InterCERT FRANCE

RAPPORT D'INCIDENTOLOGIE

ANALYSE D'UN AN DE RÉPONSE AUX INCIDENTS CYBER

2024

TLP:CLEAR

TLP:CLEAR

Table des matières

COMITÉ DE PILOTAGE

NGUYEN Vincent
Responsable du CERT Stoïk

DE NOMAZY Capucine
Cybersecurity Senior Consultant
CERT Wavestone

FOUCAULT Pierre
Analyste CTI
CERT Bouygues Telecom

DEGRUGILLIER Cécile
Responsable publication CTI
CERT Société Générale

D. Julien
Analyste CTI
CERT Sysdream

LE BASTARD Frédéric
Président InterCERT France
Responsable du CERT La Poste

COSTA Haude
Directrice InterCERT France

LOUIS-SIDNEY Barbara
Responsable du CERT OWN

PINCEAUX Tristan
Head of CERT CWATCH
CERT Almond

BAUDEAU Gregory
CTI Expert
CERT Groupe Safran

BERNI Olivier [1]
CERT Société Générale

GUIHEUX Tristan [2]
CERT La Poste

GIRALT Martine
Vice présidente InterCERT France
Program Manager Cert-IST

RIEUNIER Christophe
Expert Cyber
CERT La Poste

Le comité de pilotage remercie Jeanne Mazelier  , Cheffe de projet, pour sa contribution essentielle au rapport

1 Responsable du CERT Société Générale au moment de l'analyse de l'étude. Olivier Berni occupe désormais le poste de Directeur des Opérations de Cyberdéfense chez Capgemini

2 Responsable adjoint du CERT La Poste, il occupe aujourd'hui le poste de RSSI du groupe Manitou

ÉDITO

La communauté des CERTs a pour vocation de renforcer la capacité de chacun de ses membres à détecter et à répondre aux incidents de sécurité impactant leurs périmètres.

En ce sens, en tant qu'organisme représentatif, la raison d'être de notre association réside dans le partage de bonnes pratiques associé à la promotion active de la collaboration et de l'échange d'informations entre les CERTs français.

Les membres d'InterCERT France échangent au quotidien sur notre plateforme de communication MeMic, en présentiel deux fois par an lors des InterCERT Days, lors des Matinales qui se tiennent en distanciel tous les deux mois ou encore dans le cadre de formations, d'atelier et de groupes de travail divers.

Par l'animation de cette communauté de confiance, nous contribuons à la diversification du traitement des thématiques de sécurité numérique et à l'amélioration de la coopération entre acteurs de la sécurité numérique.

Par ailleurs, l'une des activités principales de l'association demeure l'accompagnement du développement des CERTs. InterCERT France œuvre pour sensibiliser les acteurs de la sécurité numérique sur l'importance des actions menées par ses membres et à faciliter leur mise en place. En favorisant l'émergence de CERTs performants et en les intégrant à notre réseau solide d'experts et de professionnels de la réponse sur incidents, nous agissons en faveur d'échanges plus opérationnels, de la diffusion d'une culture de partage et du développement de la résilience de ses membres.

Enfin, nous avons pour ambition d'incarner la voix des CERTs français auprès des décideurs informatiques : InterCERT France entend, par la diffusion de ses productions, porter et diffuser la parole distincte des CERT, contribuer à une démystification des activités de ces derniers et ainsi promouvoir les retours et recommandations d'acteurs présents sur le terrain.

C'est dans ce cadre que s'inscrit ce premier rapport d'incidentologie.

Dans un contexte où les menaces cyber se multiplient et se diversifient, il est crucial pour les entreprises et les organisations de disposer de données précises et exhaustives sur les incidents de sécurité réellement traités par les équipes de réponse aux incidents. La compréhension détaillée de ces incidents permet non seulement d'optimiser les stratégies de défense mais aussi de renforcer les capacités de réaction et de remédiation face aux cyberattaques. Ce besoin pressant de données statistiques pertinentes et de qualité sur les incidents de sécurité justifie la mise en œuvre de cette étude. L'objectif est donc d'apporter une vision claire et structurée des attaques subies, de leurs impacts et des réponses apportées par les équipes de sécurité.

Frédéric Le Bastard, Président d'InterCERT France

MÉTHODOLOGIE DE L'ÉTUDE ET AVANT-PROPOS

L'objectif de ce premier rapport annuel d'incidents est de partager une vision statistique et contextualisée des différents incidents et crises cybers expérimentés par les membres de l'InterCERT France sur l'année 2023. Ce bilan vise à recueillir les expériences d'attaques dites "réussies" vécues par les membres de l'association sur les périmètres de leurs systèmes d'information.

Pour cela, l'association a sollicité les efforts des membres du Comité de pilotage (cf. trombinoscope) composé d'experts membres de la communauté de l'InterCERT France. Ce comité était responsable de la définition des objectifs, de la validation des outils de collecte et des méthodologies d'analyse, ainsi que du suivi des différentes phases du projet. Leur expertise a été essentielle pour s'assurer que chaque aspect de l'étude réponde aux standards les plus élevés en matière de recherche en sécurité informatique.

La collecte de ces données, effectuée sur la période du 13 octobre 2023 au 31 janvier 2024, ainsi que la production des différents graphiques présents dans cette étude ont été rendues possibles grâce à l'utilisation de l'outil "Le Sphinx", logiciel de récolte, traitement et analyse de données.

Ce questionnaire, mêlant 62 questions ouvertes et fermées, a été soumis à **95 CERT membres**. 65 d'entre eux ont répondu, permettant de comptabiliser **un total de 212 questionnaires**, soit un taux de remplissage global s'élevant à 81,8 %.

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 nature des incidents :**
  type d'attaque, vecteurs d'intrusion, techniques utilisées par les attaquants.
- **Les impacts techniques et métiers :**
  systèmes et technologies impactées, perturbations des services, conséquences financières et réputationnelles.
- **Le soutien des forces de l'ordre :**
  interactions avec les autorités, signalements et enquêtes.
- **Les capacités d'investigation :**
  moyens techniques et humains mis en œuvre pour identifier, analyser et comprendre l'incident.
- **La remédiation et la reconstruction :**
  actions correctives, restaurations de systèmes et améliorations post-incident.

Lors du choix des thématiques abordées dans ce questionnaire - par souci d'exhaustivité et afin d'éviter tout biais d'analyse - les aspects suivants ont été pris en considération :

- *L'hétérogénéité des capacités des différents membres* : les disparités de niveau de maturité face aux incidents ou encore de quantité de temps, de personnel et d'informations qui leur est alloué pour remplir ce questionnaire.
- *La notion de volontariat* : les participants à cette étude sont libres de ne partager que les informations souhaitées.

Par ailleurs, cette étude traitera uniquement des cas d'intrusion "vérifiées" par les CERT sur leurs systèmes d'information. Par conséquent, le questionnaire et son analyse ne feront pas mention des attaques par DDoS. (cf. Encart)

Le choix d'un tel parti pris n'entend pas invisibiliser l'existence de telles attaques mais plutôt refléter un choix de cadrage délibéré permettant d'axer l'analyse sur les incidents ayant un impact direct et tangible sur les systèmes et les données des organisations.

Cette étude constitue une contribution significative à la compréhension des incidents de sécurité traités par les équipes de réponse. En se concentrant sur les intrusions avérées, en utilisant un questionnaire détaillé et en bénéficiant de l'encadrement d'un comité de pilotage expert, elle offre une vision précise des défis rencontrés et des stratégies déployées. Les résultats obtenus fourniront des bases solides pour améliorer la prévention, la détection et la réponse aux incidents de sécurité, renforçant ainsi la résilience des organisations face aux cybermenaces.

212

questionnaires remplis dans le cadre de cette étude

DONNÉES SUR L'ÉCHANTILLON

Questionnaires envoyés : **95**

CERTs ayant répondu : **65**

Total de questionnaires remplis : **212**

CERTs interne : **35%** (67)

CERTs externe : **65%** (124)

Non réponses : **12%** (26)

TLP:CLEAR

SECTION 1

ÉTAT DE LA MENACE

2024

TLP:CLEAR

PANORAMA DES PHÉNOMÈNES CYBERCRIMINELS

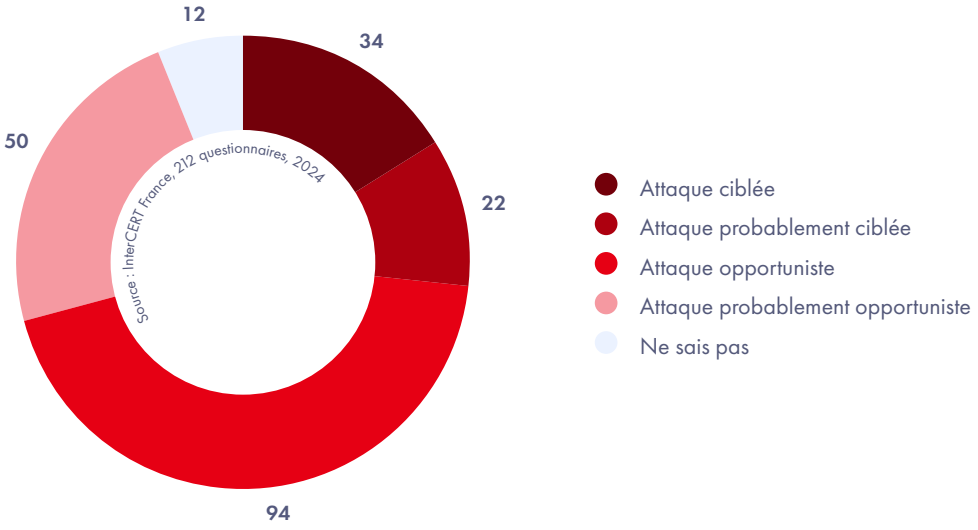
VUE D'ENSEMBLE

Prenons un peu de recul sur les incidents observés par les différents membres de l'InterCERT France. Vous retrouverez dans cette section une vue macroscopique des typologies d'incidents, motivation, outils et vulnérabilités exploité par les attaquants.

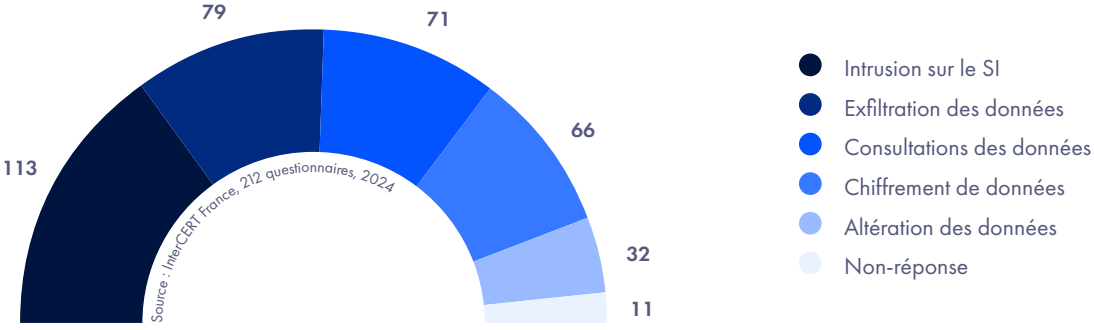
20%

des attaques sont revendiquées

Près de 3 attaques sur 4 sont menées de manière opportuniste !



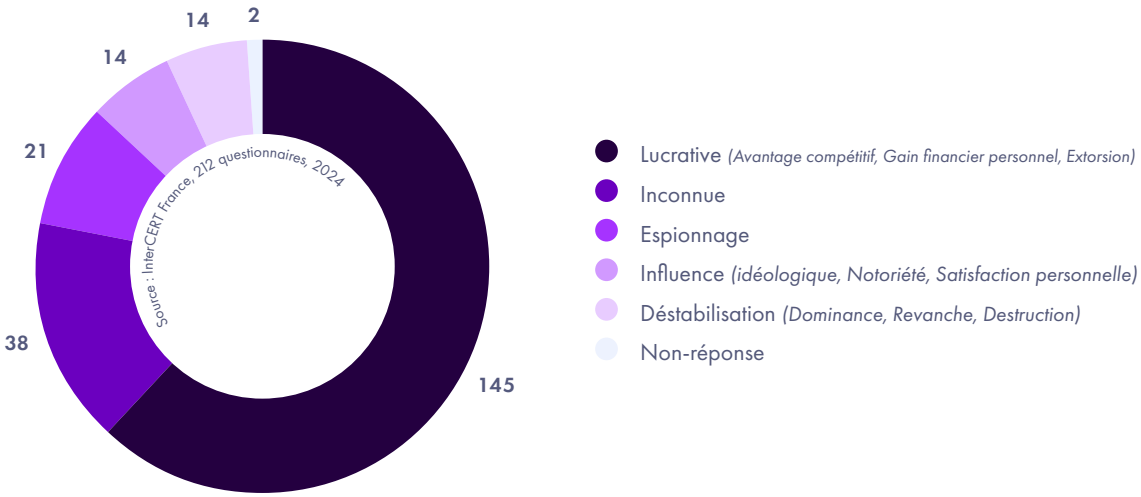
Une majorité écrasante d'attaques combinées : un chiffrement ne vient que rarement seul, il est souvent accompagné d'une exfiltration de données !



TLP:CLEAR

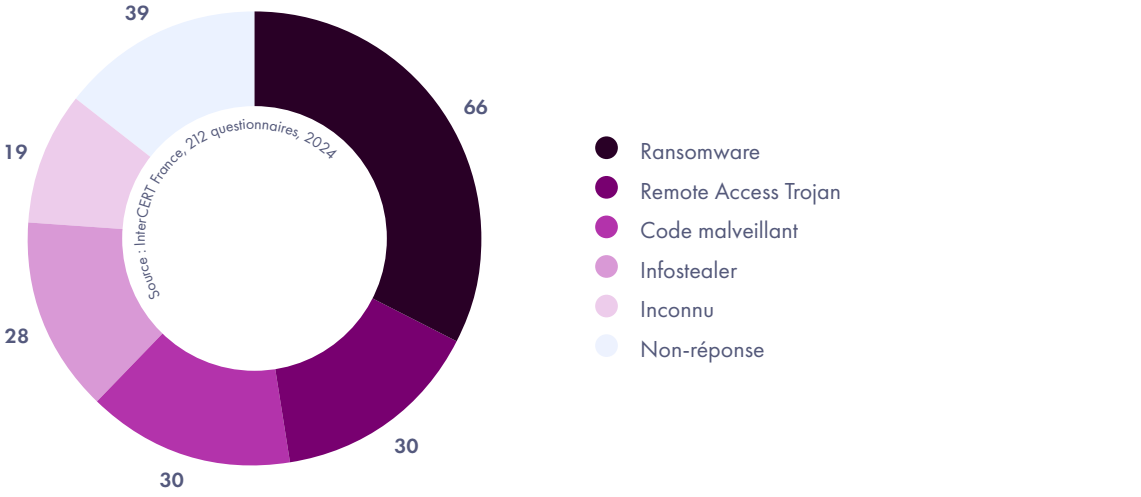
Sans aucun doute, la majorité des attaques sont conduites à des fins lucratives : l'appât du gain reste la principale motivation des attaquants. A noter tout de même que dans près de 20% des cas, il n'a pas été possible d'identifier la motivation de l'attaquant.

Principales motivations des attaquants :



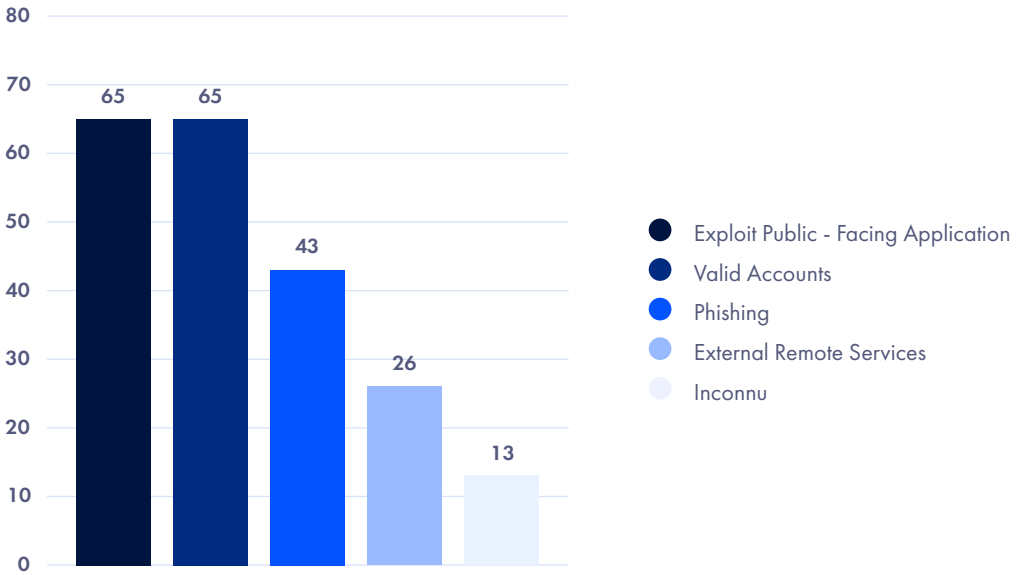
Les données de l'analyse proviennent de 188 réponses sur 217 soumises, comprenant 66 cas de ransomware, 30 incidents liés à des Remote Access Trojans (RAT), 30 cas de code malveillant, et 28 incidents d'infostealers. Les 18 réponses restantes sont classées comme inconnues, et 29 réponses n'ont pas fourni d'informations détaillées. Ces incidents révèlent un usage notable des techniques de chiffrement pour la demande de rançon (ransomware), des tactiques de contrôle à distance des systèmes compromis (RAT), et des méthodes d'exfiltration des données volées (infostealers).

Outils malveillants les plus utilisés :



Les données indiquent que les exploits d'applications accessibles publiquement et les comptes valides sont les vecteurs d'intrusion les plus prévalents, représentant environ 60% des cas rapportés. Le phishing et les services distants externes, bien que moins fréquents, soulignent l'importance de la vigilance contre les techniques d'ingénierie sociale et les accès distants non sécurisés.

Principales vulnérabilités :



Source : InterCERT France, 212 questionnaires, 2024

L'écrasante domination des infrastructures Windows dans les parcs informatiques souligne le peu de diversité au sein des SI et la très forte dépendance à certains fournisseurs, tiers et partenaires. Cette statistique reflète également la compétence développée par les attaquants qui se concentrent sur certaines briques technologiques ayant, pour eux, le plus fort ROI.

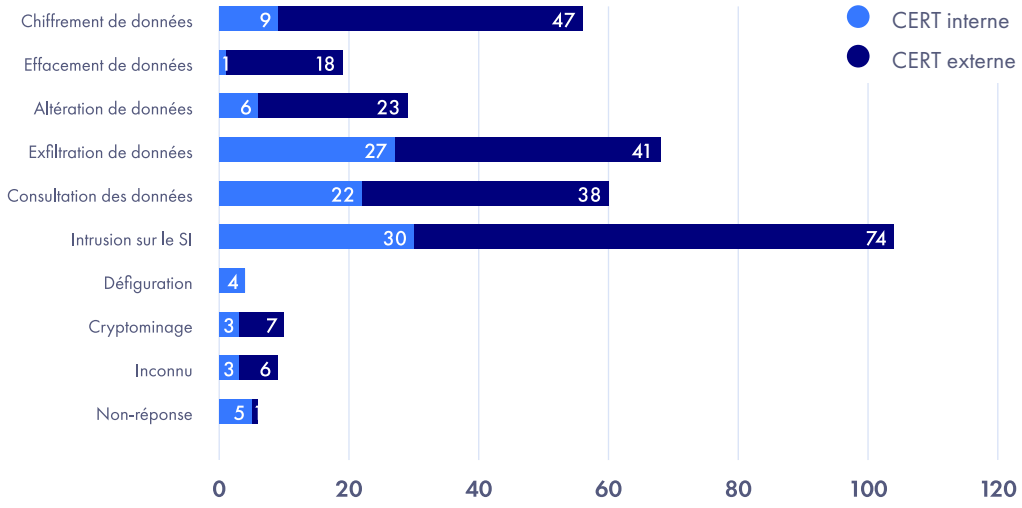
73%

de ces infrastructures compromises utilisaient un système d'exploitation Windows

GRANDES TENDANCES

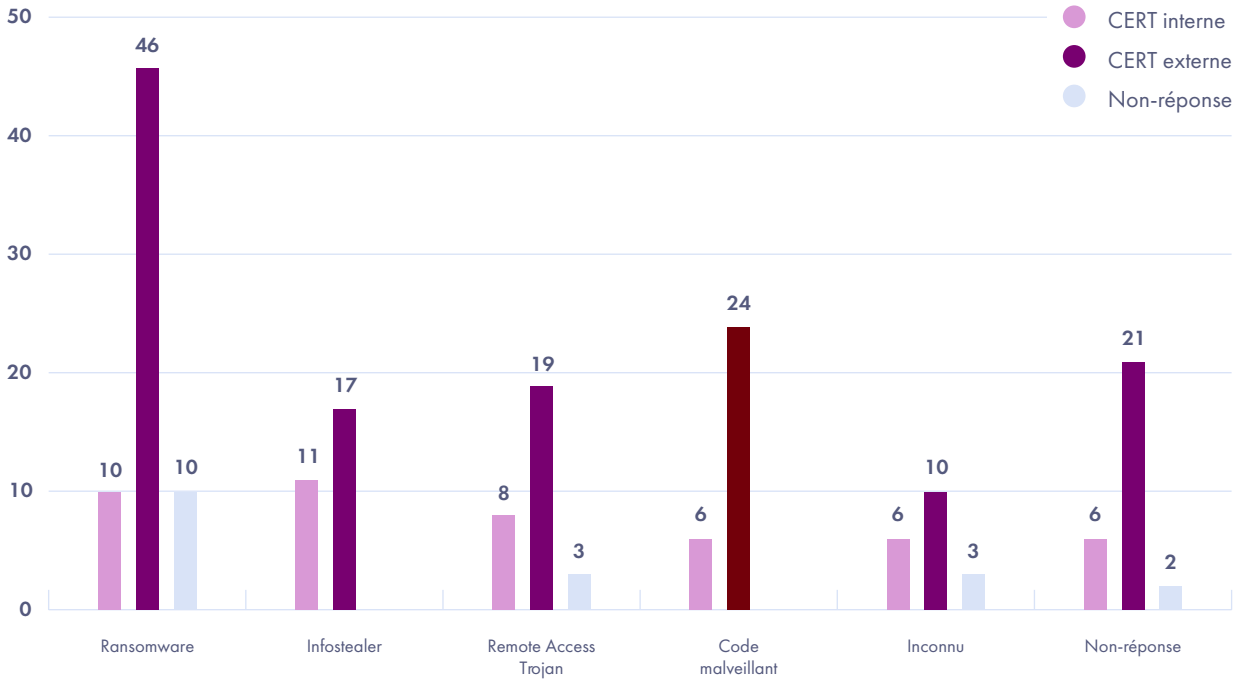
Nature d'attaque selon la typologie de CERT :

Dans les cas de ransomware, il est fréquent que les équipes CERT internes requièrent un renfort en ressources humaines ou des compétences spécifiques pour gérer l'incident de manière optimale. Ainsi, elles sollicitent souvent l'assistance de CERT externes afin d'obtenir un soutien spécialisé et complémentaire.



Source : InterCERT France, 212 questionnaires, 2024

Répartition des outils malveillants par types de CERT :



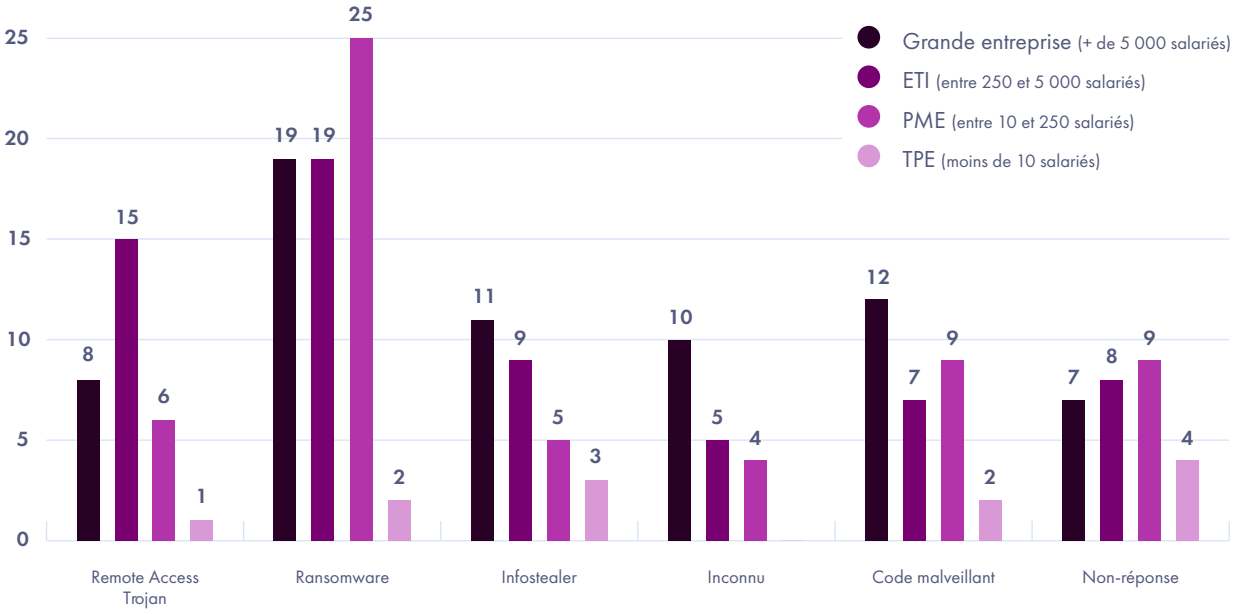
Source : InterCERT France, 212 questionnaires, 2024

TLP:CLEAR

Des disparités notables en fonction du type d'organisation victime de la cyberattaque.

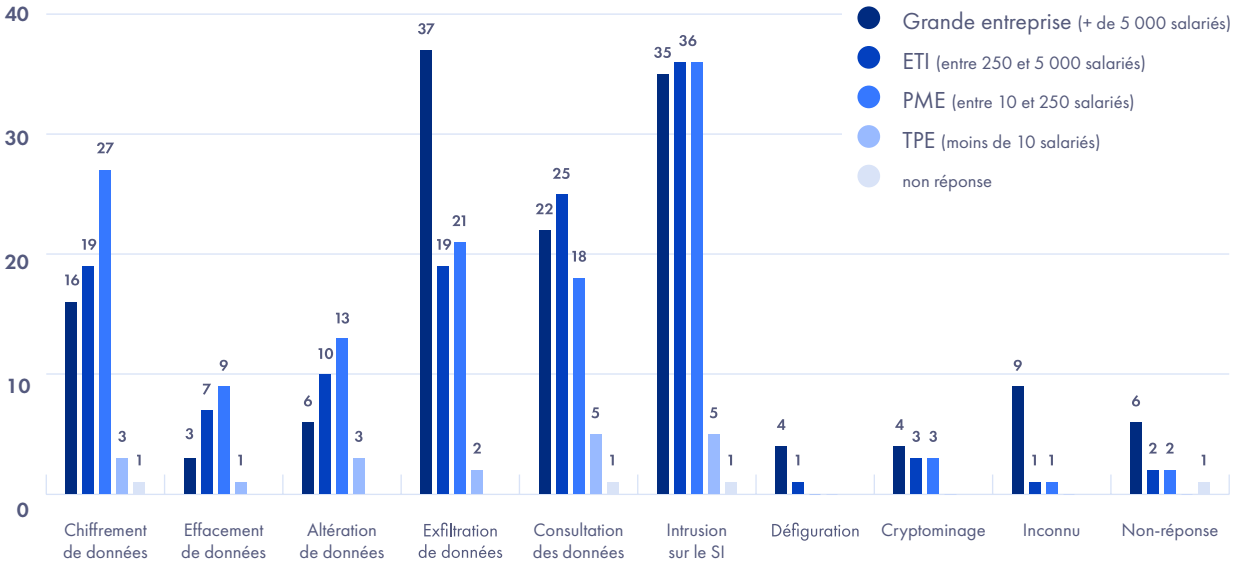
Les CERT externes traitent un nombre plus élevé d'incidents comparativement aux CERT internes, ce qui est attendu. Cela peut s'expliquer par le fait que les équipes CERT externes proposent ce type de service de manière commerciale, ce qui implique une gestion d'un volume d'incidents plus important.

Repartition des outils malveillants rencontrés lors des réponses à incidents en fonction de la taille de l'entreprise :



Source : InterCERT France, 212 questionnaires, 2024

Répartition des types d'attaques rencontrées, selon la taille de l'entreprise :



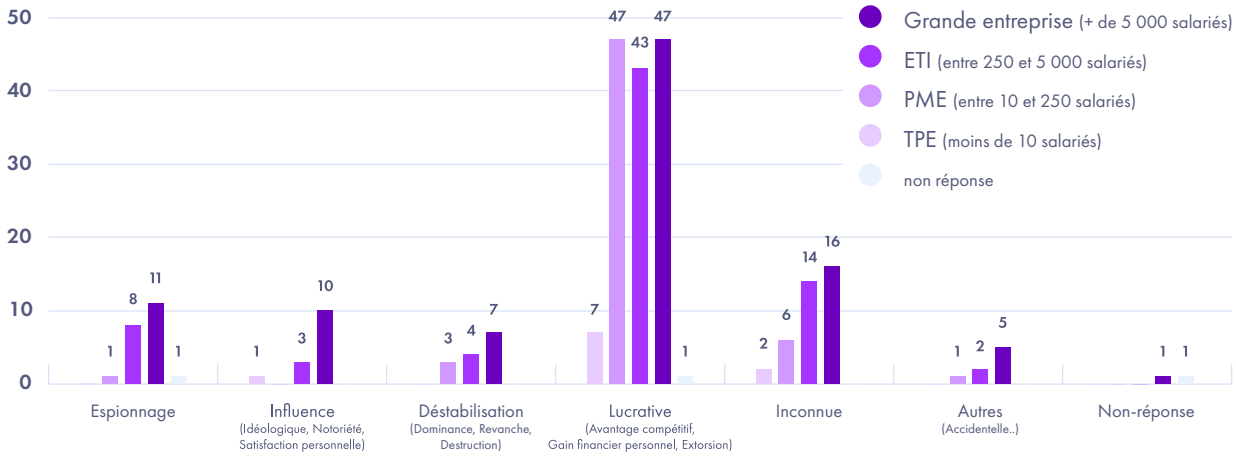
Source : InterCERT France, 212 questionnaires, 2024

Nous constatons que la menace prédominante pour les grandes entreprises est la fuite de données. Par ailleurs, dans plus d'un cas sur dix, il n'a pas été possible d'identifier la nature de l'attaque, ce qui révèle la complexité des systèmes d'information de ce type d'organisation.

Les entreprises de taille intermédiaire (ETI) sont, quant à elles, plus vulnérables à l'ensemble des types d'attaques, ce qui souligne l'importance de se préparer à toutes les formes de menaces. Ces structures possèdent une surface d'exposition plus vaste que les PME, mais ne disposent pas des mêmes ressources que les grandes entreprises.

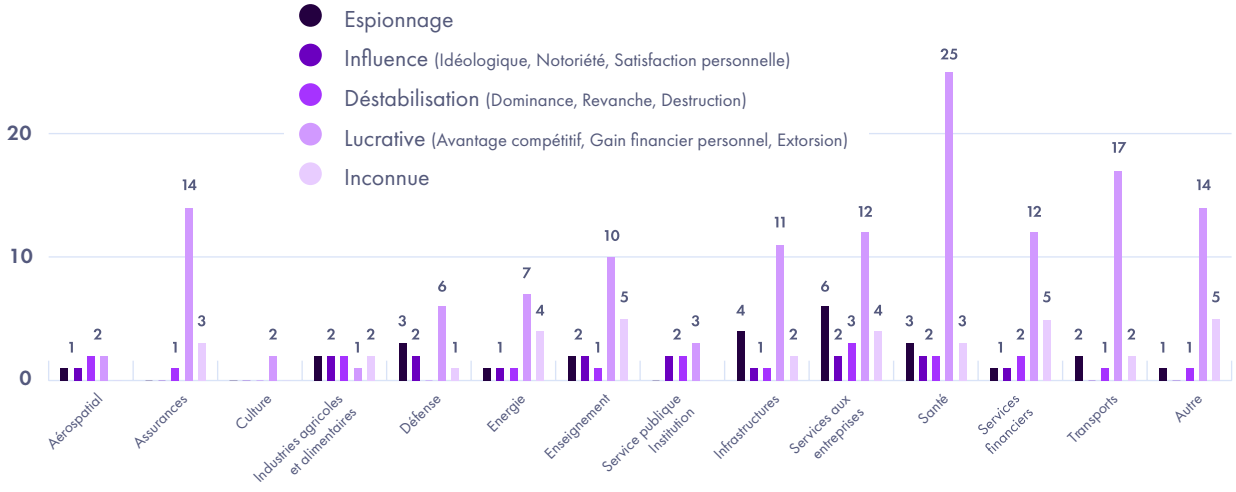
Motivations

Les attaques motivées par des objectifs lucratifs sont la principale motivation pour toutes les catégories d'organisations.



Source : InterCERT France, 212 questionnaires, 2024

Cependant, il apparaît que les secteurs dits critiques, tels que la défense, l'aérospatial, la santé, l'énergie et le secteur public, sont particulièrement vulnérables au cyber-espionnage.



Source : InterCERT France, 212 questionnaires, 2024

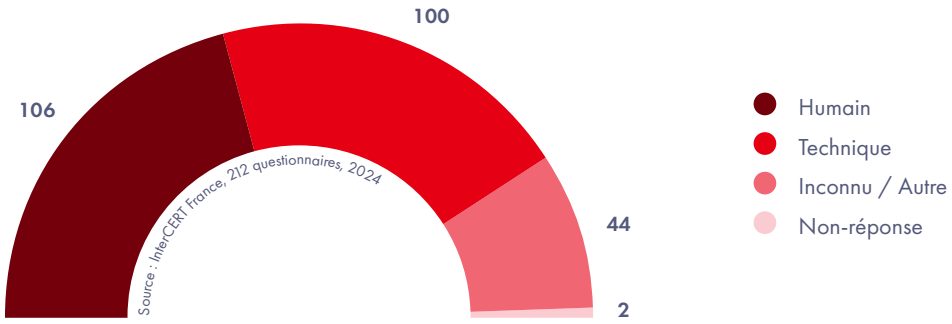
Cela se traduit par un nombre accru d'attaques ciblées dirigées vers ces secteurs critiques.

TLP:CLEAR

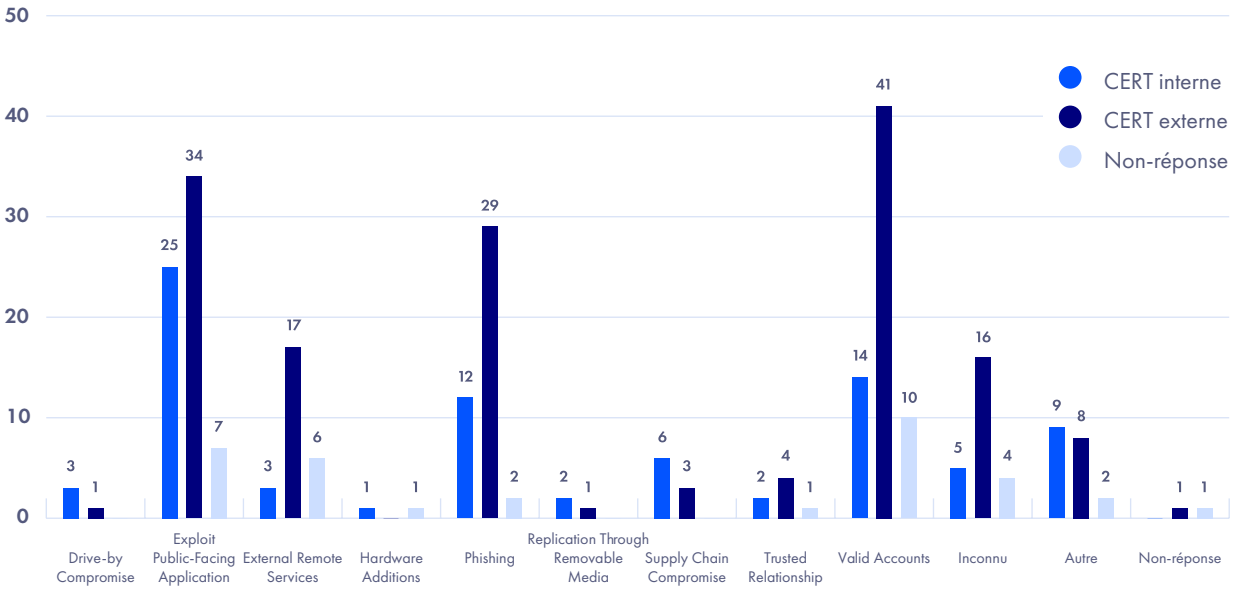
Vecteurs de compromission

Les vecteurs de compromission ont été classés en deux grandes catégories : les vecteurs humains (notamment le phishing et les attaques drive-by) et les vecteurs techniques (tels que les vulnérabilités des systèmes exposés sur Internet et les services d'accès à distance).

Cette classification révèle un équilibre presque parfait entre ces deux canaux d'attaque, soulignant que les attaques ciblent autant les utilisateurs que les systèmes techniques.



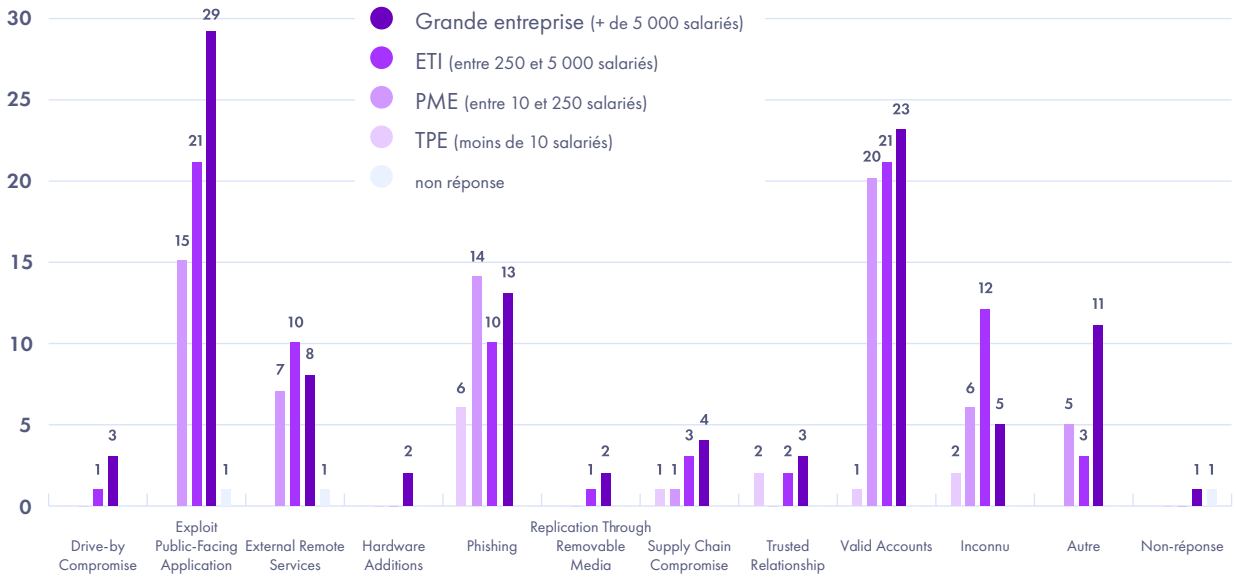
Tous les CERT, qu'ils soient internes ou externes, observent la même distribution de techniques d'intrusion.



Source : InterCERT France, 212 questionnaires, 2024

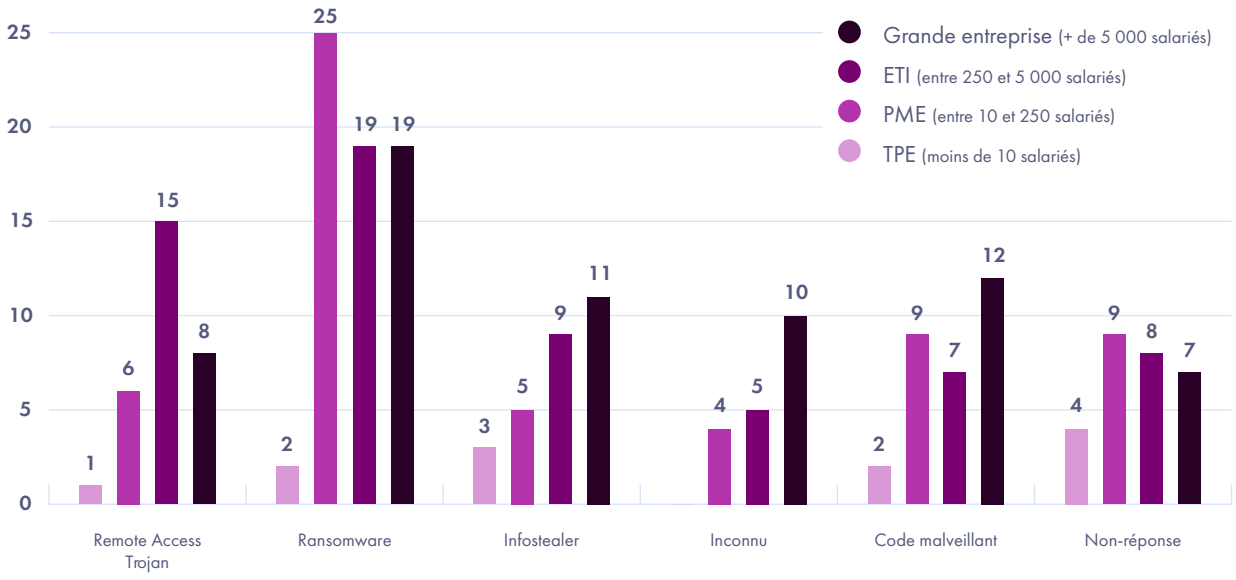
Nous n'observons pas de différence significative dans le top 3 des vecteurs d'intrusion, quelle que soit la taille de l'organisation. Cependant, pour les très petites entreprises (TPE), le vecteur d'intrusion le plus fréquent reste le phishing.

Conseil : Pour se protéger efficacement contre cette menace, il est essentiel de sensibiliser les collaborateurs des petites et moyennes entreprises. Globalement, les meilleures pratiques pour se prémunir contre ces menaces sont bien connues : l'authentification multifactorielle (MFA), l'authentification contextuelle et la gestion des correctifs.



Source : InterCERT France, 212 questionnaires, 2024

Les profils de risques varient selon les types de structure : les besoins cyber des uns ne sont pas forcément ceux des autres !



Source : InterCERT France, 212 questionnaires, 2024

De manière plus précise, si toutes les organisations sont ciblées par les infostealers, il est à noter qu'en 2023, les organisations type PME et ETI sont plus sensibles aux infections par ransomwares et RAT. En effet, bien souvent les grandes organisations ont développé des programmes cyber permettant de lutter efficacement contre ces menaces, là où les PME et ETI doivent encore trouver des modèles adaptés à leurs spécificités.

Enfin, dans près d'un cas sur 10, il n'a pas été possible d'identifier d'outil malveillant spécifique, corroborant d'autres études comme le rapport de l'ANSSI soulignant une utilisation de plus en plus forte de LOLbins (Living Off the Land Binaries, des exécutables et des scripts légitimes déjà présents sur un système).

Durée des incidents

27

le nombre de jour moyen entre l'intrusion et la détection

Des disparités fortes apparaissent néanmoins en fonction du type de structure. En effet, plus la structure est importante et complexe...

1. Plus le temps de détection est long ; contrairement aux plus petites structures, où les impacts sont généralement plus rapidement visibles... malgré l'absence de moyens de détection.
2. Plus le temps de résolution est long, notamment à cause de systèmes d'information plus complexe et d'une distribution plus importante de la connaissance et des compétences que dans les structures plus petites où quelques individus centralisent la capacité de gestion et de relance du SI.

Structure	Temps de détection en moyenne (en jours)	Temps de résolution en moyenne (en jours)
TPE	10,1	3
PME	21	11,5
ETI	27	19,7
Grandes Entreprises	32,3	28,5

Peu d'équipes ont exprimé le besoin d'obtenir davantage de journaux d'événements, mais plusieurs ont souligné l'importance de centraliser les journaux existants et de disposer de ressources de stockage et d'analyse plus adaptées.

Dans le cadre d'incidents majeurs, de nombreux CERT indiquent se trouver avec des effectifs insuffisants et manquer de compétences spécialisées en forensic.

De manière générale, il est nécessaire de renforcer les relais locaux dans les filiales ainsi que les équipes métiers, en les formant aux enjeux cyber pour une gestion plus efficace des incidents.

ZOOM RANSOMWARE

QU'EST-CE QU'UNE ATTAQUE PAR RANSOMWARE

Un ransomware (ou rançongiciel en français) est un logiciel malveillant qui verrouille l'accès à votre appareil ou à vos fichiers en les chiffrant, puis exige le paiement d'une rançon pour les déchiffrer.

Les cybercriminels exploitent le plus souvent des vulnérabilités connues dans les logiciels, que les victimes n'ont pas encore corrigées.

> Les attaquants cherchent principalement à extorquer de l'argent en promettant - souvent sans tenir parole - de rendre l'accès aux données bloquées.

Cependant, ils peuvent aussi simplement vouloir endommager le système de la victime pour lui causer des pertes d'exploitation et nuire à sa réputation.

Aujourd'hui, les attaques par ransomware sont souvent précédées d'une intrusion dans le réseau de la victime. Les cybercriminels mènent alors une reconnaissance discrète pour identifier les actifs numériques importants et les sauvegardes avant de déclencher leur attaque. Cette phase de reconnaissance peut durer plusieurs jours voire plusieurs semaines. Les attaques sont généralement lancées pendant des périodes de moindre activité (la nuit, le week-end etc.) afin de maximiser les chances de succès sans être détectées ni interrompues.

Lors d'une attaque par ransomware, le cybercriminel met hors service l'ordinateur ou le système d'information de la victime, rendant toutes les informations stockées inaccessibles. Il envoie ensuite généralement un message à la victime, proposant de fournir le moyen de déchiffrer les données en échange d'une rançon. Les pirates informatiques exigent souvent le paiement en cryptomonnaie pour garantir leur anonymat et compliquer les efforts des autorités pour les retrouver.

Il est nécessaire de souligner que, malgré ce qui peut être communiqué par les attaquants,

> **une attaque par ransomware n'est pas une fatalité pour une entreprise si elle est gérée à temps et de manière encadrée.**

La plupart des victimes pensent à tort qu'elles ne pourront pas déjouer une attaque par ransomware ou encore que le paiement d'une rançon constitue leur seule opportunité de récupérer leurs données.

> **Or, c'est en sollicitant les autorités et en bénéficiant ainsi d'un support de la part d'experts que l'entreprise victime aura le plus de chance de récupérer ses fichiers chiffrés.**

Par ailleurs, le travail des autorités peut permettre la détection d'éléments de compromission non détectés auparavant.

Retrouvez en annexe un schéma résumant les étapes du processus de dépôt de plainte pour le ransomware.

LE RANSOMWARE AS A SERVICE (RAAS)

Les cybercriminels, dans l'intention d'amplifier la portée, l'impact et la rentabilité de leurs attaques, ont développé et démocratisé le concept du *ransomware as a service* (RaaS).

Ce processus fonctionne sur le même modèle que la gestion de logiciel en tant que service (SaaS). Les développeurs de ransomwares, également appelés opérateurs RaaS, se chargent du développement et de la maintenance des outils et de l'infrastructure des ransomwares. Ils regroupent leurs outils et services dans des kits RaaS, disponibles sur des forums du *dark web*, qu'ils vendent à d'autres pirates informatiques, appelés affiliés RaaS.

Bien que le potentiel de profit soit un moteur majeur de la prolifération du RaaS, ce système offre aux hackers et aux développeurs de ransomwares des avantages supplémentaires, tout en posant des défis additionnels aux professionnels de la cybersécurité :

En effet, dans le modèle RaaS, les personnes qui mènent les cyberattaques ne sont pas nécessairement celles qui ont développé le logiciel malveillant utilisé. De plus, différents groupes de hackers peuvent utiliser les mêmes ransomwares.

> **Cela complique la tâche des professionnels de la cybersécurité, qui peuvent avoir du mal à attribuer les attaques à des groupes spécifiques, rendant le profilage et l'identification des opérateurs et affiliés RaaS plus difficiles.**

Le RaaS permet aux opérateurs et affiliés de partager le risque, rendant chacun plus résilient. L'arrestation d'affiliés n'arrête pas les opérateurs, et les affiliés peuvent passer à un autre kit de

ransomware si un opérateur est appréhendé. Les hackers réorganisent et rebaptisent souvent leurs activités pour échapper aux autorités.

Enfin, l'utilisation du procédé RaaS limite les obstacles pour accéder à la cybercriminalité. Il permet à des acteurs de la menace ayant des compétences techniques limitées de mener des cyberattaques.

Quelques exemples d'attaquants utilisant le *ransomware as a service* :

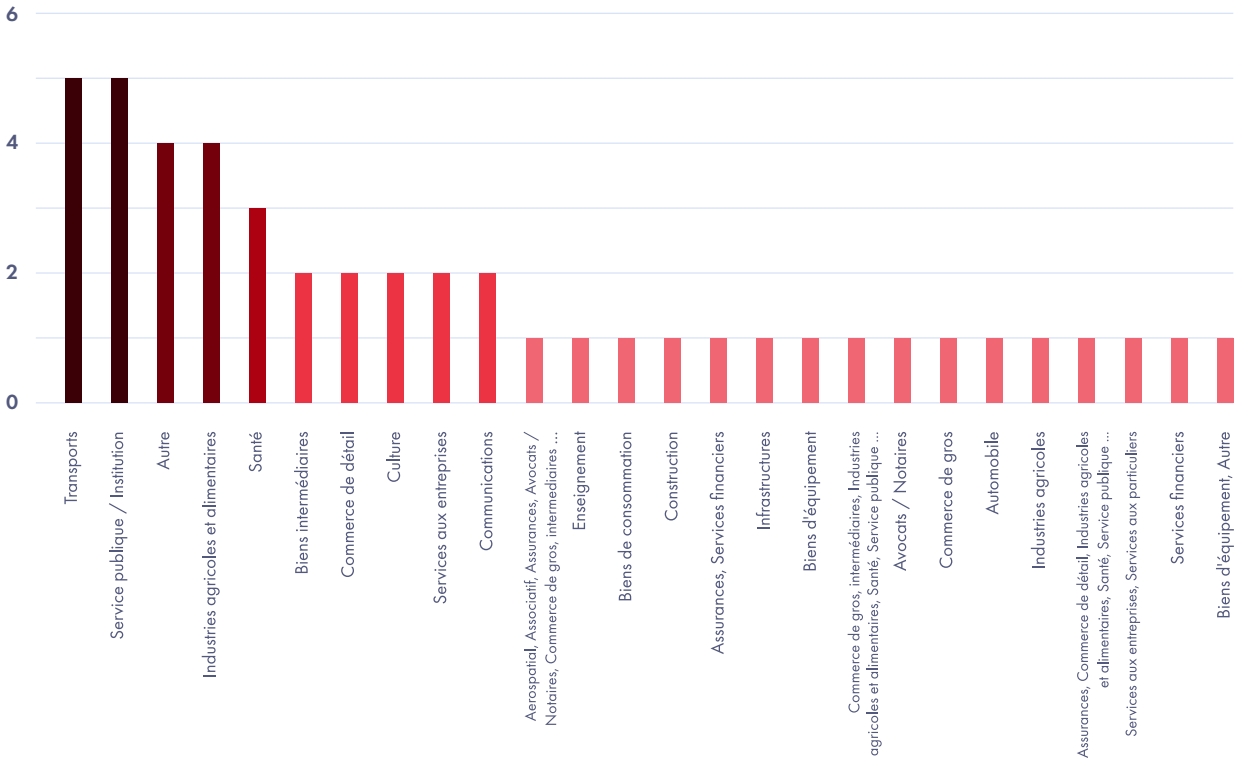
- Lockbit
- DarkSide
- REvil
- Hive
- Tox

INTRODUCTION DE L'ÉTUDE ET PÉRIMÈTRE

Lors de l'étude 2024 InterCERT sur les incidents de 2023, nous avons étudié plus de 200 incidents. Dans cette partie nous allons aborder spécifiquement les ransomwares qui représentent près d'un quart de ces incidents.

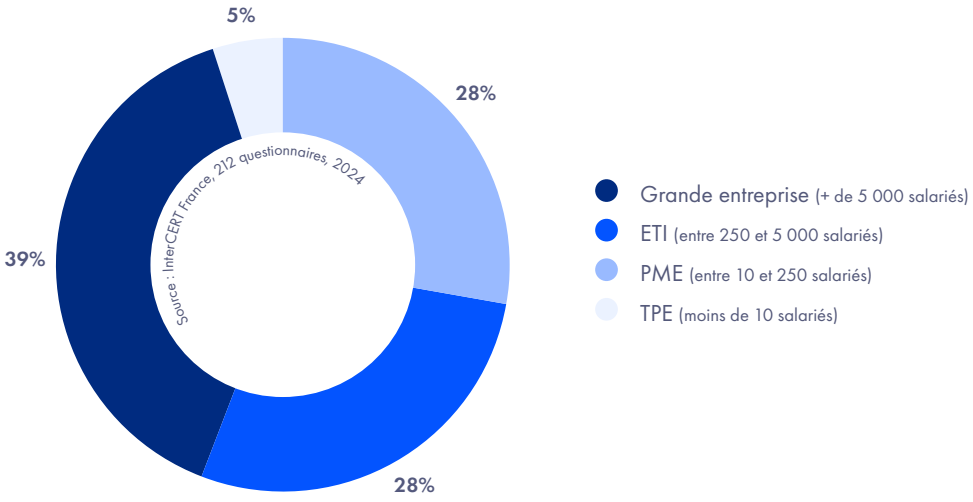
Parmi les ransomwares, un tiers touche une filiale seulement et 2 tiers touchent le groupe.

Aucun secteur d'activités n'est épargné, comme le montre le graphe ci-dessous qui correspond aux taux de réponses issus des questionnaires :



Source : InterCERT France, 212 questionnaires, 2024

De la même manière, les entreprises de toute taille sont concernées :



Les attaques par ransomware sont en grande majorité opportunistes, c'est-à-dire que les victimes sont choisies pour leur facilité d'accès / vulnérabilités plutôt que par volonté de nuire spécifiquement. Moins de **10%** des incidents semblent être donc ciblés.

Il est à noter que parmi les attaques par ransomwares, **10%** sont d'origine interne, qu'elle soit accidentelle ou malveillante.

Enfin, le questionnaire a été rempli par les CERT impliqués dans les différents incidents. L'échantillon est majoritairement composé de CERT externe, à 63%, contre 15% de CERT interne (22% des répondants n'ont pas précisé). Cela peut avoir un impact quant à la précision de certaines réponses, un CERT externe n'étant pas forcément impliqué de la même façon qu'un CERT interne dans certains aspects de la gestion d'une crise, par exemple la reconstruction post-incident.

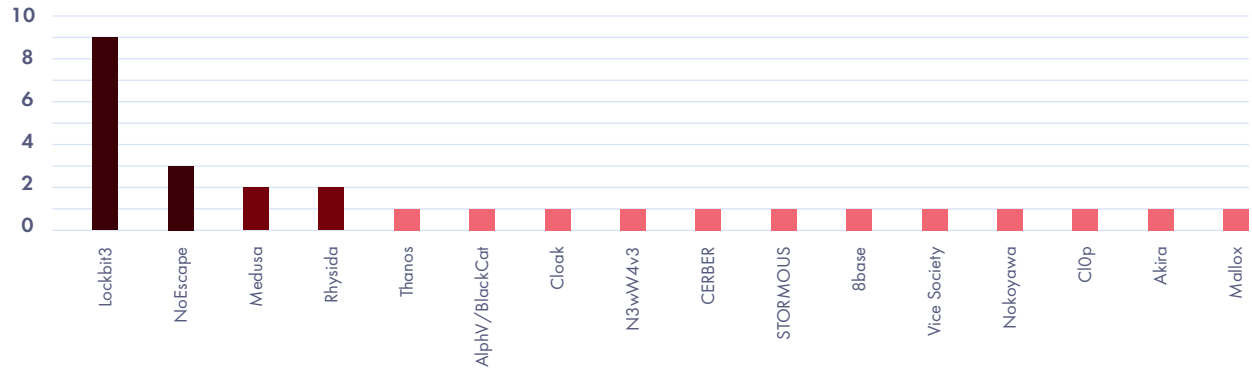
NOTIFICATION

Les cybercriminels des cercles de ransomware postent régulièrement sur leurs DataLeak Site (DLS), le « **Wall of Shame** » (mur de la honte) des victimes qu'ils ont réussi à compromettre. C'est aussi sur ces billets de blog qu'ils publient les échantillons de données ou les données en libre téléchargement, une fois le compte à rebours de la rançon terminé.

Seulement une attaque par ransomware sur 2 (50%) est cependant revendiquée.

Il arrive régulièrement (**40%** des cas) que le ransomware ne puisse pas être identifié. Parmi le palmarès des ransomwares les plus prolifiques et actifs sur 2023, nous retrouvons les suivants :

Part des ransomwares identifiés :



Source : InterCERT France, 212 questionnaires, 2024

Note : Certaines spécificités sont à noter : on identifie deux attaques par Ransomware Rhysida qui touchaient le **secteur public** et particulièrement la **santé** dans le cadre de cette étude, comme le montre le graphe ci-dessus qui correspond aux taux de réponses issus des questionnaires.

L'attaque est dans **68%** des cas détectée par les **collaborateurs** : soit des utilisateurs classiques qui ne peuvent plus utiliser une ressource (car elle a été chiffrée), soit les administrateurs des systèmes qui n'arrivent plus à se connecter. Les outils tels que les systèmes de détection technique (SIEM, EDR, ...) ne sont que dans **24%** des cas à l'origine de la détection de l'incident.

Dans de rares cas (**<6%**), ce sont les autorités elles-mêmes qui détectent l'incident et préviennent la victime directement.

Un quart du panel (27%) fait toutefois état d'une difficulté pour avoir les bons contacts auprès des autorités (pas de contact identifié ou de moyen facile pour les trouver). Ce sont principalement des TPE/PME qui sont dans cette situation, représentant 75% des répondants ayant signalé cette difficulté. Ces structures plus petites ont généralement moins de moyen pour mettre en place des procédures de réponses à incident, qui incluent souvent une section sur la notification aux autorités.

MTTD ET MTTR : SOUS QUELS DÉLAIS LES INCIDENTS SONT-ILS DÉTECTÉS ET TRAITÉS ?

Lorsqu'on mesure la rapidité de détection et de réaction à une crise, on parle de MTTD (Mean-Time to Detect) et MTTR (Mean-Time-To-Respond). Le MTTD et le MTTR sont respectivement le délai entre le début de l'attaque et sa détection et le délai entre le début de l'attaque et la fin de la réponse c'est-à-dire la résolution de l'incident incluant les phases d'endiguement, éviction, éradication et reconstruction (séquence E3R[1]).

1 ANSSI (Décembre 2023), « La séquence E3R », Cyberattaques et remédiation, les clés de décision, p.2

Dans l'étude Ransomware 2023, 43% des incidents sont cependant en dessous de la barre des 10 jours, contre seulement 32% des incidents au-dessus. Ainsi le **MTTD médian** se situe à **5 jours**.

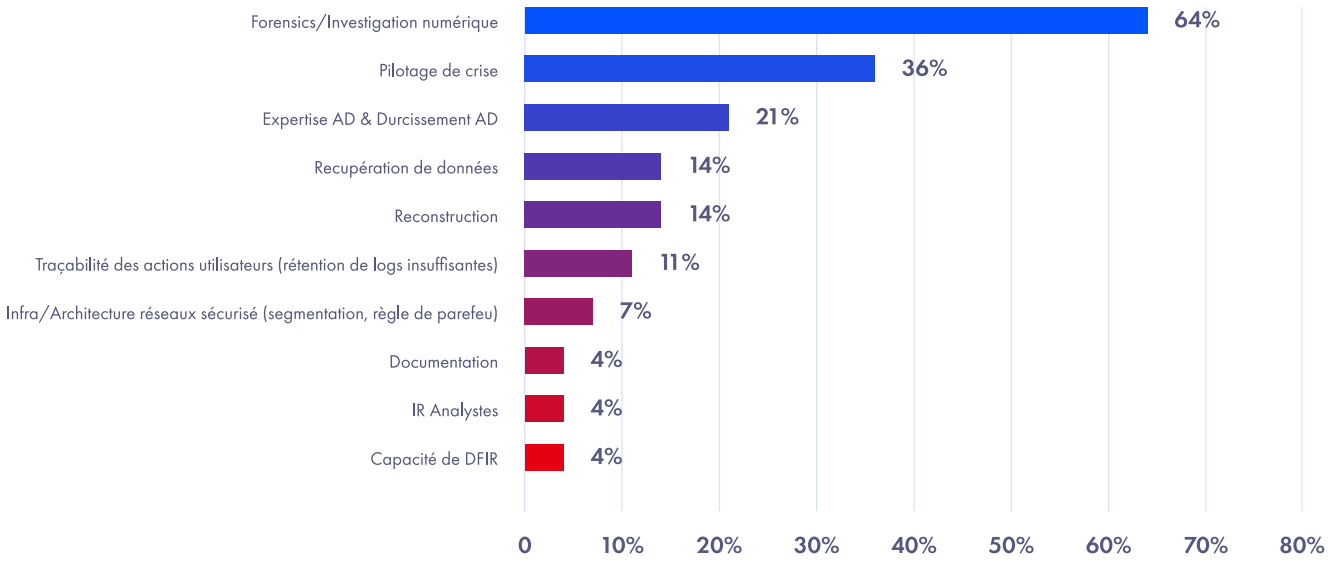
> **Note :** Dans plus d'un cas sur quatre (26%), le MTTD reste inconnu. En effet, il n'est pas toujours possible d'obtenir la date exacte de l'intrusion initiale.

Concernant la durée de la crise, les réponses traduisent un impact des incidents assez variés. Les crises signalées durent 50 jours en moyenne, mais avec des valeurs extrêmes qui rendent la médiane de 23 jours plus pertinente pour l'analyse.

En termes de moyens déployés, les réponses indiquent une charge moyenne de 40 jours/hommes, avec une médiane à 25. Là encore, les valeurs sont très hétérogènes : 38% des incidents ont mobilisé une charge de moins de 10 jours/hommes, et 13% une charge au-delà de 50 jours hommes.

Si l'on s'intéresse aux moyens et compétences nécessaires pour réagir au mieux en cas de crise, un déficit de compétence est globalement constaté. Une grande majorité des répondants (80%) ont en effet indiqué qu'il avait manqué des compétences au sein des équipes de la victime pour répondre à l'incident.

Quelles compétences étaient manquantes en interne chez la victime ?



Source : InterCERT France, 212 questionnaires, 2024

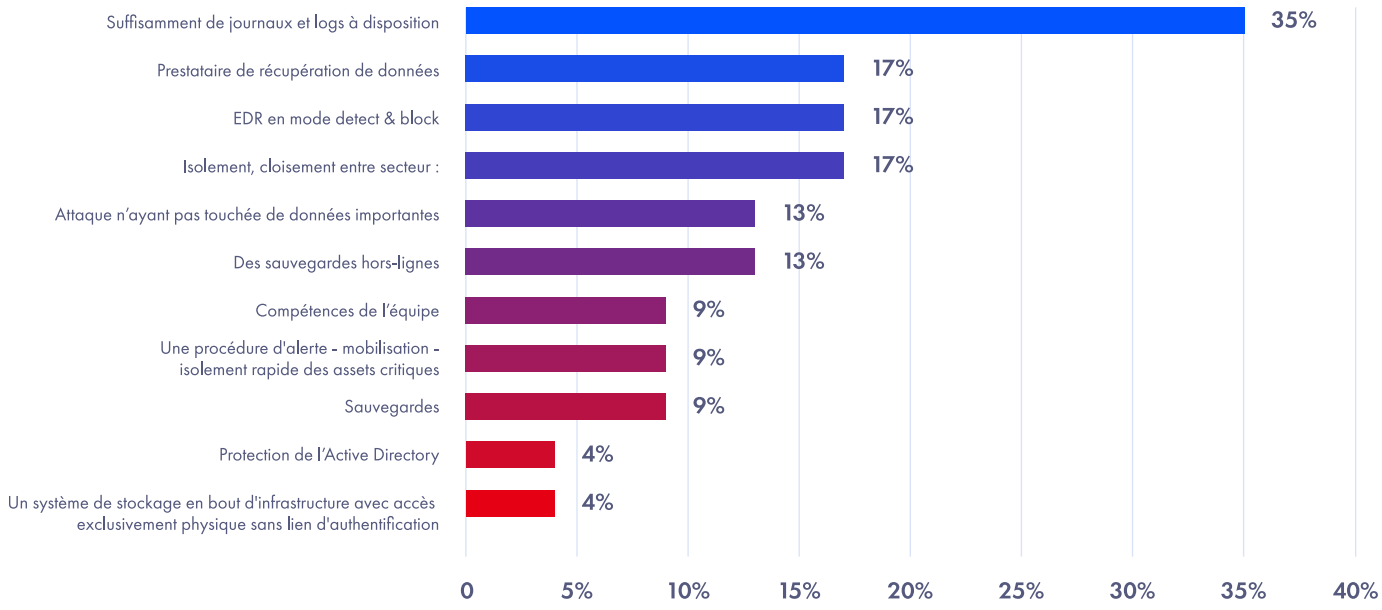
Les deux principaux savoir-faire manquants sont des compétences en forensics, citées dans 64% des réponses, et le pilotage de crise à 36%. Ce sont cependant des compétences qu'une organisation peut vouloir externaliser en contractualisant justement avec un CERT externe. On remarque d'ailleurs que 73% des réponses qui mentionnaient un manque de compétence en forensics concernent des ETI, PME et TPE, qui n'ont pas toujours les moyens d'avoir en interne ce genre de compétence pour faire face à des incidents d'ampleur. Les autres principales compétences manquantes citées sont l'expertise sur Active Directory (21%), ou la récupération de données chiffrées ou effacées (14%). Comme vu précédemment, l'Active Directory est assez

souvent visé par les attaquants dans ce type d'attaque, pour permettre une élévation de privilège... La reconstruction, également citée dans 14% des cas, est un exercice difficile qui peut nécessiter l'intervention de prestataires externes (par exemple sur la récupération de données effacées).

Si l'on s'intéresse aux outils et ressources les plus utiles pour la résolution des incidents, deux d'entre eux se détachent dans cette étude : la journalisation, et la présence d'un EDR (Endpoint Detection & Response).

- L'importance de disposer des journaux, ou logs pour la réponse à incident est en effet visible dans l'enquête 2024. Ils permettent, lorsqu'ils sont collectés sur les différents équipements du système d'information, de tracer certaines actions effectuées sur par les criminels. Un peu plus d'un tiers des répondants les jugent « différenciant » pour résoudre l'incident, toute sources de log confondues (e.g équipements réseaux, équipements de sécurité, ...), Cependant, plus d'un CERT sur deux (54%) interrogés affirment qu'ils ne disposaient pas des sources de logs nécessaires pour la résolution de l'incident. Les défaillances en matière de journalisation ne concernent pas uniquement l'absence de collecte ou de mauvaise règle de détection dans un SIEM, mais aussi des paramètres comme la durée de rétention des logs, trop courtes pour permettre l'investigation a posteriori.

Facteurs de succès dans la gestion de l'incident : éléments de sécurité décisifs :



Source : InterCERT France, 212 questionnaires, 2024

- D'autre part, installés sur les serveurs ou les postes de travail, les EDR sont des logiciels permettant de détecter et réagir contre des comportements potentiellement malveillants. Ces capacités et leur efficacité sont probablement à l'origine de leur mention fréquente dans les éléments différenciant : la présence d'un EDR est jugée comme particulièrement utile pour l'investigation dans 37% des cas, et comme « différenciant » dans la réponse à incident dans 17% des cas. Ils sont ainsi jugés aussi utiles pour la résolution de l'incident que l'isolement et le cloisonnement des différentes parties du SI, une pratique de sécurité bien connue et qui montre son efficacité ici.

COMMUNICATION PENDANT LA CRISE

Une question qui revient souvent lors d'une gestion de crise est « faut-il communiquer en interne ? En externe ? Que dire et quand ? ».

Une fois qu'une attaque ayant des impacts sur le SI est confirmée, il est généralement recommandé de communiquer en interne sur l'incident, pour maitriser les informations qui pourraient être partagées vers l'extérieur par les membres de l'organisation et diffuser les consignes et bonnes pratiques à adopter. Ces dernières permettent d'éviter des comportements aggravant la crise, et de continuer à faire fonctionner les processus métiers en mode dégradé si cela est possible. La communication en externe est un sujet plus sensible pour certaines organisations touchées, mais il est généralement préférable de le faire pour éviter que des clients, partenaires ou parties prenantes potentiellement affectées par l'attaque l'apprennent d'une autre façon que par la victime elle-même.

On constate cependant ici que seulement 48% des répondants ont fait état d'une communication en interne sur l'évènement. Dans plus de deux tiers des cas où il n'y a pas eu de communication en interne, l'attaque avait pourtant été détectée par un collaborateur.

Concernant la communication vers l'extérieur, l'enquête révèle que 78% des répondants n'ont pas communiqué vers l'extérieur. Il faut cependant noter que les répondants ont semblé considérer que la communication vers l'extérieur n'incluait pas les échanges avec les autorités, comme nous l'avons vu précédemment.

TECHNIQUES DE COMPROMISSION ET NOUVELLES MÉTHODES D'ATTAQUE

Dans l'échantillon d'attaques analysées, nous retrouvons en cause un grand nombre de serveurs et de services exposés sur Internet et souvent vulnérables (tels que RDP, SSH, MOVEit) ou encore des VPN, machines Citrix ou autres appliances comme FortiNet, PaloAlto, CheckPoint mal patchés.

Un autre facteur d'accès initial très commun est l'utilisation de comptes valides («Valid Account»[2]) via leur compromission (bruteforce, password spraying et réutilisation de mots de passe issus de Combolists et de fuites de données).

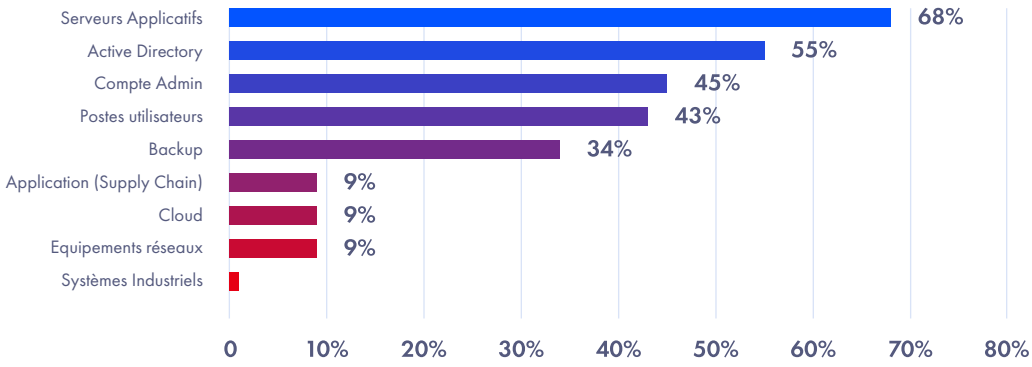
Une fois sur le réseau, les attaquants utilisent énormément les techniques de scan réseau afin d'effectuer une reconnaissance et une cartographie du SI des victimes. Cela les aide à identifier rapidement les systèmes d'intérêts comme les Active Directory ou les serveurs de fichiers et de sauvegardes.

Dans les actifs les plus visés, on retrouve évidemment les serveurs applicatifs et l'Active Directory, l'annuaire permettant la gestion des identités dans les environnements Windows. Sur le podium

2 Voir la sous-technique « Valid Accounts » de la base de connaissance ATT&CK, du MITRE : https://attack.mitre.org/techniques/T1078/

également, les comptes administrateur (notamment du domaine), permettant aux attaquants d'élever leurs privilèges afin de se déplacer à loisir dans les SI :

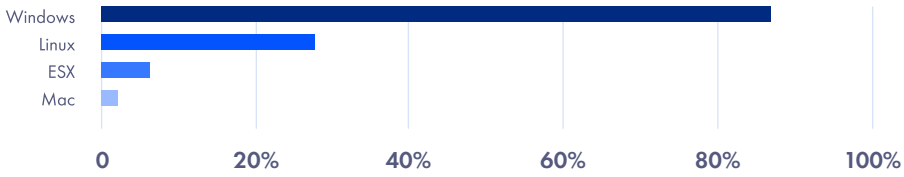
Part des incidents où ce type d'actif a été compromis :



Source : InterCERT France, 212 questionnaires, 2024

On observe que tous les incidents ayant mobilisé plus de 25 jours/homme (médiane sur les incidents signalés) et 75% de ceux pour lesquels la crise a duré plus de 23 jours (médiane sur la durée des crises) ont impliqué la compromission de l'Active Directory, d'un compte administrateur, ou des serveurs applicatifs. Cela souligne l'impact que peut avoir la compromission de ces actifs en cas de cyberattaque, et donc la nécessité de s'assurer de leur sécurisation.

Systèmes d'exploitation compromis :



Source : InterCERT France, 212 questionnaires, 2024

Nous notons par ailleurs l'utilisation massive de logiciels d'accès à distance (RMM ou RAT) permettant de conserver une persistance sur les systèmes même après la suppression d'un implant comme Cobalt Strike[3].

Bien qu'on réussisse à définir une KillChain[4], chaque attaque est unique et ne se ressemble pas. Des cas plus exotiques ont ainsi eu lieu. Parmi ces incidents, nous pouvons citer un cas de mouvement latéral via l'EDR ou encore un Escape-to-Host d'une victime permettant un « Third party compromise » chez son hébergeur. Nous observons également des téléchargements de charge active via BITS, un service natif de Microsoft Windows.

3 Pour plus d'information sur le logiciel Cobalt Strike, voir l'entrée Wikipedia associée : Cobalt Strike (Novembre 2022). Dans Wikipedia. https://fr.wikipedia.org/wiki/Cobalt_Strike

4 Pour plus d'information sur la notion de « Kill Chain », voir l'entrée Wikipedia associée : Kill Chain (Août 2024). Dans Wikipedia, https://fr.wikipedia.org/wiki/Kill_chain_(s%C3%A9curit%C3%A9_informatique)

EXFILTRATION DE DONNÉES ET RANÇON

Chaque attaque reste unique. Leur nature en témoigne : une exfiltration des données a été observée dans 64% des ransomwares. De même, seulement 17% des incidents montrent un effacement de certaines données comme des sauvegardes (en plus du chiffrement des systèmes qui lui est présent dans plus de 80% des incidents).

> **Note :** Si les sauvegardes sont fréquemment citées comme un moyen de pouvoir rapidement rebondir après une attaque par ransomware, l'enquête révèle des défaillances en la matière : 1 incident sur 3 a fait état de sauvegardes compromises (chiffrement ou effacement) au moins partiellement. De plus, 25% des réponses indiquaient que les sauvegardes étaient utilisables, mais uniquement partiellement. Cela était dû dans certains cas à une compromission par l'attaquant mais aussi à cause d'une fréquence de sauvegarde inadaptée (certaines réponses parlent de plusieurs semaines depuis la dernière sauvegarde), ou de l'absence de campagne de tests de restauration à partir des sauvegardes avant la crise.

Les opérations de sécurité et la surveillance des systèmes et réseaux en temps réel permet de limiter l'impact de ces attaques. Dans 4% des incidents, les ransomwares n'ont pas été exécutés ou n'ont pas réussi à chiffrer les données.

Une spécificité du ransomware est la rançon. En effet, l'objectif premier des cybercriminels étant de générer des revenus (>93%), ils extorquent l'argent des victimes en échange de rendre l'accès aux données chiffrées. Les montants des rançons observés varient entre 100 000$ et 250 000$, parfois en équivalent Bitcoin ou autre cryptomonnaie. Cependant, une grande majorité des rançons n'est pas connue. Cette technique permet aux attaquants d'entrer plus facilement en contact avec leurs victimes et d'établir un premier lien d'échange direct. Ils ont donc plus de chance de pouvoir utiliser les biais cognitifs de l'humain qu'avec une simple note de rançon et un montant dissuasif. Les victimes entrent donc en contact avec les cybercriminels via des chats sur le site des criminels. Certains de ces chats sont notamment disponibles ici[5].

L'exfiltration de données s'est faite dans de nombreux cas via des outils de synchronisation de fichiers tel que rclone[6] et à destination d'espaces Cloud sur des plateformes comme MEGA[7].

Il existe d'autres impacts que la fuite de données confidentielles et les conséquences en termes d'image ou de règlementation et législation. Parmi ceux-là, nous observons la consommation de ressources dans 4% des incidents. Il arrive parfois que les criminels profitent d'avoir de la ressource « compute » pour miner des cryptomonnaies par exemple. Cependant, dans plus d'un cas sur deux des indisponibilités totales ou partielles des SI sont les conséquences directes du chiffrement et de l'effacement des données.

5 Ransomchats Wiever, projet GitHub de mise à disposition de transcription anonymisée de chat entre groupe d'attaquants et victimes dans des cas réels d'attaque : https://:%20https:/github.com/Casualtek/Ransomchats

6 Pour plus d'info sur le logiciel rclone, voir l'entrée Wikipedia associée : Rclone (Octobre 2024). Dans Wikipedia, https://en.wikipedia.org/wiki/Rclone

7 Pour plus d'info sur le logiciel Mega, voir l'entrée Wikipedia associée : Mega (Juillet 2024). Dans Wikipedia, https://fr.wikipedia.org/wiki/Mega_(site_web)

RECONSTRUCTION ET PHASES POST-CRISE

Une fois l'attaque contenue, il faut se tourner vers l'après, avec d'une part la reconstruction du SI touché, pour restaurer le fonctionnement normal du SI, et d'autre part de potentielles actions de durcissement de la sécurité du système d'information. Ces actions de durcissement dérivent généralement des défaillances constatées pendant la crise elle-même. Dans notre enquête, un tiers des incidents ont été suivis d'une phase de reconstruction (33%) ou de durcissement (38%).

Concernant la reconstruction, les durées sont très variables dans les réponses, leur longueur étant liée à l'ampleur de l'attaque : 56% des attaques où la reconstruction a duré plus de 30 jours sont des cas où l'Active Directory était compromis, et parmi les 44% restants, les trois quarts avaient vu la compromission d'au moins un compte administrateur. La qualité des sauvegardes joue un rôle crucial dans la reconstruction, et comme nous l'avons vu précédemment, 46% des répondants signalement une défaillance dans les sauvegardes les ayant rendus partiellement ou totalement inutilisables. Ces défaillances étaient soit le fruit d'une action de l'attaquant, soit liées à des soucis dans la gestion des sauvegardes (e.g fréquence de sauvegarde trop faible, manque de test des sauvegardes, ...).

Concernant le durcissement enfin, plusieurs CERT ont signalé ne pas avoir été impliqué sur cette phase, ou n'avoir émis que des recommandations sans savoir si elles avaient été suivies. Cela peut expliquer le faible taux de réponse positive (38%) lorsqu'il leur a été demandé s'ils avaient été impliqués sur cette phase. Parmi les réponses positives, on retrouve comme mesure de durcissement le déploiement d'un EDR sur tout ou partie du SI chez un tiers des répondants, recoupant les réponses soulignant son importance pour la résolution de la crise, et le durcissement de l'Active Directory chez un quart.

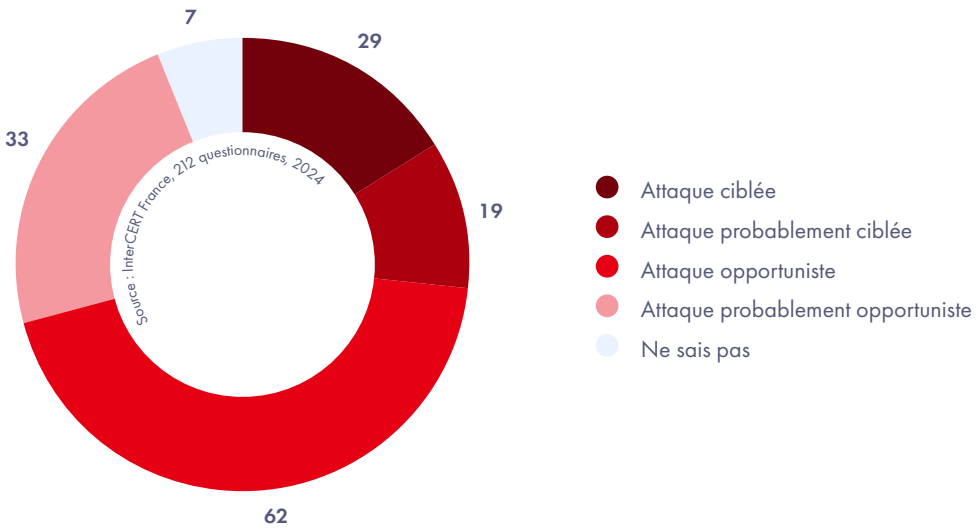
ZOOM
AUTRES PHÉNOMÈNES

Par « autres phénomènes », l'étude désigne tous les incidents référencés n'étant pas classés comme ransomware, ou du phénomène cybercriminel traditionnel.

FOCUS SUR LES ATTAQUES CIBLÉES

Sur l'ensemble des incidents renseignés comme "autres phénomènes", 48 sont considérés comme des attaques ciblées. Une attaque ciblée se distingue de l'attaque opportuniste par le fait que l'attaquant a délibérément cherché à compromettre la victime, en la ciblant pour ce qu'elle représente, les données en sa possession, sa nature vitale ou son écosystème, et non par l'identification opportuniste de vulnérabilités, l'envoi massif de phishing ou l'achat d'accès obtenus par d'autres.

Répartition des attaques : ciblage spécifique vs opportunisme

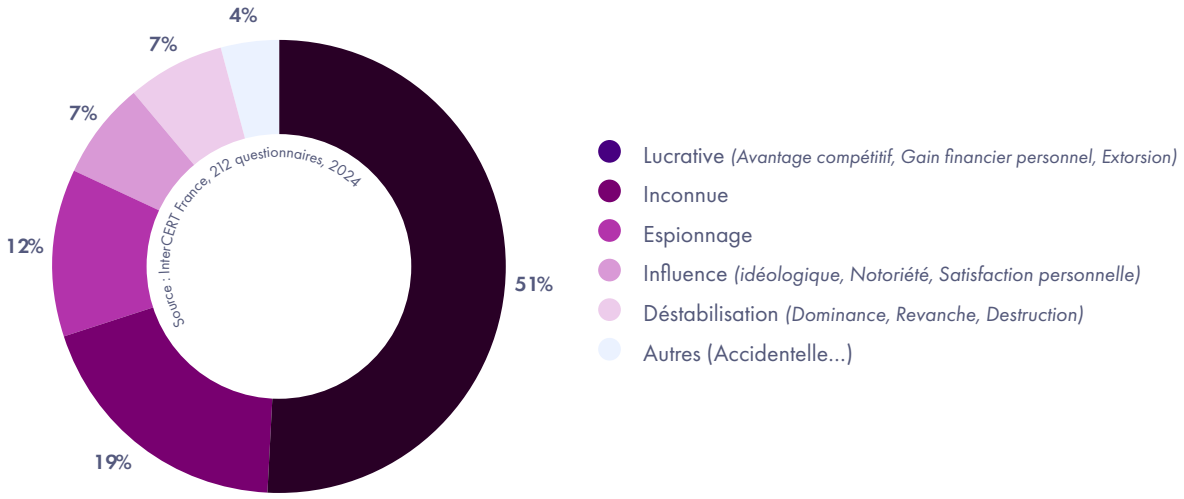


L'analyse des motivations derrière les attaques ciblées

Sans surprise, la finalité lucrative reste la motivation principale, tous incidents confondus (51%) sur cette étude.

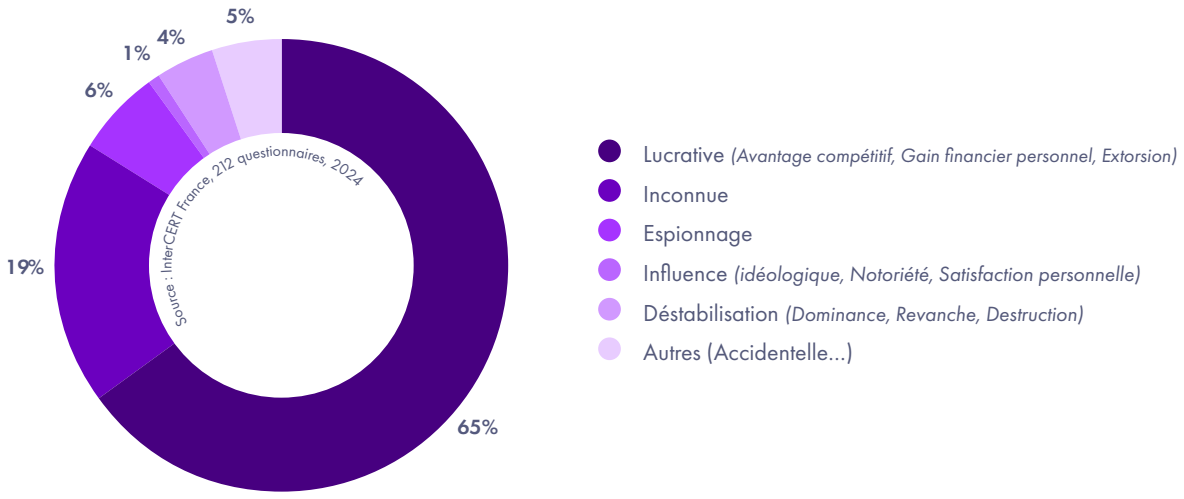
Mais ces attaques ciblées présentent également des motivations plus spécifiques, notamment l'espionnage ou l'idéologie. Cet alignement des motivations abonde dans le sens d'une potentielle prédation économique ou de l'intérêt que peut représenter la donnée exfiltrée ou potentiellement exfiltrée.

Motivations sur l'ensemble du périmètre de l'étude :



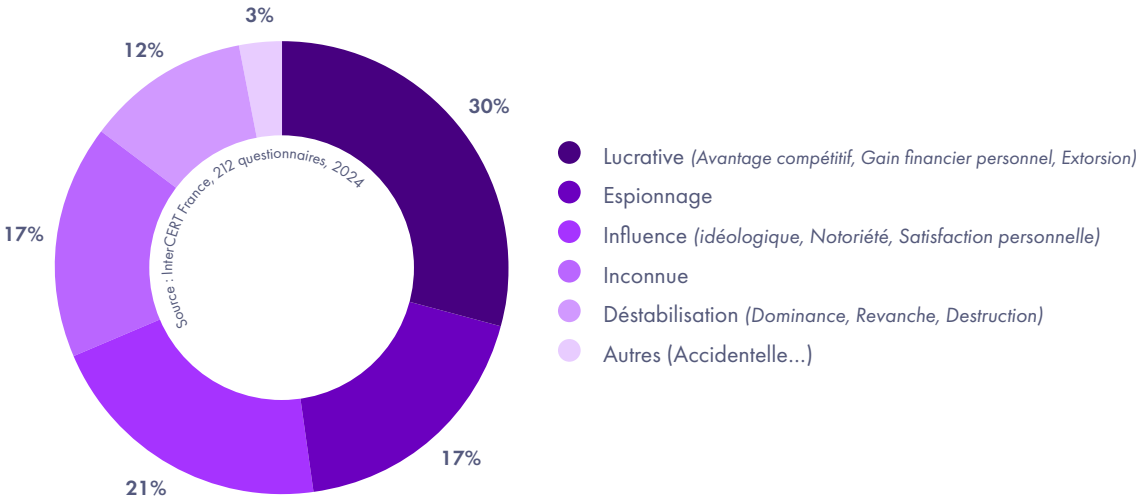
La part de motivation lucrative gagne du terrain lorsque l'on zoome sur les attaques qualifiées d'opportunistes, passant de 51% à 65%.

Motivations des attaques opportunistes :



A l'inverse, cette part diminue lorsqu'il s'agit des attaques ciblées ou potentiellement ciblées (de 51% à 30%), grignotée par l'espionnage qui passe de 6 à 21%. En effet, seules 6% des attaques opportunistes ou potentiellement opportunistes sont motivées par l'espionnage, et 12% à l'échelle de l'ensemble de l'étude. Un chiffre qui s'élève à 21% lorsqu'on observe les statistiques des attaques ciblées ou potentiellement ciblées.

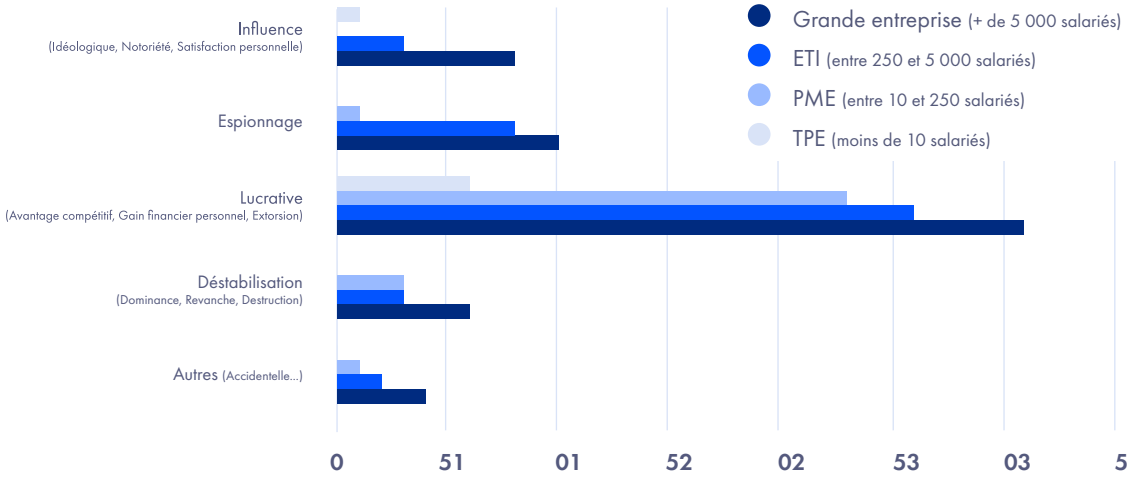
Motivations des attaques ciblées :



Il est également intéressant de souligner que les attaques d'influence prennent une part plus importante, passant de 1% des attaques opportunistes, à 17% des attaques ciblées.

Lorsqu'il s'agit d'attaques ciblées, les grandes entreprises et les entreprises de taille intermédiaire sont plus souvent concernées par les opérations qualifiées d'espionnage. Les très petites entreprises sont, quant à elles, proportionnellement principalement concernées par les attaques ciblées à motivation lucrative. Ainsi, il est possible d'émettre l'hypothèse que certaines TPE seraient ciblées en raison de leur niveau de sécurité supposé plus faible.

Motivations et taille des cibles : analyse des attaques ciblées ou probablement ciblées :



Source : InterCERT France, 212 questionnaires, 2024

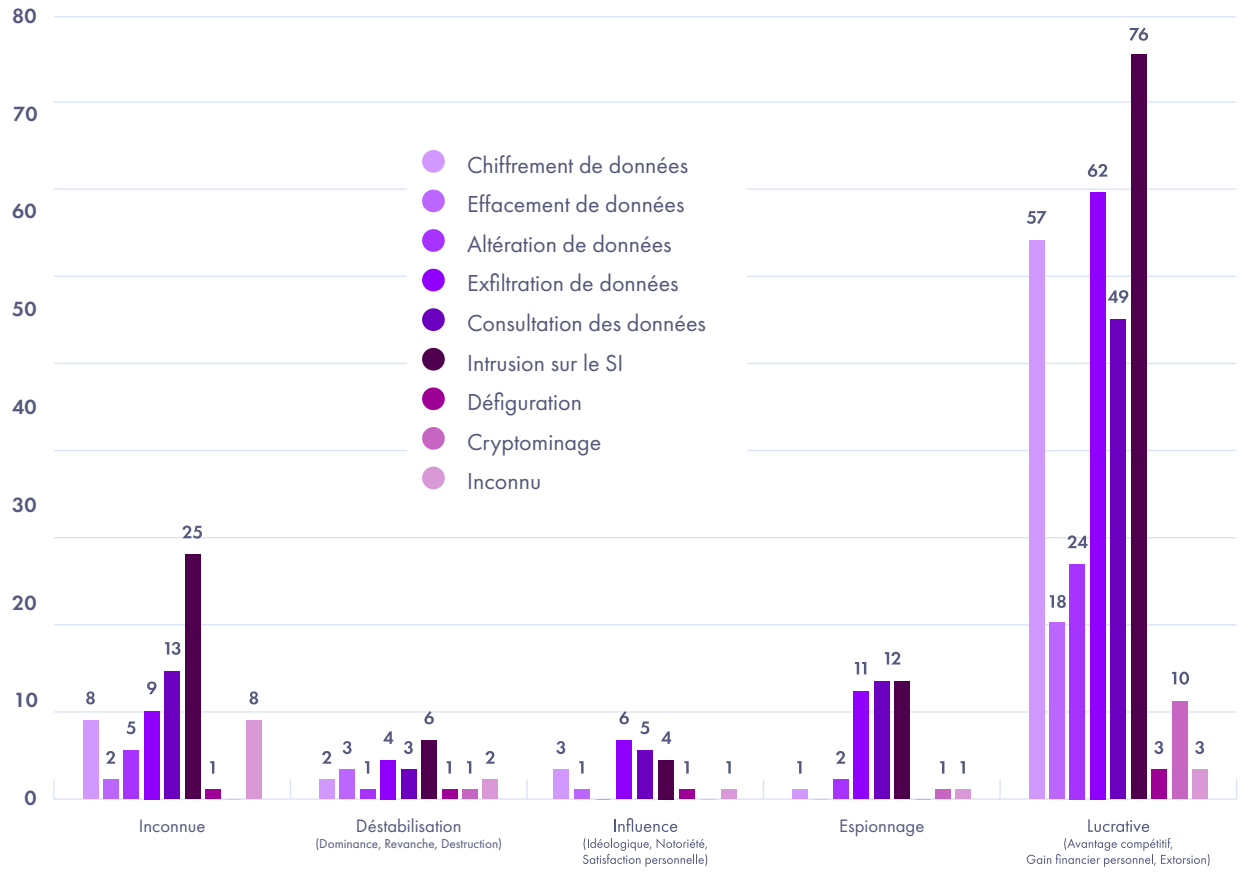
Une part significative des interrogés (38, soit 18%) déclarent ne pas avoir pu déterminer la motivation derrière l'attaque qu'ils ont subie. Après les attaques à buts lucratifs, cette mention est la plus représentée au sein des CERTs répondants.

Il existe plusieurs hypothèses d'explications à cette répartition. Tout d'abord, l'identification des motivations justifiant une attaque est une tâche complexe qui requiert la possession d'un contexte et d'une position de recul dont les CERTs internes ou commerciaux ne sont pas toujours en mesure de disposer lors de leurs investigations.

Si le travail d'analyse lors de la réponse à incident consiste à reconstituer la chronologie des évènements, les actions menées par l'attaquant, ses outils, il permet parfois d'identifier ses objectifs sur le système d'information (répertoire spécifique, données stratégiques, compte utilisateur à privilège...). Mais ces éléments ne permettent pas systématiquement de statuer avec un niveau de confiance suffisant sur les intentions réelles des attaquants. Ainsi, un attaquant peut souhaiter subtiliser des accès ou identifiants, afin de les revendre à d'autres dont les motivations sont inconnues, ou les utiliser lui-même à des fins d'élévation de privilège ou de prépositionnement.

La notion de pré-positionnement n'était pas proposée explicitement comme option de réponse dans les questionnaires. Il est toutefois possible d'émettre l'hypothèse que cette tactique pourrait représenter une part non négligeable des cas englobés sous la motivation "inconnue", au même titre que le vol d'identifiants à des fins de revente (infostealers, courtiers en accès initiaux).

Motivations de l'attaquant et typologie de l'attaque :

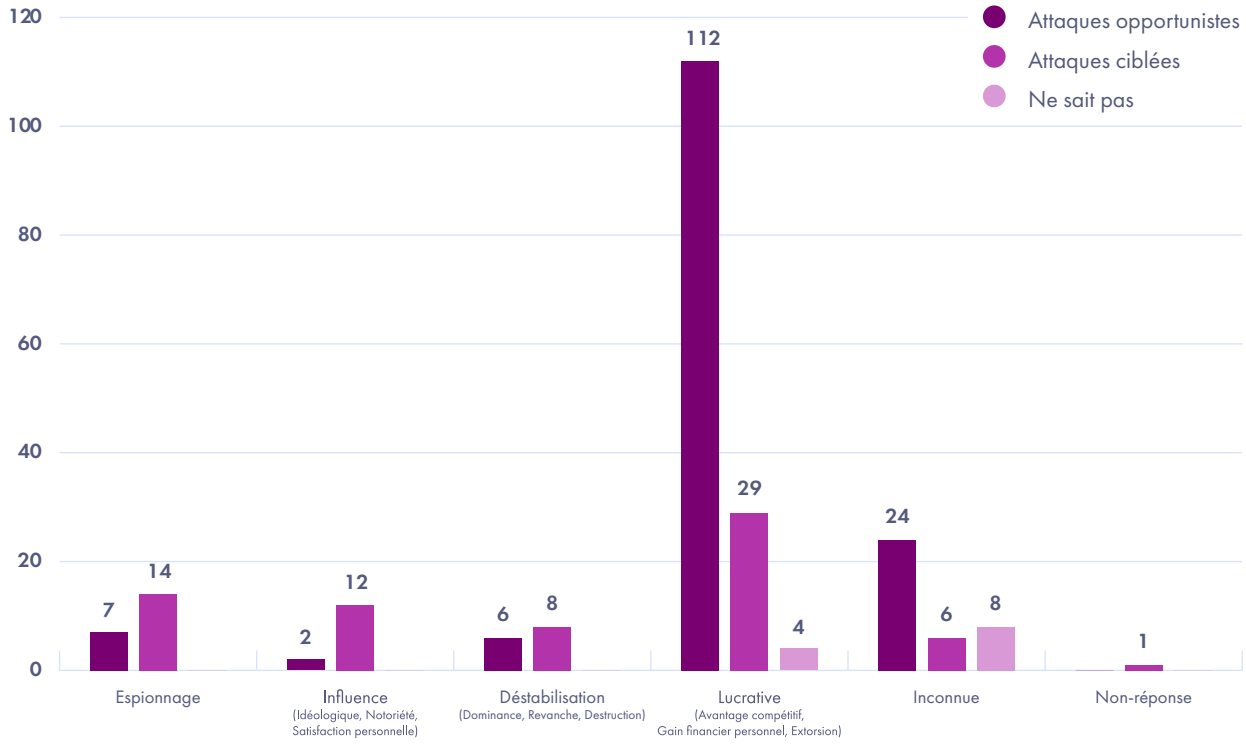


Source : InterCERT France, 212 questionnaires, 2024

L'évolution du contexte géopolitique encourage certains acteurs malveillants à s'introduire et à se maintenir sur des réseaux, potentiellement en vue de conduire des opérations ultérieures de sabotage et/ou d'espionnage. Il est très difficile de déterminer si la présence d'un attaquant au sein d'un SI relève d'une posture de pré-positionnement ou s'il s'apprête à déployer un ransomware, par exemple. Ce type de compromission implique néanmoins de mener des actions ciblées une fois dans le système d'information.

Il est ainsi essentiel de décorréler le ciblage de la victime, en amont, par une compromission assortie d'une reconnaissance ciblée, de la réalisation d'actions manuelles précises, pouvant apparaitre comme "ciblées" par l'attaquant une fois sur le système d'information de la victime compromise.

Type d'attaque vs attaque opportuniste ou ciblée :



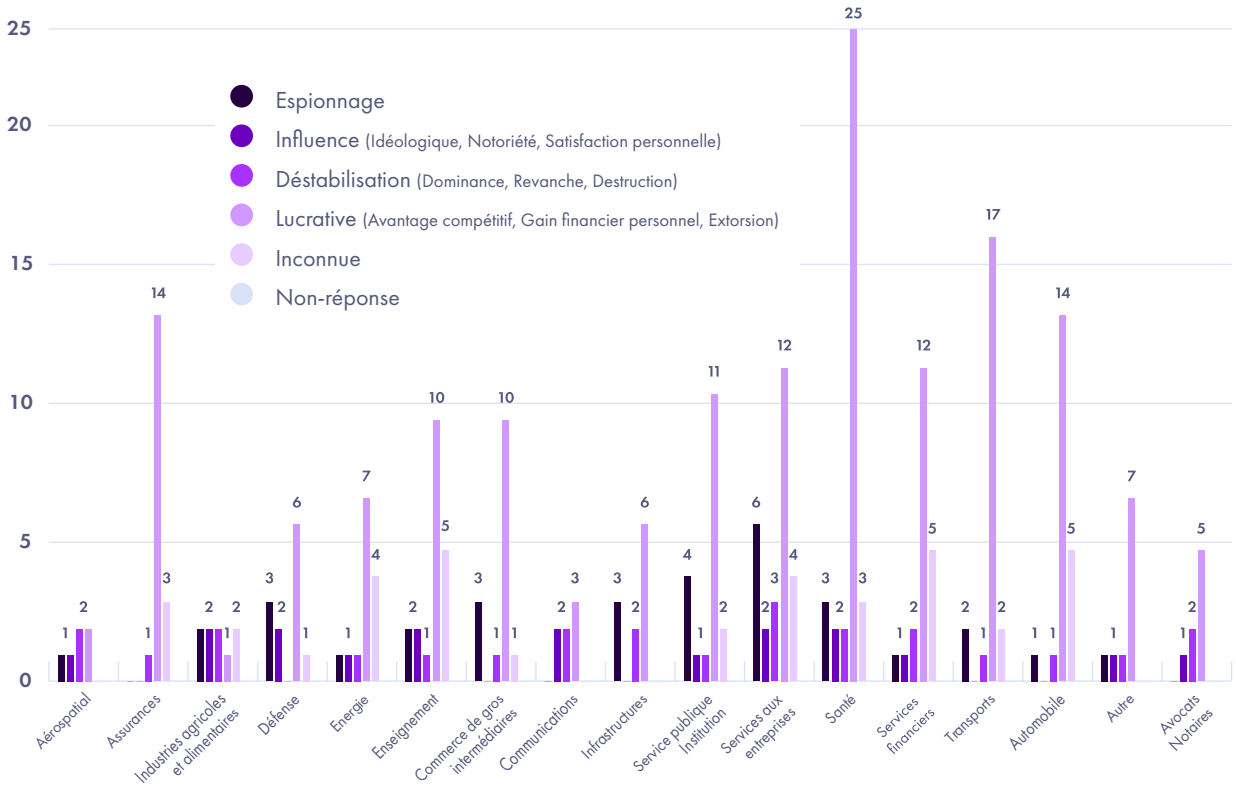
Source : InterCERT France, 212 questionnaires, 2024

La victimologie des attaques ciblées

Les secteurs

Les attaques ciblées renseignées dans cette étude se répartissent harmonieusement sur l'ensemble des secteurs. Même si l'étude implique intrinsèquement un biais en raison des secteurs des répondants, l'énergie est le secteur le plus représenté. Sur les 48 occurrences d'attaques ciblées et probablement ciblées, 6 le mentionnent. S'en suivent les services aux entreprises et services financiers, puis le secteur public et institutionnel, les transports et enfin, la santé.

Secteur d'activité de la cible et motivations potentielles de l'attaquant :



Source : InterCERT France, 212 questionnaires, 2024

Le secteur de l'aérospatial a subi autant d'attaques à but lucratif que d'incidents de déstabilisation.

Les CERT interrogés dans le domaine de la défense constatent une majorité à part égale d'attaques de type espionnage, déstabilisation et influence contre seulement une attaque à but lucratif.

On observe une part importante de motivations non déterminées dans les secteurs de l'enseignement, des industries agricoles et alimentaires, du service public et des institutions et des services financiers.

Le domaine de la santé enregistre 4 incidents sur 19 relevant d'actions d'espionnage. C'est sans comptabiliser les 2 instances dont les motivations n'ont pas pu être déterminées.

Le secteur des infrastructures n'a pas constaté d'occurrence d'espionnage et fait davantage face à des évènements de déstabilisation.

Profils des victimes d'attaques ciblées

Sur la totalité des attaques ciblées analysées, **les grandes entreprises sont sur-représentées** avec 27 occurrences (dont 8 filiales), soit 56% des victimes d'attaques ciblées ou potentiellement ciblées. 16 incidents ciblés ont affecté les entreprises de taille intermédiaire (dont 6 filiales), 6 les petites ou moyennes (dont 4 filiales), et 2 les très petites entreprises (dont 1 filiale). La majorité (5 sur 7) d'entité filiales chez les petites et moyennes entreprises et les très petites entreprises souligne l'importance des acteurs de taille moyenne en tant qu'acteurs clés de la **chaîne d'approvisionnement** (supply chain) à protéger.

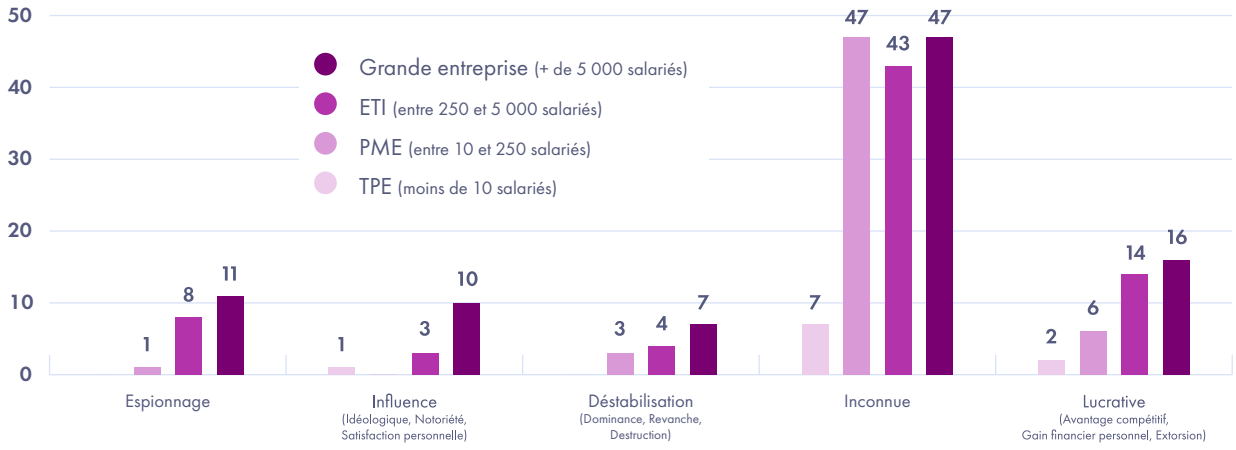
Si plus de la moitié des entités attaques ciblées (26 sur 48) concerne évidemment la France eu égard au scope des CERTs participants sollicités, il est intéressant de noter que les attaques traitées peuvent avoir un impact mondial, principalement chez les grandes entreprises :

- 18 s'étendent sur l'Europe,
- Et 12 hors du continent Européen dont :
  - Amérique du nord : 3
  - Moyen-Orient : 1
  - Asie - Indonésie & Inde : 2

Les grandes entreprises représentent la majorité des cas d'espionnage et d'attaques à but idéologique. La majorité des cas d'attaques ciblées concernent les grandes entreprises.

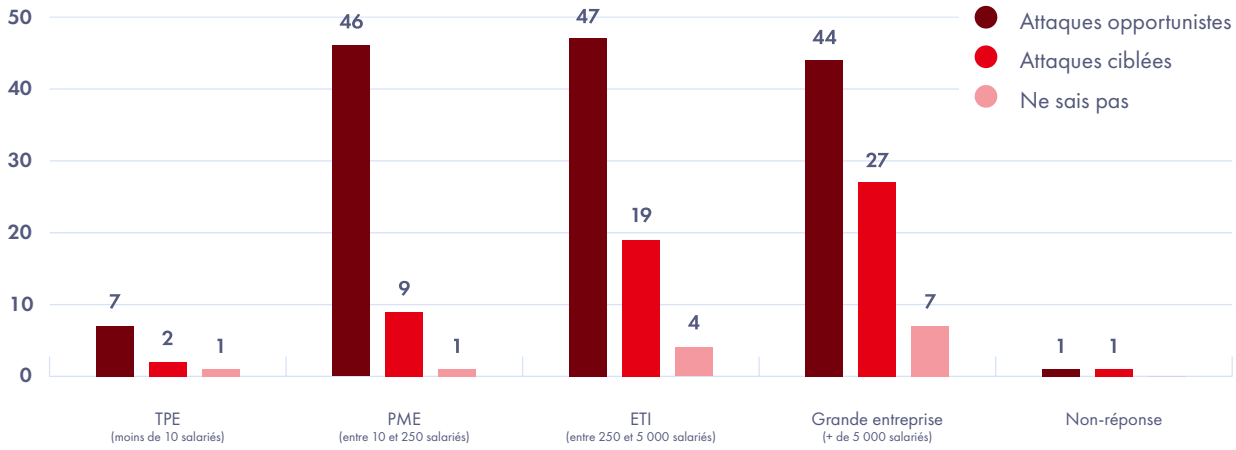
Les attaques opportunistes sont majoritaires chez les entreprises de taille intermédiaire (ETI).

Analyse de l'attaque : motivations de l'attaquant et profil de la cible :



Source : InterCERT France, 212 questionnaires, 2024

Profil de la cible et analyse du caractère ciblé de la campagne :



Source : InterCERT France, 212 questionnaires, 2024

Hypothèses d'attribution des attaques ciblées

20% des incidents reportés dans ces questionnaires ont été revendiqués par les attaquants.

Les attaques ayant pour objectif l'exercice d'une influence sont celles majoritairement revendiquées. En effet, sur les 13 comptabilisées pour cette question, 9 d'entre elles ont été revendiquées. Sans surprise, sur les 21 cas d'espionnage rapportés seul 1 a été revendiqué. Quelques autres ont été imputés à des acteurs de la menace.

La portée de l'attribution dans le cadre de l'activité d'un CERT

Il est important de souligner que l'attribution reste un exercice complexe. Peu priorisé dans le cadre de l'activité de réponse à incident, l'attribution (ou imputation), s'appuie sur les revendications des attaquants, ou par le rapprochement de données techniques ou d'infrastructures d'attaques. Les attributions présentées dans cette étude sont donc présentées à l'état d'hypothèses.

L'attribution peut être de plusieurs ordres : politique, judiciaire ou encore technique. L'attribution politique désignant un pays ou un acteur influencé par un Etat, reste l'apanage des acteurs publics ; l'attribution judiciaire est entre les mains des forces de l'ordre et du système judiciaire.

Les équipes de réponse à incidents et les analystes CTI procèdent à de l'attribution technique, grâce à un faisceau d'indices qui peuvent être techniques (artefacts système, traces réseau, éléments d'infrastructures tels que des IP, domaines, les outils tels que les malware), tactiques (comportement spécifique à un attaquant ou un mode opératoire d'attaque), et parfois géopolitiques (convergence de motivations et de déclencheurs politiques, économiques, sociétaux).

Cette attribution a pour impact de rattacher un attaquant à un mode opératoire désigné, ou à un cluster d'activité qui se caractérise ou se distingue par ses techniques, ses outils, sa victimologie, son comportement, ses infrastructures.

Si l'attribution à un Etat ne peut être une priorité lorsque l'on est en situation de crise lors d'un incident informatique, l'attribution technique permet, elle, de mieux connaitre son adversaire, et d'enrichir la connaissance de ses techniques, outils (hashes), les traces qu'il est susceptible de laisser sur le système d'information (IOCs), son comportement global. Ces informations peuvent être utiles, en amont, à la détection, la réalisation d'exercices de simulation d'attaques, mais aussi au durcissement du SI afin d'endiguer certaines techniques spécifiques. En aval, elles sont utiles à la réponse à incident et peuvent parfois donner de nouvelles pistes à investiguer.

Sur les 48 occurrences d'attaques ciblées ou probablement ciblées, seules 8 rattachées par les CERTs répondants à des acteurs de la menace précis. Dans le cadre de cette étude, nous ne disposons pas des moyens de challenger ces attributions, du niveau de confiance accordé par les CERTs à ces attributions, ni des éléments techniques appuyant ces hypothèses d'attribution.

Toutefois, deux modes opératoires d'attaque se distinguent : Hafnium et NSO/Cytrox.

Un premier incident notable est imputé au mode opératoire d'attaque Hafnium. La victime est un acteur du secteur public. Après un scan actif de la surface d'attaque de la victime, l'attaquant a exploité une vulnérabilité et s'est introduit dans le système d'information afin d'exfiltrer des données.

Focus - HAFNIUM

HAFNIUM est un acteur de la menace soutenu par l'État et opérant depuis la Chine, rendu public par Microsoft en mars 2021 et qualifié par celui-ci comme un « acteur hautement qualifié et sophistiqué ». Il serait actif depuis janvier 2021 et est lié au groupe APT40. L'acteur de menace cible principalement des entités aux États-Unis dans un certain nombre de secteurs industriels, notamment des chercheurs spécialisés dans les maladies infectieuses, des cabinets d'avocats, des établissements d'enseignement supérieur, des entreprises de défense, des groupes de réflexion sur les politiques et les ONG. Hafnium à pour but l'espionnage.

Hafnium s'est illustré par son attaque sur Microsoft Exchange en 2021, exploitant plusieurs vulnérabilités inédites. Le 2 mars 2021, Microsoft avait publié un avis de sécurité majeur portant sur sept vulnérabilités affectant différentes versions du logiciel de serveur de messagerie Exchange : CVE-2021-26412, CVE-2021-26854, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-202 1-27065 et CVE-2021-27078. Quatre d'entre elles, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 et CVE-2021-27065, ont été alors identifiées comme des vulnérabilités « 0 day » activement exploitées dans la nature. Près de 30 000 organisations américaines auraient ainsi été concernées par de potentielles fuites de données liées à cette attaque. La Cybersecurity and Infrastructure Security Agency (CISA) du département de la Sécurité intérieure des États-Unis (DHS) avait ensuite publié une directive d'urgence, exhortant les organisations à corriger immédiatement les failles dès que possible, citant la « probabilité d'une exploitation généralisée des vulnérabilités après la divulgation publique et le risque que les services du gouvernement fédéral au public américain puissent être dégradés ».

Hafnium aurait été lié à la création de Tarrask, un logiciel malveillant d'évasion utilisé lors d'attaques précédentes. Le logiciel malveillant a été utilisé dans des attaques ciblant les télécommunications, les fournisseurs de services Internet et les entreprises de services de données d'août 2021 à février 2022. Le logiciel malveillant utilise l'abus des tâches planifiées pour masquer les charges utiles livrées aux serveurs.

Plusieurs autres incidents mentionnent CYTROX et NSO dans le cadre de compromission ayant affecté des entités du secteur public. Les incidents impliquent la compromission de smartphones de collaborateurs, l'installation d'un spyware et la consultation puis l'exfiltration de données. Des techniques totalement cohérentes avec les modes opératoires et acteurs de la menace désignés.

CYTROX

Cytrox est une entreprise créée en 2017 qui développe des logiciels malveillants utilisés pour les attaques informatiques et l'espionnage. Cytrox a été créée comme une start-up

en Macédoine du Nord et a reçu un financement initial d'Israel Aerospace Industries. Le PDG de Cytrox est Ivo Malinkovski. Cytrox serait également présent en Israël et en Hongrie. En 2019, Cytrox a été acquis pour moins de 5 millions de dollars par Tal Dilian, un ancien commandant des Forces de défense israéliennes. Cytrox ferait partie d'une alliance connue sous le nom d'Intellexa, un label marketing pour une gamme de fournisseurs de surveillance mercenaire, créé par Dilian.

Predator est un logiciel espion développé par Cytrox qui cible les systèmes d'exploitation Android et iOS. En mai 2022, des chercheurs du Threat Analysis Group (TAG) de Google ont rapporté que Predator avait regroupé cinq exploits « 0 Day » et les avait vendu à plusieurs acteurs soutenus par un gouvernement, qui l'ont utilisé dans trois campagnes distinctes. Après avoir infecté un appareil, Predator a un accès complet à son microphone, à sa caméra et aux données de l'utilisateur telles que les contacts et les messages texte. Predator a également accès aux services de localisation d'un appareil et aux applications de messagerie telles que WhatsApp, Telegram et Signal.

En décembre 2021, Meta a annoncé que Cytrox et six autres groupes de surveillance pour compte d'autrui avaient été interdits d'utiliser ses plateformes pour cibler d'autres utilisateurs. En 2023, le département du Commerce des États-Unis a ajouté les sociétés Cytrox AD en Macédoine du Nord, et Cytrox Holdings Crt en Hongrie à sa liste noire. Le 5 mars 2024, le département du Trésor des États-Unis a imposé des sanctions à Cytrox AD en Macédoine du Nord et au Consortium Intellexa, qui est la société mère de Cytrox AD, « pour trafic d'exploits utilisés pour accéder aux systèmes d'information, menaçant la vie privée et la sécurité des personnes et des organisations dans le monde entier ».

Une enquête menée en octobre 2023 par des organismes de presse dirigés par le réseau European Investigative Collaborations, connu sous le nom de Predator Files, a révélé que Predator a été vendu à au moins 25 pays, dont l'Autriche, l'Allemagne, la Suisse, la République démocratique du Congo, la Jordanie, le Kenya, Oman, le Pakistan, le Qatar, Singapour, les Émirats arabes unis et le Vietnam. Son logiciel espion Predator a notamment été utilisé pour cibler des hommes politiques égyptiens 20211 et espionner une centaine de téléphones appartenant à des hommes d'affaires, des journalistes, des hommes politiques, des ministres du gouvernement et leurs associés en Grèce. Parmi les victimes figure également une ressortissante greco-américaine ayant la double nationalité et ancienne responsable de la politique de sécurité chez Meta, qui avait vu son téléphone infecté par Predator pendant un séjour en Grèce, en mars 2023. En octobre 2023, plusieurs législateurs américains ont été pris pour cible par le Vietnam. Des experts américains sur l'Asie de divers groupes de réflexion et plusieurs journalistes ont également été pris pour cibles.

Les solutions de surveillance et outils malveillants se sont multipliées avec l'exportation de compétences offensives à l'échelle internationale.

NSO

NSO Group Technologies (NSO étant le nom des fondateurs de l'entreprise, Niv, Shalev et Omri) est une société israélienne d'espionnage cyber connue pour son logiciel espion

Pegasus, de surveillance de smartphones, fondée en 2010. Elle employait près de 500 personnes en 2017. Presque toute l'équipe de recherche de NSO est composée d'anciens membres du renseignement militaire israélien, la plupart ayant servi à la Direction du renseignement militaire d'Israël, et nombre d'entre eux de l'unité 8200.

NSO affirme qu'elle fournit aux gouvernements autorisés une technologie qui les aide à lutter contre le terrorisme et le crime. L'entreprise affirme qu'elle ne traite qu'avec des clients gouvernementaux. Le logiciel espion Pegasus est classé comme une arme par Israël et toute exportation de la technologie doit être approuvée par le gouvernement.

Selon plusieurs rapports, le logiciel espion de NSO Group a été utilisé pour cibler des militants des droits humains et des journalistes dans divers pays, a été utilisé pour l'espionnage d'État contre le Pakistan, pour la surveillance intérieure sans mandat de citoyens israéliens par la police israélienne, et a joué un rôle dans le meurtre du dissident saoudien Jamal Khashoggi par des agents du gouvernement saoudien.

En 2019, la société de messagerie instantanée WhatsApp et sa société mère Meta ont poursuivi NSO en vertu de la loi américaine relative à la fraude et aux abus informatiques. En 2021, Apple a intenté une action en justice contre NSO aux États-Unis. Ces derniers ont inclus NSO Group dans leur liste noire pour avoir agi contre les intérêts de sécurité nationale et de politique étrangère des États-Unis.

Enfin, nous notons la mention de l'acteur de la menace APT15 dans une attaque, bien que mentionnée comme opportuniste. Si les techniques renseignées sur cet incident ne semblent pas, de prime abord, habituelles du mode opératoire APT15, il reste particulièrement intéressant de souligner la mention de cet acteur.

APT15

APT15 est un acteur de menace connu pour le cyber-espionnage, avec des serveurs enregistrés en Chine, et qui serait affilié au gouvernement chinois. APT15 cible le pétrole, le gouvernement, la diplomatie, l'armée et les ONG en Amérique centrale et du Sud, dans les Caraïbes, en Europe et en Amérique du Nord depuis au moins 2010. Le groupe est aussi connu sous les noms de « Ke3chang », « Vixen Panda GREF », « Playful Dragon » et « Mirage ». APT15 avait lancé en 2018 une campagne avec un nouveau logiciel malveillant baptisé « MirageFox », qui semble être une variante ou une version améliorée du cheval de Troie d'accès distant « Mirage » (RAT) qui a démarré en 2012. Pour mener à bien ses attaques d'espionnage, APT15 a employé bien plus d'une douzaine d'outils, malveillants et autres. APT15 a également déjà utilisé le logiciel malveillant « RoyalAPT ».

Dans le cadre d'une campagne d'attaques qui s'est déroulée de la fin de 2022 au début de 2023, ciblant le ministère des Affaires étrangères des Etats-Unis, APT15 a notamment utilisé la porte dérobée Graphican. Elle a la même fonctionnalité que Ketrican, une porte dérobée qu'APT15 a utilisée dans les attaques précédentes, mais utilise l'API Microsoft Graph pour se connecter à OneDrive et récupérer des informations de commande et de contrôle (C&C). En fonction des commandes reçues du serveur C&C, Graphican peut créer une ligne de commande interactive, créer des fichiers, télécharger des fichiers et créer des processus avec des fenêtres masquées.

FOCUS SUR L'ESPIONNAGE

Comme présenté ci-dessus, la proportion de motivation d'espionnage augmente significativement pour les attaques ciblées. Ces chiffres justifient que l'on s'attarde sur ces cas précis.

Les attaques ayant pour finalité l'espionnage représente 12% des attaques de cette étude.

Plusieurs CERTs répondants ont pu documenter de façon plus ou moins précises les tactiques, techniques et parfois les procédures employées par les attaquants. La chaîne d'exécution des attaques a parfois également été renseignée.

Ces données nous offrent un aperçu des tendances en la matière. Dans un souci de lisibilité, nous avons reproduit la chaine d'exécution consolidée de l'ensemble des tactiques, techniques et procédures renseignées dans le cadre des attaques de type espionnage *(cf. en annexe Matrice MITRE ATT&CK)*.

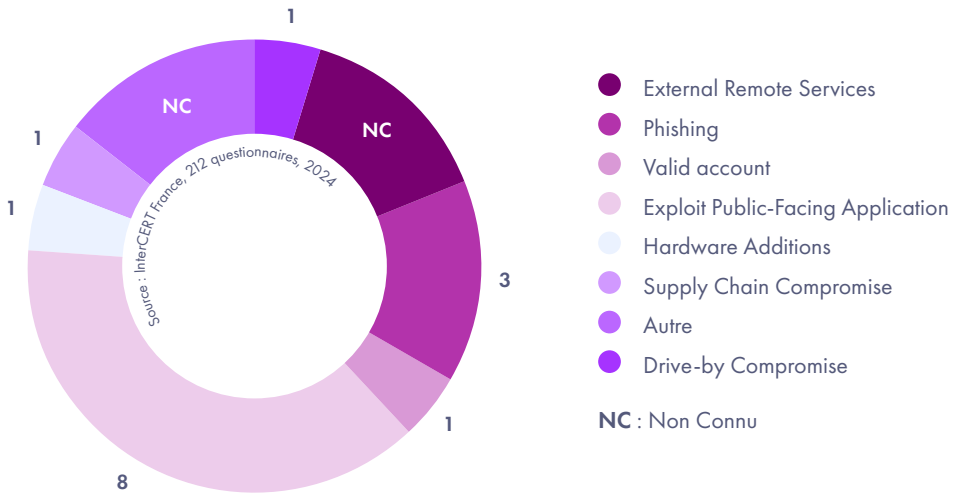
Cette analyse met en lumière une variété de techniques. Toutefois, nous pouvons observer que les techniques Valid Account, Exploit Public-Facing Application et Phishing sont grandement représentées. L'exploitation de vulnérabilités sur des actifs exposés sur Internet, ainsi que le Phishing et Spear Phishing, sont en effet les techniques les plus employées à des fins d'intrusion initiale.

L'évolution de l'écosystème cybercriminel met en lumière le rôle joué par les courtiers en accès initiaux, chargés de la revente d'accès, identifiants, et autres cookies de session offrant un accès initial prêt à l'emploi. Cela souligne également la hausse significative de l'usage d'infostealers, la réutilisation de fuites de données, etc.

La technique Valid Account est en elle-même la clé de voûte de nombreuses attaques réussies, puisqu'elle sert également aux tactiques d'élévation de privilèges, de contournement des défenses et de persistance. Il est à noter que dans 82% des attaques étudiés, un compte admin de domaine a été compromis *(cf. en annexe Matrice MITRE ATT&CK)*.

Le deuxième point visuellement frappant sur la Matrice MITRE ATT&CK consolidée est l'omniprésence de la tactique Exfiltration dont toutes les techniques sont représentées indistinctement. En effet, dans 14 cas sur 20, la tactique « Exfiltration » apparaît. Il est possible d'émettre l'hypothèse que dans les 6 cas restants, l'exfiltration n'a pu se faire du fait de la détection de l'attaque.

Vecteurs initiaux d'intrusion :



ANALYSE DES INCIDENTS CYBER : GESTION, IMPACTS ET ENSEIGNEMENTS CLÉS

De façon générale, l'incident a été géré dans 42% des cas étudiés par un CERT interne. La durée de la crise en jours varie de 0 à 120 jours, avec une moyenne de 14 jours.

La charge de travail en jours-homme au cours de la crise va de 1 à 1000 jours, avec une moyenne de 35 jours.

Dans 60% des attaques traitées, l'organisation n'avait pas les compétences en internes.

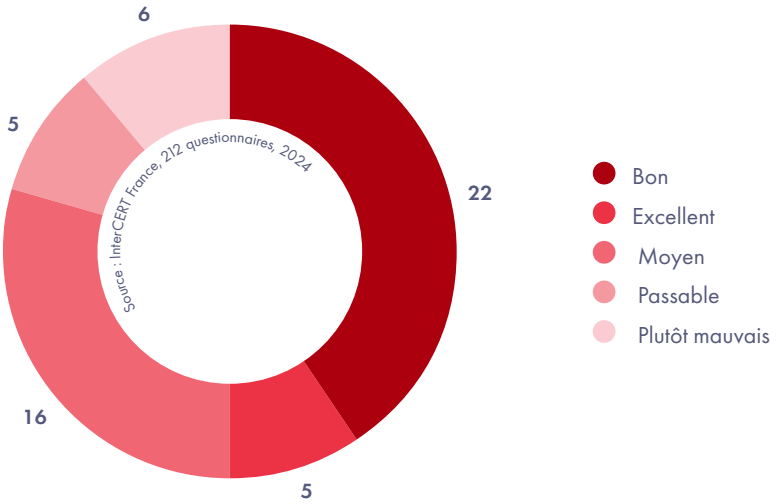
Dans 85% des cas étudiés, l'entité considérait avoir les ressources matérielles en interne. Pour les cas de ressources manquantes figurent les ressources systèmes, l'absence d'outil de détection sur un type de phishing, globalement de SIEM ou d'humains.

Dans un tiers des cas analysés, des logs manquaient pour permettre une analyse fine et une compréhension globale de l'attaque. Parmi les logs manquants figurent principalement ces journalisations : firewall, réseau, SAaS, anti-DDoS, Vpn.

Cet événement a ainsi entraîné la mise en place de nouveaux projets de sécurité ou changements dans les programmes dans un tiers des cas.

Dans 79% des cas analysés, il n'y a pas eu de reconstruction, contre 15% nécessitant de deux jours de reconstruction. Pour une entité la reconstruction fut de 120 jours.

Estimation du niveau de maturité sur la réponse à incident, à la suite d'une reconstruction :



Parmi les éléments de sécurité différenciants dans la résolution de l'incident figurent principalement l'automatisation de la réponse à incident, les alertes EDR/SIEM, les logs, ainsi que la réactivité des équipes.

La moitié des entités concernées n'ont pas effectué de communication interne sur l'incident, tandis que seuls 9% des entités ont effectué une communication externe.

Dans 48% des attaques étudiées, l'entité a prévenu les autorités (parquet, police, gendarmerie, ANSSI, CNIL ...), et dans 36% des cas, une plainte a été déposée.

TLP:CLEAR

SECTION 2

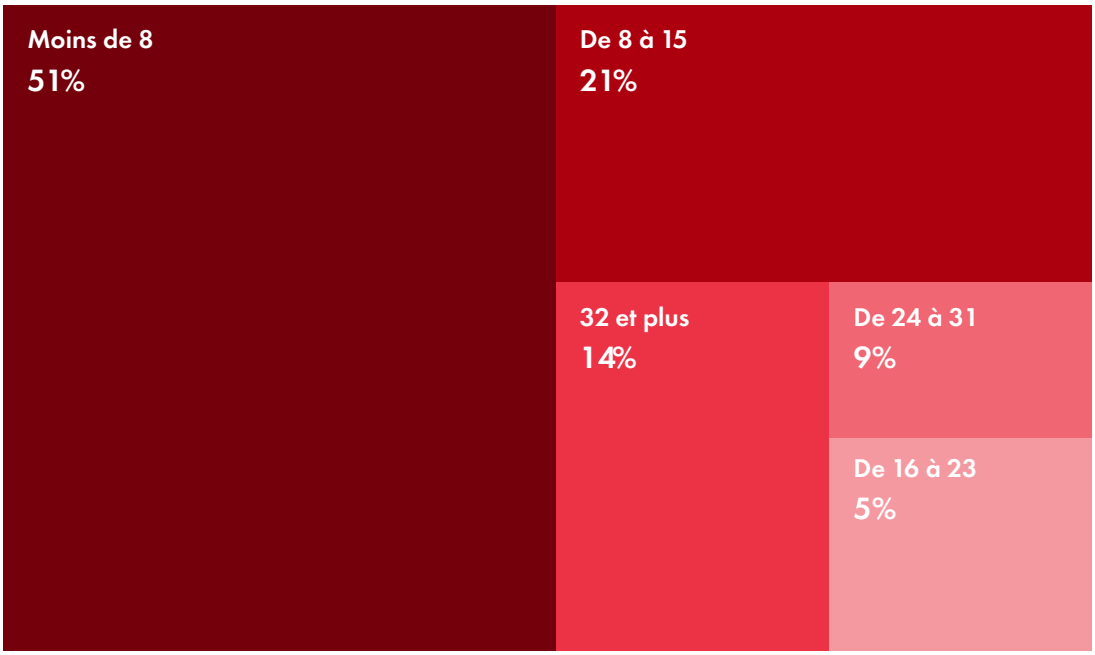
RECOMMANDATIONS ET POINTS DE VIGILANCE

2024

TLP:CLEAR

DÉTECTION ET GESTION DE CRISE

Lorsque l'on a questionné les CERT à propos de la durée des crises qu'ils ont eu à gérer durant l'année 2023, **51%** d'entre eux ont déclaré avoir résolu l'incident en **moins de 8 jours**.

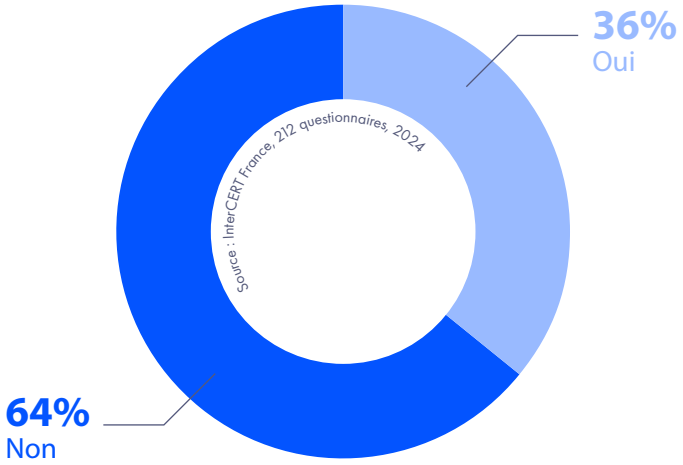


Cependant, il est important de noter le pourcentage significatif de crises (**14%**) dont la durée **excède 32 jours**. Lorsque l'on rentre dans le détail de cette donnée, on peut constater que dans 77% des cas ce sont des CERTs externes qui sont intervenus.

Cette corrélation peut être expliquée par le fait que, le plus souvent, les efforts des CERTs externes sont sollicités lorsque la crise est très avancée, après le déclenchement d'un ransomware par exemple. La tendance des entreprises à externaliser lorsqu'une crise est jugée irrécupérable explique donc la proportion très majoritaire de CERTs externes dans la gestion de crises longues et complexes.

À l'inverse, les équipes de CERT internes vont être amenés à gérer des incidents aux impacts bien moindres qui n'évolueront pas en crises significatives.

De nombreuses victimes ont tendance à prévenir de la présence d'une compromission le plus tard possible, souvent en fin de semaine, quelques heures avant le week-end. Il convient de pousser les entreprises à dépasser cet état de déni, qui empêche les équipes d'intervenir à un stade encore gérable de la crise, et ainsi les faire accepter au plus tôt la présence d'un incident afin de pouvoir agir au plus vite dans le sens d'une résolution.



Au-delà de ces premiers constats, les CERT interrogés s'accordent en grande majorité (**64%**) à dénoncer le **manque de compétences** mis à disposition **en interne** pour la réponse sur incidents.

Plus précisément, c'est le **manque à gagner en termes de compétences cyber et forensic sur lequel nous alertent les CERT**.

En effet, afin d'intercepter les incidents rapidement, il est crucial de déceler et interpréter au plus tôt une situation à risque pour potentiellement chasser un attaquant du réseau avant qu'il ne provoque des dégâts notables. Il est donc primordial pour tout type d'entreprise de mobiliser des moyens afin de superviser son réseau, en interne ou en externe.

C'est en ce sens que les CERT soulignent la nécessité de **garantir une plus grande réactivité dans la détection et l'anticipation d'incidents**.

Pour cela, les entreprises doivent orienter leur stratégie cyber vers la constitution d'équipes d'experts qui seront chargés de mettre en place une **journalisation rigoureuse des réseaux, de l'analyse des logs applicatifs et de développer des alertes**, tant de procédés qui ont été révélés par les membres d'InterCERT comme étant salvateurs et cruciaux pour faire face aux menaces cyber.

Il est également possible d'avoir recours à un service managé qui se chargerait de la supervision du système de l'entreprise non pas en interne mais en externe.

Dans le cas de PME ou TPE qui hésiteraient à dédier une partie de leur budget à la coordination d'une équipe de réponse sur incidents, il est essentiel de rappeler que la supervision de ses infrastructures représente un travail moindre en termes de biens à surveiller et les logs d'application sont moins nombreux que pour une ETI ou une grande entreprise : l'entreprise mobilisera donc moins de ressource et de personnel que ces dernières.

Par ailleurs, une grande majorité de CERT déplore un manque de ressources déployées dans le recrutement d'experts en forensic. L'analyse forensic n'est autre qu'une investigation numérique. Au même titre qu'une enquête de police sur une scène de crime, elle collecte les données électroniques pour comprendre et solutionner une intrusion. Le traitement des données permet d'**établir les différentes étapes de l'attaque** et ses origines. Les experts se reposent sur la concordance des preuves avant d'apposer des conclusions. Les analystes forensics procèdent à de nombreux tests et vérifications pour apporter des éléments de réponse concrets et ainsi limiter les risques de propagations ou de nouvelles intrusions similaires.

Ces enquêtes sont donc précieuses à la fois pour la résolution de ces crises mais également pour la lutte contre les futures cybermenaces : les entreprises ayant fait appel à ces enquêteurs peuvent désormais identifier leurs actifs les plus vulnérables et ainsi mettre en place des stratégies de cybersécurité plus ciblées.

TLP:CLEAR

ANNEXES

2024

TLP:CLEAR

CAS GÉNÉRAL : Procédure immédiate de dépôt de plainte, les bons reflexes

POURQUOI PORTER PLAINTE ?

- Être reconnu comme victime et faire valoir ses droits
- Obtenir le droit à réparation du préjudice subi (LOPMI)
- Bénéficier d'un accompagnement face à des situations complexes (rançons, etc.)
- Obtenir les résultats de l'enquête (connaître l'auteur des faits, être indemnisé, récupérer des données dérobées, déchiffrement)

QUELLES SONT LES ÉTAPES ?

01 Analyser sa situation afin de caractériser efficacement les fait

Il est possible d'obtenir une aide préalable :

- En contactant **la plateforme 17Cyber.**
- **En ligne via le chat internet** du service consacré à la cybercriminalité de la gendarmerie, **ouvert 24/24h**, https://www.gendarmerie.interieur.gouv.fr/contact/echanger-avec-un-gendarme
- ou via le chat de la police nationale, ouvert 24/24h, https://www.masecurite.interieur.gouv.fr/fr

02 Préparer son dossier de dépôt de plainte.

- **Regrouper toutes les traces de cette attaque** (photos, captures d'écran, disques durs etc.) et de récolter un maximum d'éléments de preuve.
- **Retracer la chronologie de vos actions** depuis la détection de l'intrusion jusqu'au dépôt de la plainte. Il est donc préférable de prendre des notes détaillées dont le contenu sera utile pour les équipes CSIRT.

03 Se rendre au commissariat de police ou à la gendarmerie pour déposer plainte

Il est essentiel de déposer sa plainte dans un délai de 72 heures après la découverte de l'attaque.

Ce délai est imposé par l'article 5 de la loi du 24 janvier 2023 d'orientation et de programmation du ministère de l'Intérieur (LOPMI) qui oblige, depuis le 24 avril 2023, tous les professionnels à effectuer un dépôt de plainte dans un délai de 72 heures suivants la connaissance d'une cyberattaque pour pouvoir être indemnisé par leur assureur, sous réserve leur contrat le prévoit. **Ce délai débute à partir de la découverte de la cyberattaque par la victime.**

IMPORTANT

Déposer plainte permet aux autorités de produire des recoupements et des analyses sur les tactiques, techniques et procédures (TTPs) utilisées par les cybercriminels.

Payer la rançon sans faire appel aux autorités compétentes entraîne donc la perte d'informations significatives pour la lutte contre les menaces dans le cyberespace.

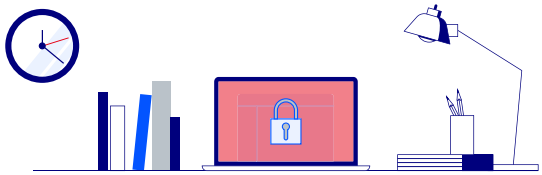
Si des données personnelles d'utilisateurs ont été volées, une déclaration auprès de la CNIL est obligatoire

CONTACTS ET LIENS UTILES

- Pour l'administration, les OIV et toute organisation impliquant des informations classifiées :
  ANSSI (https://cyber.gouv.fr/notifications-reglementaires)
- Dans le cadre d'une violation de données personnelles :
  CNIL (https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles)
- Dans le cas d'une plainte pour une attaque ransomware :
  CSIRT PJ (csirt-pj@interieur.gouv.fr)
- En fonction du secteur d'activité, il est possible de se référer à certains CERT spécifiques (ex : CERT Santé ; COSSIM ; RENATER)
  InterCERT France (intercert-france.fr)

TLP : CLEAR

CAS PARTICULIER : Lors d'une attaque par ransomware, que faire ?



NE PAS PAYER LA RANÇON

On alerte immédiatement les autorités sous **72 heures**

Pourquoi ?

- Car **le paiement d'une rançon ne garantit pas à la victime de récupérer ses fichiers. L'intervention des autorités est le seul moyen d'atteindre ce but**
- Les sociétés assistant la victime dans le paiement de la rançon **peuvent théoriquement être poursuivies pour complicité d'atteinte à STAD et blanchiment**
- En cas de prise de contact avec les auteurs de l'attaque, il est donc fortement recommandé de le faire avec **l'assistance d'un service de police spécialisé qui dispose d'un cadre légal pour ce faire**
- Pensez également à **consulter la Fiche Reflexe** : https://www.intercert-france.fr/fichesreflexes-remediation/files/FicheReflexe-Chiffrement-Endiguement.pdf

Si la rançon a été payée, on alerte immédiatement les autorités sous 72 heures

- Car **ce paiement représente une piste supplémentaire pour l'enquête qui aura lieu pour identifier les attaquants** (ex : adresse de bitcoin, trace de transaction financière)

POUR DÉPOSER PLAINTE

▶ Ce qui ne change pas :

Le dépôt de plainte se fait :

- Soit dans un commissariat ou une brigade de gendarmerie
- Soit en envoyant une lettre plainte au parquet local + une copie numérique au csirt-pj

▶ Ce qui diffère :

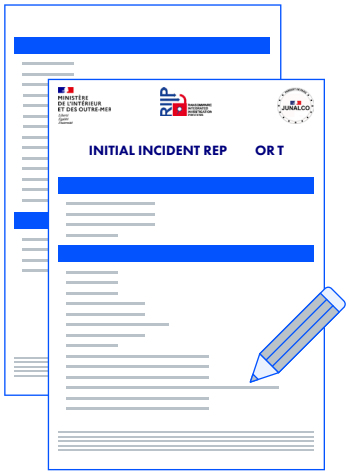
Le contenu des éléments d'identification de l'attaque :

A minima :

- Note de rançon
- Preuves (2 fichiers chiffrés)

Transmettre le formulaire R2IP a annexer à la plainte disponible ci-dessous :

lien : https://www.cyberveille-sante.gouv.fr/sites/default/files/media/document/2024-03/initial%20incident%20report%20v5b.pdf



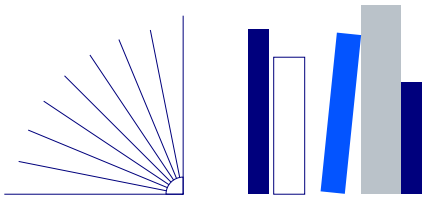
TLP : CLEAR

MATRICE MITRE ATT&CK
pour les attaques motivées par l'espionnage

Resource Development		Initial Access		Execution		Persistence		Privilege Escalation	
Acquire Access		Drive by compromise		Command and Scripting Interpreter	Windows Command Shell	Extemal Remote Services		Valid Accounts	Default Accounts
Acquire infrastructure	Botnet	Exploit Public-Facing Application		User Execution	Malicious File	Server Software Component	Web Shell		Local Accounts
		External Remote Services				Valid Accounts			
		Hardware Additions							
		Phishing							
		Replication Through Removable Media							
		Supply Chain Compromise							
		Valid Accounts	Valid Accounts						
			Local Accounts						

Defense Evasion		Credential Access		Discovery	Lateral Movement		Collection	Command and Control	Exfiltration	Impact
Masquerading	Match Legitimate Name or Location	Brute Force	Password Sproying		Remote Services	Remote Desktop Protocol	Automated Collection	Data Obfuscation	Automated Exfiltration	Data Manipulation
Use Alternate Authentication Material	Application Access Token				Replication Through Removable Media		Data from Network Shared Drive	Multi-Stage Channels	Data Transfer Size Limits	
Valid Accounts					Use Alternate Authentication Material				Exfiltration Over Alternative Protocol	
									Exfiltration Over C2 Channel	Resource Hijacking
									Exfiltration Over Other Network Medium	Service Stop
									Exfiltration Over Web Service	
									Scheduled Transfer	
									Transfer Data so Cloud Account	

TAXONOMIE



Crise de cybersécurité	Une crise « d'origine cyber » se définit par la déstabilisation immédiate et majeure du fonctionnement courant d'une organisation (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, etc.) en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques (cyberattaques de type rançongiciel, déni de service, etc.). La crise nécessite une organisation spécifique à sa remédiation.
Incident de cybersécurité	Un incident de cybersécurité est tout événement qui compromet ou perturbe la confidentialité, l'intégrité ou la disponibilité d'un système d'information. Un incident peut produire un impact sur l'organisation et entrainer la nécessité d'une intervention et d'un rétablissement. Les impacts et les risques peuvent varier selon les organisations et secteurs d'activités.
Campagne	Une campagne est un ensemble d'incidents qui se produisent sur une période de temps spécifique et qui sont liés les uns aux autres par des indicateurs, des outils, une infrastructure ou des TTP partagés qui indiquent qu'ils ont été exécutés par le même ensemble d'intrusions/acteur de menace et/ou ont un objectif partagé.
Intrusion	Un événement de sécurité, ou une combinaison de plusieurs événements de sécurité, qui constitue un incident de sécurité dans lequel un intrus obtient, ou tente d'obtenir, l'accès à un système ou à une ressource système sans avoir l'autorisation de le faire.
Attaque ciblée	Une attaque visant spécifiquement une organisation ou un secteur.
Attaque opportuniste	Une attaque ayant exploité une opportunité présente (une vulnérabilité exploitable, credentials...)

Réponse à incident / Crise	La réponse aux incidents/crises est la pratique qui consiste à examiner et à corriger les campagnes d'attaque actives sur une organisation. Selon l'ampleur de l'incident, elle peut être menée au niveau technique ou managérial et juridique. Généralement, elle consiste (de manière non chronologique) à : • Identifier l'étendue de l'attaque. (Enquête et analyse) • Identifier l'objectif de l'attaque. • Participer à la définition des plans : d'atténuation, de remédiation et de reconstruction • Suivre l'atténuation, la remédiation et le début de la reconstruction. Selon les événements, elle peut requérir l'usage de différentes expertises, nécessiter de la coordination entre équipes, nécessiter la récupération de preuves pour une utilisation dans un cadre juridique...
Reconstruction	Phase lors d'un incident destructif consistant à restaurer le système d'information. Cette phase peut être plus ou moins complexe et longue selon les dégâts réalisés.
Threat Actor / Groupe d'attaquants	Personnes physiques ou morales, opérant avec une intention malveillante. (ANSSI)
MOA *(Mode Opératoire Attaquant)* **/ Intrusion Set**	Ensemble cohérent de techniques, tactiques et procédures (TTP), de codes et d'infrastructures utilisés pour réaliser des attaques informatiques. (ANSSI)
Espionnage	La finalité de l'attaque est d'acquérir du renseignement sur la cible, ou auprès d'elle, et éventuellement de se positionner des moyens (accès, codes) pour une future attaque. Les éléments espionnés peuvent être de différentes natures : communications (courriel, téléphonique...), documents (image, document, géolocalisation...), d'activité humaine ou de ressources...

Influence *(Idéologique, Notoriété, Satisfaction personnelle)*	Les attaques d'influence ont pour but de déstabiliser la cible en mettant à mal sa notoriété ou de revendiquer une position pour des raisons : • Politique, idéologique et/ou religieuse, des idées et/ou des valeurs sociales ou sociétales, • Afin de gagner en notoriété, en visibilité, en influence politique • Satisfaction personnelle : supériorité face à une concurrence ou vis-à-vis de soi-même. • Revanche : d'assouvir un désir de revanche • Destruction : de provoquer des dégâts que l'on veut irréversibles sur les infrastructures.
Lucrative *(Avantage compétitif, Gain financier personnel, Extorsion)*	La finalité de l'attaque est de réaliser des gains financiers de façon directe ou indirecte, par exemple par avantage compétitif ou des gains directs (fraude)...
Déstabilisation *(Dominance, Revanche, Destruction)*	Les attaques de déstabilisation ont souvent comme intérêt de cibler des actifs à haute visibilité pour dominer ou se venger. La finalité de l'attaque est de dégrader les moyens et/ou l'image de la cible afin d'établir une domination sur celle-ci.

Nous tenons à exprimer nos remerciements à l'ensemble des membres qui ont contribué à la Première étude d'incidentologie de l'Intercert France. Votre participation active et votre engagement ont été essentiels pour recueillir des données précieuses et donner naissance à cette analyse inédite. Grâce à vous, nous avons pu dresser un panorama détaillé des incidents, permettant ainsi d'identifier les principaux enjeux et les meilleures pratiques de notre secteur.

Cette étude marque une étape importante vers une meilleure compréhension des risques et la mise en place de stratégies adaptées pour renforcer la sécurité et la résilience de nos organisations. Votre implication témoigne d'un esprit collaboratif et d'un engagement fort au service de l'amélioration continue.

Accenture
Advens
AG2R La Mondiale
Air Liquide - IT - GIO
Airbus SAS
Airbus Protect
AISI
Almond
Alter Solutions
Amadeus
AMOSSYS
ANS
ANSSI
Arkéma
Ariane Group
Association CERT-IST
CERT Aviation
AXA Group Operations
Banque de France
BNP Paribas
BFC
Bouygues Telecom
BPCE
Breizh Cyber
Brigade des Sampeurs Pompiers de Paris
Caisse des Dépôts et Consignations
Cap Gemini
Capgemini CIS
Carrefour
CCF
Colas
ComCyberGend
CNES
Cossim
Crédit Agricole
Crédit Mutuel Arkéa
Crédit Mutuel Euro-Information
CSIRT Ile de France
CYNA
Danone
Dassault Aviation
Dassault Systems
Decathlon
Deloitte Conseil
Devoteam
Evident
CERT ED
EDF
ENEDIS
ENGIE
Equans
ExaTrack
Ernst and Young Advisory
EssilorLuxottica
FiveNines
France Cyber Maritime
Generali VIE
GIE SYnerGIE
GIP Renater
GRT GAZ
Hermès
I-Tracing
Intrinsec Sécurité
Kering
L'Oréal
Le Groupe La Poste
Lexfo
MBDA
Olivier Caleff - Membre Liaison
Paul Rascagnère - Membre Liaison
Metsys
MGEN
Michelin
Ministère de l'Intérieur
Ministère des Armées
Nameshield
Naval Group
KNDS France
ON-X Groupe
Orange
Orange Cyberdefense
Osiris
OVH
Own
Paris 2024
Pernod Ricard
Police Judiciaire
RATP
PwC France
RTE
Safran
SagemCom
Saint Gobain
Schneider Electric
Sekoia.io
SNCF
SNS Security
Société Générale
Sopra Steria Group
STET
STMicroelectronics
Stoïk
Suez
Synacktiv
Synetis
Sysdream
Thales
TotalEnergies SE
Ubisoft International
VADE
Vinci
Wavestone SA
XMCO

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

Conception graphique et mise en page www.aurelielegrand.fr

InterCERT
FRANCE