parce que les incidents avec l'utilisation de rançongiciels constituent une proportion importante de notre jeu de données, nous avons décidé d'analyser les incidents impliquant d'autres types d'outils séparément. Nous ferons un focus sur les « infostealers », deuxième type d'outil le plus utilisé derrière les rançongiciels, suivi d'un deuxième focus sur les attaques non-lucratives, qui reflètent la complexité de la situation géopolitique de 2025.

FOCUS SUR LES INFOSTEALERS

Un « infostealer » est un logiciel malveillant qui permet de voler de manière discrète des données des appareils qu'il infecte. Il se dissimule souvent de manière invisible dans des logiciels qui semblent fonctionner de manière normale pour l'utilisateur. Les attaquants l'utilisent souvent dans le but de récupérer des secrets d'authentification, leur permettant de mener à bien leur attaque.

Nous observons en 2025 une hausse importante du nombre d'incidents qui utilisent un « infostealer » par rapport à nos données de 2024. Cette augmentation a eu lieu en même temps que des campagnes mondiales telles que « Clickfix » ou « Epibrowser » qui ont touché plusieurs milliers d'entreprises.

Campagnes d'« infostealers » récentes

« ClickFix » est une technique consistant à publier du contenu à sur internet, souvent sous forme de tutoriels rapides permettant de régler des problèmes informatiques communs (pilotes manquants, problèmes de performance...). Ces derniers font en réalité copier et exécuter aux victimes des commandes permettant aux attaquants de récupérer un accès à leurs appareils.

« EpiBrowser » est un faux navigateur web ressemblant fortement à Google Chrome. Lorsque la victime rentre un URL, le programme la redirige vers un vrai moteur de recherche. Le programme ne dirige pas les utilisateurs vers les URLs rentrés. Ces derniers sont souvent installés à l'insu des victimes lors du téléchargement de logiciels compromis par les attaquants.

L'augmentation importante de l'utilisation de ces technique notée par l'ANSSI dans son Panorama de la cybermenace 2025 concorde avec l'augmentation de cas avec « infostealers » observée dans nos incidents.

Recommandations :

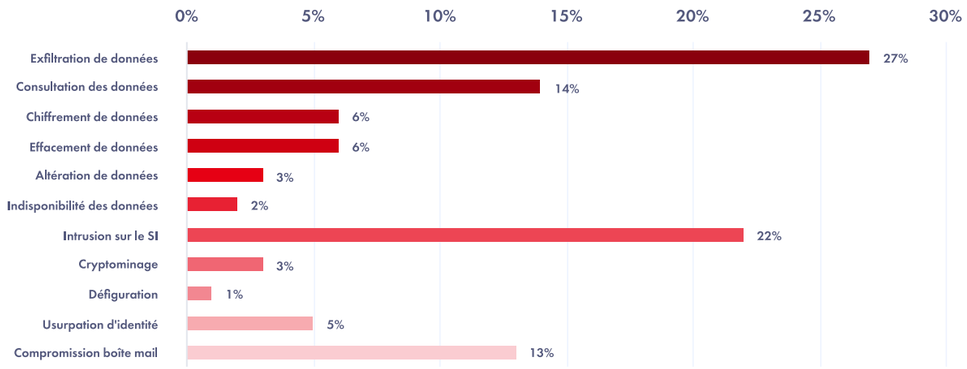
1. Interdire l'utilisation d'ordinateurs et de comptes personnels dans un cadre professionnel ;
2. Obliger l'utilisation d'un gestionnaire de mot de passe robuste ;
3. Exiger des collaborateurs de ne pas utiliser de mots de passe utilisés pour des comptes personnels.

ANALYSE

Conformément aux objectifs recherchés par l'utilisation de l'outil, la majorité des impacts lors d'incidents impliquant l'utilisation d'infostealers sont liés à la fuite ou au vol de données, voire à de la fraude (usurpation d'identité).

Répartition des natures d'attaques lors d'utilisations d'« infostealers ».

Taille de l'échantillon : 120 combinaisons

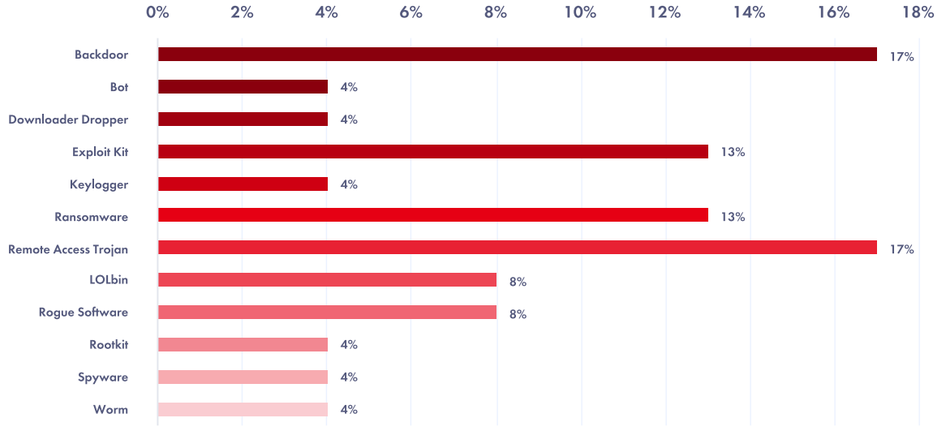


Les « infostealers » sont rarement utilisés seuls, et sont dans un cas sur trois utilisés pour déployer des outils permettant d'accéder au SI des entreprises affectées (« backdoors », « RATs »).

Dans 13% des cas, un « infostealer » est utilisé en amont de la « kill-chain » pour récupérer les accès permettant d'exécuter un rançongiciel.

Répartition des outils utilisés lors d'utilisations d' « infostealers ».

Taille de l'échantillon : 24 combinaisons



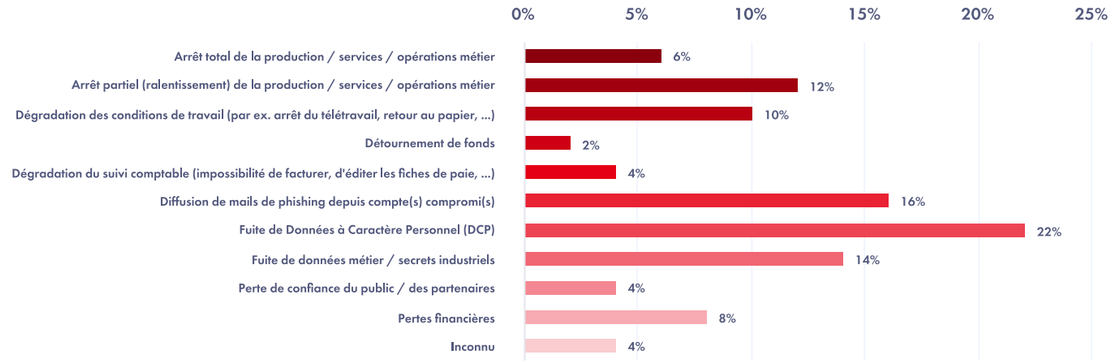
TLP:CLEAR

Les attaques durant lesquelles un « infostealer » est utilisé causent dans la majorité (36%) des cas des fuites ou des pertes de données. Ces impacts sont souvent attendus car les « infostealers » sont spécifiquement conçus pour ces tâches. Cela dit, dans 18% des incidents relevant de leur utilisation, des arrêts d'activités métier ont été observés. Ces données renforcent l'hypothèse émise dans la partie rançongiciel selon laquelle les « infostealers » sont utilisés en amont d'attaques plus destructrices.

Les attaques utilisant un « infostealer » ont aussi causé dans 13% des cas des campagnes de phishing ultérieures. Ces vols de données initiaux peuvent permettre aux attaquants de mener par la suite des campagnes de « phishing » personnalisées.

Répartition des impacts métiers observés lors d'utilisations d'« infostealers ».

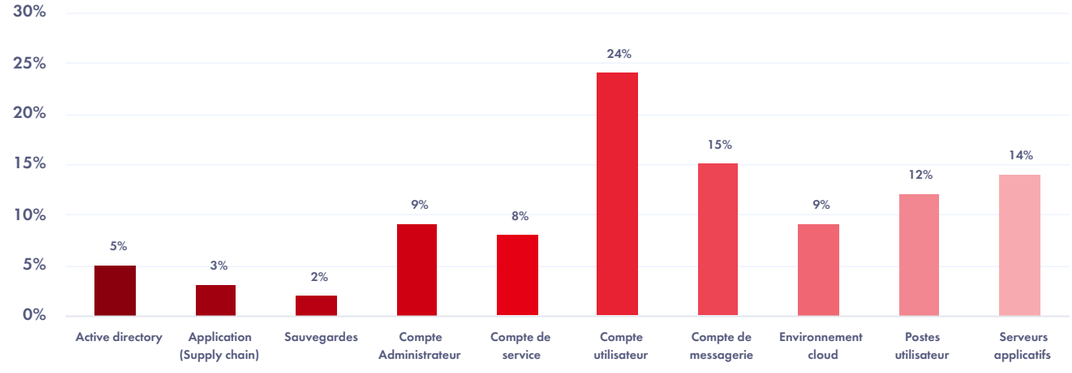
Taille de l'échantillon : 51 combinaisons



Conformément à la nature de l'outil, les actifs les plus touchés lors d'attaques utilisant des « infostealers » sont des actifs liés au stockage d'informations personnelles, tels que les comptes utilisateurs, les comptes de messagerie, ou les postes utilisateurs.

Répartition des actifs touchés lors d'utilisations d'infostealers.

Taille de l'échantillon : 51 combinaisons



TLP:CLEAR

Répartition de l'auto-évaluation de la maturité post-incident de l'entité touchée.

Taille de l'échantillon : 38

FOCUS SUR LES ATTAQUES NON-LUCRATIVES

Ce focus porte sur les attaques non-lucratives que nous avons observées dans notre jeu de données, en particulier les 4 catégories suivantes :

1. **Espionnage :** Actions consistant à infiltrer les systèmes afin d'accéder à des informations sensibles, sans être détecté.
2. **Pré-positionnement :** Actions visant à établir une présence dans un système d'information dans le but d'atteindre un objectif futur.
3. **Déstabilisation :** Actions visant à affaiblir ou paralyser une organisation.
4. **Influence :** Actions ayant pour objectif de manipuler l'opinion publique ou d'altérer la perception d'une entité.

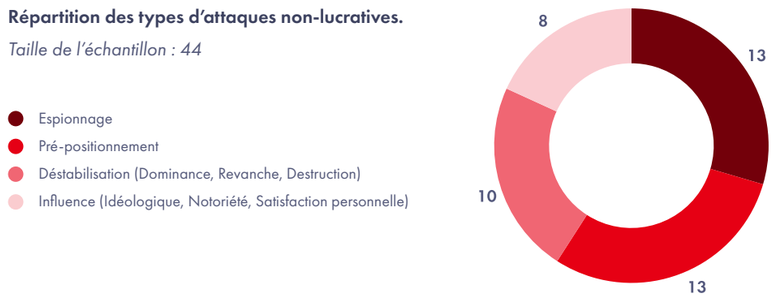
Il est très difficile pour les CERT de déterminer précisément les motivations exactes derrière les attaques non-lucratives. De plus, elles présentent un danger particulier : les acteurs, les objectifs et les impacts recherchés sont différents des attaques lucratives et peuvent être le reflet de la situation géopolitique.

Nos analyses se portent sur un échantillon de 44 incidents, un échantillon que l'on peut considérer petit par rapport à celui des attaques lucratives. Cela s'explique par la difficulté qu'ont les CERT à catégoriser les motivations derrière ces attaques.

On observe que les attaques non-lucratives sont en majorité liées à des activités d'espionnage et de pré-positionnement. Ces chiffres sont en légère baisse par rapport à 2024 malgré un contexte géopolitique tout aussi complexe. Cette différence peut s'expliquer par l'organisation des Jeux Olympiques en 2024, vus par les attaquants comme une opportunité de médiatisation mondiale.

Répartition des types d'attaques non-lucratives.

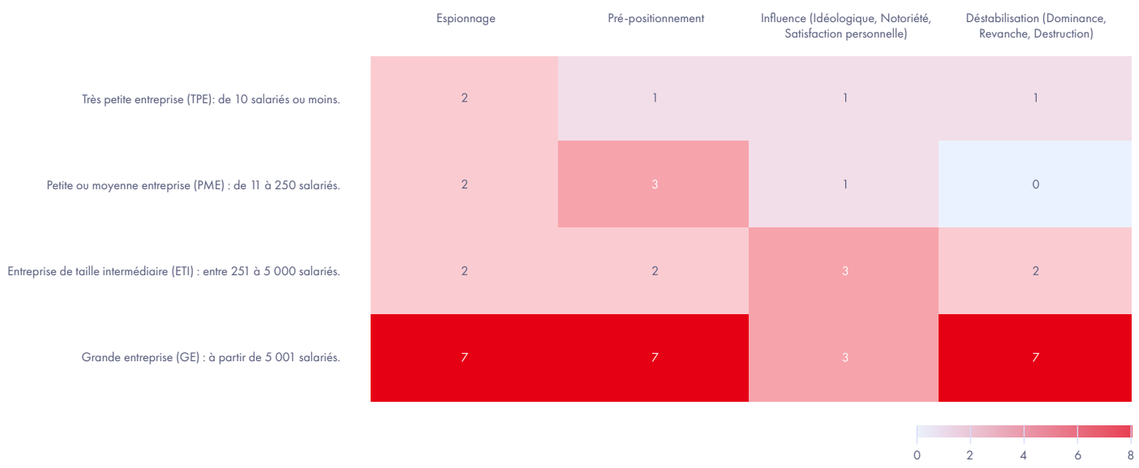
Taille de l'échantillon : 44



Les Grandes Entreprises sont les plus touchées par tous types d'attaques non-lucratives. On peut expliquer ce phénomène par le fait que les Grandes Entreprises ont plus de moyens de détection, ce qui leur permettrait de mieux identifier les motivations des attaquants que les entités de plus petite taille.

Répartition des entreprises touchées par des attaques non-lucratives en fonction de leur taille.

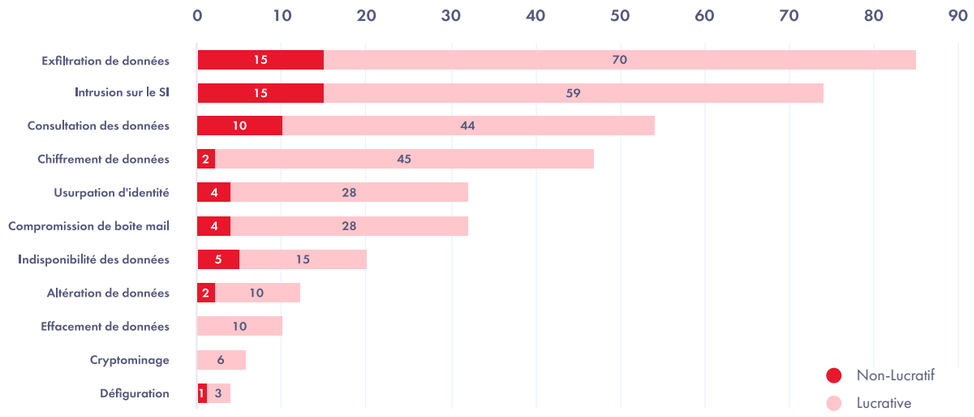
Taille de l'échantillon : 44 combinaisons



On peut voir que les natures d'attaques liées à la récupération de données représentent la majorité des attaques non-lucratives. On peut lier cette information au fait que les attaques non-lucratives seraient en majorité plutôt liées à de l'espionnage, qui vise en priorité à collecter des informations.

Comparaison de la répartition des attaques non-lucratives et lucratives en fonction de leurs natures.

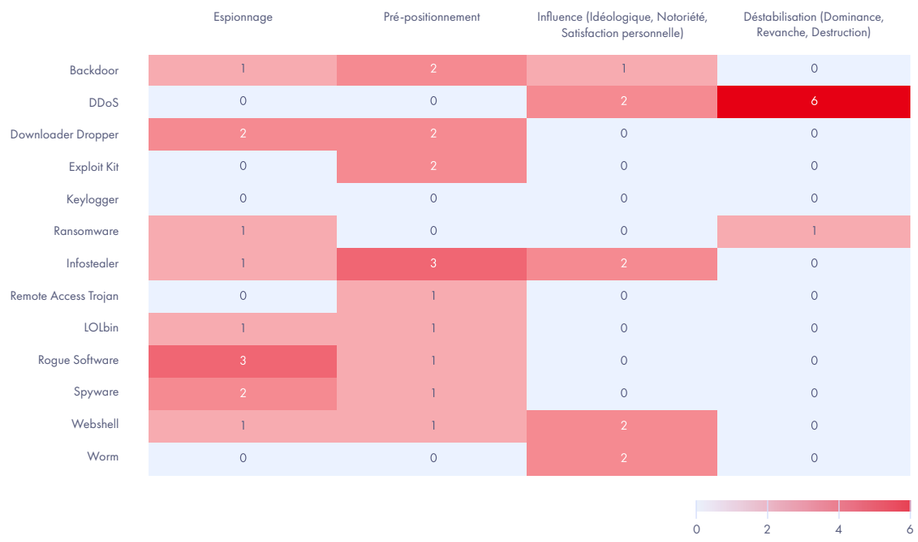
Taille de l'échantillon : 58 combinaisons non-lucratives, 318 lucratives.



La majorité des attaques motivées par la déstabilisation ont été menées via des attaques par déni de service (DDoS), tandis que les « infostealers » sont en majorité utilisés à des fins de pré-positionnement. Cette donnée est corroborée avec notre analyse précédente, qui montre que les « infostealers » sont utilisés en amont des kill-chains d'attaques visant à causer des dégâts importants.

Répartition des outils utilisés en fonction du type d'attaque non-lucratif.

Taille de l'échantillon : 42 combinaisons.



Les impacts liés aux fuites de données (fuite de données à caractère personnel, diffusion de mails de « phishing ») sont les impacts les plus observés. Dans un contexte géopolitique de plus en plus complexe, les acteurs étatiques sont poussés à mener des actions dont l'objectif est de créer des impacts sur un périmètre limité afin d'appliquer une pression constante sur les entités visées. Ces fuites sont un moyen efficace d'y arriver et permettent aussi de décrédibiliser les victimes. Elles sont souvent médiatisées et revendiquées, et peuvent être utilisés comme des moyens permettant d'accroître la popularité de groupes d'attaquants.

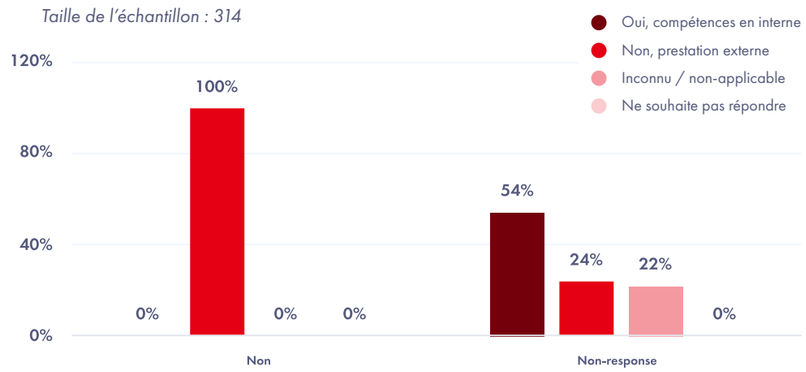
Répartition des impacts en fonction du type d'attaque non-lucratif.

Taille de l'échantillon : 32 combinaisons.

Constat : plus de la moitié des entités touchées par des attaques non-lucratives avaient les compétences en interne afin de gérer l'incident. Les Grandes Entreprises étant celles qui sont en majorité touchées par ces attaques, il est normal de voir qu'elles ont plus de moyens internes pour y répondre.

Répartition de la présence des compétences nécessaires avant l'incident pour les attaques non-lucratives.

Taille de l'échantillon : 314



RECOMMANDATIONS

Les tendances statistiques observées dans ce rapport mettent en lumière la nécessité d'organiser sa ligne de défense cyber en interne afin de limiter plus efficacement les impacts des activités malveillantes.

Pour se faire, il est important de prévoir des ressources matérielles et humaines permettant de faire face à la menace cyber qui pèse sur votre organisation.

En complément, les CERT externes permettent d'apporter une expertise supplémentaire pour répondre aux crises les plus complexes et impactantes.

Nos CERT membres recommandent de prioriser les sujets suivants afin de limiter au maximum la vulnérabilité de votre organisation :

Sécurisation des identités :

Comme nous l'avons observé, l'exploitation de « valid accounts » est la technique la plus utilisée pour compromettre une organisation en 2025. Il est primordial d'imposer une authentification à multiples facteurs pour limiter l'exploitation de secrets d'authentification compromis. Les privilèges liés aux identités doivent être restreints au strict minimum et revus dans le temps, pour restreindre les impacts d'une identité compromise. En complément, une supervision de l'utilisation des identités doit être mise en place pour alerter lorsque des comportements inhabituels sont détectés.

Sauvegardes pour la reconstruction :

Après avoir établi une persistance dans le système d'information de leurs cibles, l'outil le plus fréquemment déployé par les attaquants dans les incidents que nous avons recensés sont les rançongiciels. Dans ce contexte, des sauvegardes fiables et actualisées deviennent un élément essentiel pour :

- **Accélérer la reconstruction du SI** en restaurant les données et les systèmes critiques, ce qui vous permet la reprise des activités métier sans céder aux demandes des attaquants ;
- **Evaluer l'ampleur des fuites de données :** ces dernières étant prévalentes dans les natures des attaques recensées, les sauvegardes vous permettront :
  - **D'évaluer l'ampleur des fuites et d'identifier les données compromises** en cas de fuite avérée ;
  - **Vérifier la véracité des revendications** des groupes cybercriminels.

L'EDR, pilier de la détection :

Un EDR vous permet d'avoir une visibilité sur l'ensemble des trafics des appareils de votre SI. C'est l'outil de première ligne qui vous détectera et bloquera les comportements anormaux. Il est crucial de l'intégrer à l'ensemble de votre SI, que ce soit pour protéger votre entité activement, ou pour vous fournir assez d'information après une cyber-attaque pour identifier les attaquants et reconstruire votre SI. Nous vous conseillons de :

- **Couvrir l'ensemble de votre SI.** Cela vous permettra de bloquer et de détecter tout comportement anormal sur l'ensemble des appareils de votre SI ;
- **Corréler les logs de votre EDR avec ceux de vos autres actifs :** centraliser et croiser les logs de votre EDR avec ceux de votre pare-feu ou de votre Active Directory peut vous permettre de mieux détecter les attaques et réduire le nombre de faux positifs.

Sensibilisations, formations :

Les vecteurs de compromission les plus utilisés dans les attaques recensées sont des techniques visant à récupérer ou à exploiter des comptes valides. Ces méthodes ne se limitent pas à la compromission d'actifs dans les systèmes d'information des victimes, mais incluent aussi l'exploitation de failles humaines à l'aide de l'ingénierie sociale. Les techniques comme l'« hameçonnage » (phishing en anglais) incitent vos collaborateurs à divulguer involontairement leurs identifiants, et ce, sans que les attaquants n'aient besoin d'infiltrer votre SI. Dans un contexte où les attaquants commencent à améliorer leurs techniques à l'aide de nouvelles technologies, il est impératif :

- **De sensibiliser et de former les collaborateurs** aux bonnes pratiques (vigilance, gestion d'identifiants, ne pas utiliser d'appareils personnels...) et aux techniques utilisées par les attaquants ;
- **D'avoir un outillage robuste** (outils de détection, gestion d'identité, MFA...) et de l'imposer à ses collaborateurs.

La séparation des appareils personnels et professionnels :

la prévalence d'exfiltrations de données présentes dans les incidents recensés peut laisser penser que les fuites les plus critiques ne proviennent uniquement de votre organisation. Il est essentiel de garder en tête que les fuites externes peuvent également compromettre votre entité si vos collaborateurs réutilisent leurs identifiants ou s'ils utilisent leurs comptes professionnels pour des activités personnelles. Pour limiter ces risques, il est crucial de mettre en place :

- **Une séparation des comptes :** Interdire de l'utilisation de comptes professionnels dans d'autres contextes ;
- **Une séparation des mots de passe :** Interdire la réutilisation des mots de passe et l'obligation d'utiliser un gestionnaire de mot de passe robuste ;
- **Une séparation des appareils :** Interdire l'utilisation d'appareils personnels à des fins professionnels, et vice-versa.

InterCERT
FRANCE

InterCERT France
Campus Cyber, Tour Eria
5-7 rue Bellini
92800 PUTEAUX
contact@intercert-france.fr
07 52 08 04 21

Conception graphique www.aurelielegrand.fr