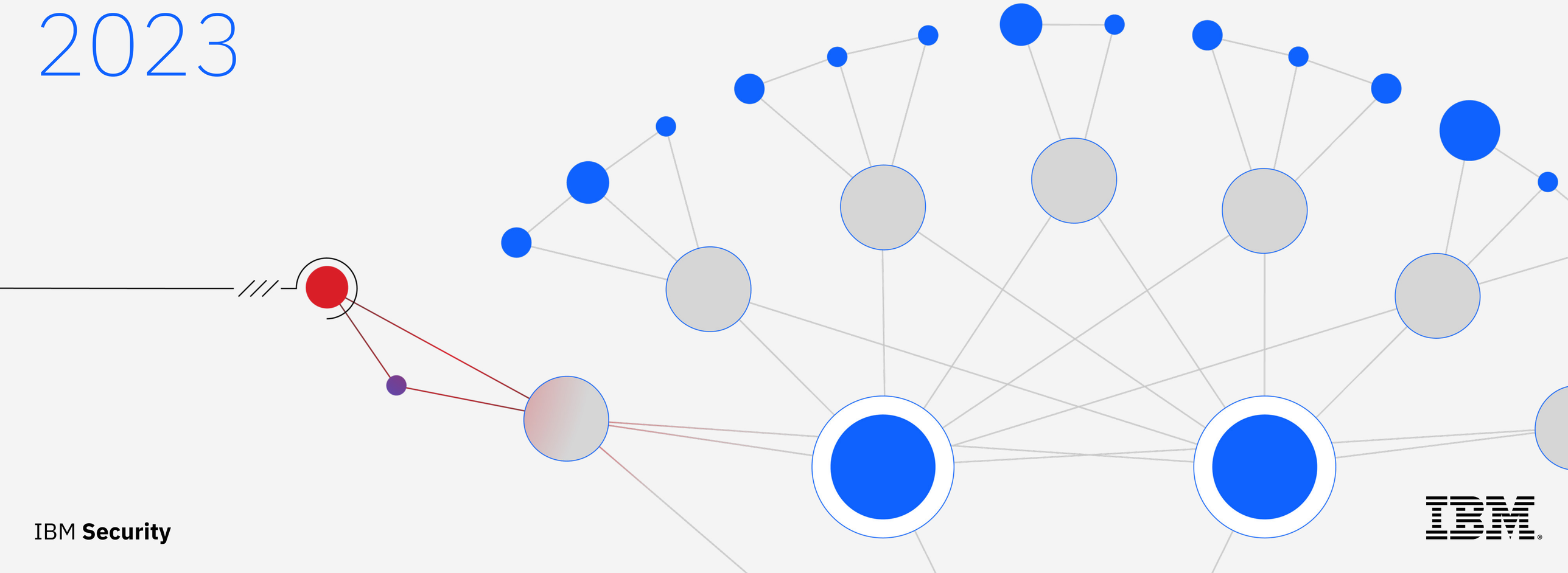
X-Force Threat Intelligence Index 2023

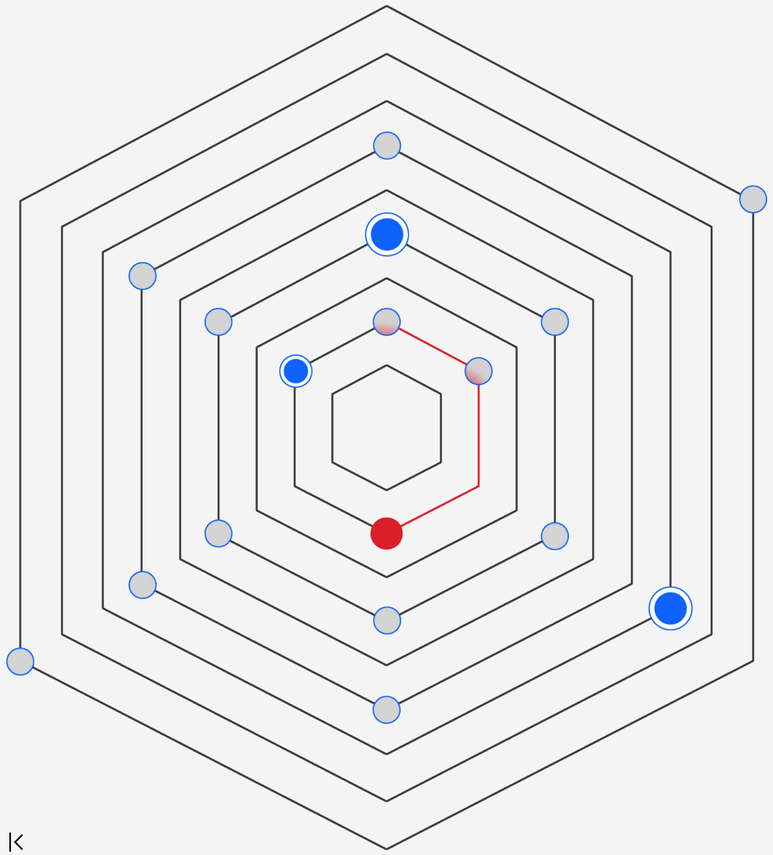


IBM **Security**

Sommaire

01

Synthèse



L’année 2022 fut une année mouvementée pour la cybersécurité et les événements ayant contribué au tumulte n’ont pas manqué. Toutefois, les effets persistants de la pandémie et le déclenchement du conflit armé en Ukraine ont été parmi les plus importants. Les perturbations ont fait de 2022 une année marquée par les bouleversements économiques, géopolitiques et humains, créant exactement le genre de chaos dans lequel les cybercriminels prospèrent.

Et ça a marché !

IBM Security® X-Force® a constaté que des acteurs opportunistes de la menace profitaient du chaos en utilisant le contexte à leur avantage pour infiltrer des gouvernements et des organisations dans le monde entier.

Le rapport IBM Security X-Force Threat Intelligence Index 2023 suit les tendances et les mécanismes d’attaque nouveaux et existants. Il s’appuie sur des milliards de points de données provenant de dispositifs réseau et de terminaux, d’interventions de réponse aux incidents (RI), de bases de données de vulnérabilités et d’exploits, etc. Ce rapport est un recueil complet de nos données de recherche allant de janvier à décembre 2022.

Nous mettons ces résultats à la disposition des clients d’IBM, des chercheurs en cybersécurité, des décideurs, des médias et de la communauté étendue des professionnels de la sécurité et des leaders du secteur. Le paysage instable d’aujourd’hui, avec ses menaces de plus en plus sophistiquées et virulentes, nécessite un effort de collaboration pour protéger les entreprises et les citoyens. Plus que jamais, vous devez disposer de renseignements sur les menaces et d’analyses sur la sécurité pour garder une longueur d’avance sur les attaquants et renforcer vos actifs essentiels.

Et prospérer vous aussi...

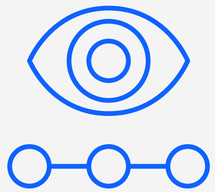
Comment notre analyse des données a changé en 2022

En 2022, nous avons changé notre façon d'examiner certaines de nos données. Ces changements nous permettent d'offrir une analyse plus perspicace et de nous aligner plus étroitement sur les cadres standard du secteur. Cela vous permet de prendre des décisions de sécurité plus éclairées et de mieux protéger votre organisation contre les menaces.

Voici quelques-uns des changements apportés à notre analyse en 2022 :

- **Vecteurs d'accès initial :** l'adoption du cadre MITRE ATT&CK pour suivre plus étroitement les vecteurs d'accès initial nous permet d'aligner plus étroitement nos résultats de recherche sur le secteur de la cybersécurité au sens large et d'identifier les tendances importantes au niveau technique.
- **Exploits et attaques zero day :** grâce à l'extrapolation à partir de notre solide base de données de vulnérabilités, qui compte près de 30 ans de données, nous pouvons contextualiser notre analyse et identifier la menace réelle posée par les vulnérabilités. Ce processus explique également la diminution de la proportion d'exploits utiles et de zero days ayant un impact.
- **Les méthodes des acteurs de la menace et leur impact :** dissocier les mesures prises par les acteurs de la menace de l'impact réel d'un incident nous a permis d'identifier les étapes critiques de celui-ci. Par ailleurs, ce processus nous a permis de mettre au jour des domaines que les intervenants doivent être prêts à gérer à la suite d'un incident.

Faits marquants du rapport



Principales actions sur l'objectif observées : dans près d'un quart de tous les incidents résolus en 2022, le déploiement de portes dérobées (21 %) était la principale action sur l'objectif. Un pic en début d'année avec Emotet, un logiciel malveillant polyvalent, a grandement contribué à l'augmentation de l'activité de porte dérobée observée d'une année à l'autre. Malgré ce pic d'activité, les ransomwares, qui occupaient la première place depuis au moins 2020, représentaient une part importante des incidents (17 %), renforçant ainsi la menace persistante que présente ce logiciel malveillant.

L'extorsion était l'impact le plus courant des attaques sur les organisations : à 27 %, l'extorsion était l'impact privilégié des acteurs de la menace. Les victimes dans le secteur de la fabrication représentaient 30 % des incidents ayant entraîné une extorsion, les cybercriminels continuant ainsi d'exploiter un secteur mis à rude épreuve.

L'hameçonnage était le principal vecteur d'accès initial : l'hameçonnage reste le principal vecteur d'infection, identifié dans 41 % des incidents, suivi par l'exploitation d'applications destinées au public avec 26 %. Les infections par macros malveillantes ont perdu leur attrait, probablement en raison de la décision de Microsoft de bloquer les macros par défaut. L'utilisation de fichiers ISO et LNK malveillants est la principale tactique pour diffuser des logiciels malveillants par le biais de courriers indésirables en 2022.

Augmentation de l'hacktivisme et des logiciels malveillants destructeurs : la guerre en Ukraine a ouvert la porte à ce que de nombreux membres de la communauté de la cybersécurité prévoyaient d'être une démonstration de la façon dont la cybercriminalité favorise la guerre moderne. Bien que les prédictions les plus sombres du cyberespace ne s'étaient pas concrétisées au moment de cette publication, l'hacktivisme et les logiciels malveillants destructeurs ont connu un remarquable essor. X-Force a également observé des changements sans précédent dans le monde de la cybercriminalité avec une coopération accrue entre les groupes cybercriminels et le ciblage d'organisations ukrainiennes par le gang Trickbot.

03

Statistiques clés

27 %

Pourcentage d’attaques avec extorsion

Les acteurs de la menace ont cherché à extorquer de l’argent aux victimes dans plus d’un quart de tous les incidents auxquels X-Force a répondu en 2022. Les tactiques qu’ils utilisent ont évolué au cours de la dernière décennie, une tendance qui devrait se poursuivre à mesure que les acteurs de la menace recherchent plus agressivement à faire des profits.

21 %

Part des incidents impliquant le déploiement de portes dérobées

Le déploiement de portes dérobées a été la principale action sur objectif l’année dernière et concernait plus d’un incident signalé sur cinq dans le monde. L’intervention réussie des défenseurs a probablement empêché les acteurs de la menace d’atteindre d’autres objectifs qui auraient pu inclure des ransomwares.

17 %

Part des attaques impliquant des ransomwares

Malgré une année chaotique pour certains des groupes de ransomwares les plus prolifiques, les ransomwares ont continué de perturber les opérations des organisations et constituaient la deuxième action la plus courante sur l’objectif, suivant de près les déploiements de portes dérobées. La part des incidents liés aux ransomwares est passée de 21 % en 2021 à 17 % en 2022.

41 %

Pourcentage d’incidents impliquant l’hameçonnage comme vecteur d’accès initial
En 2022, les attaques par hameçonnage demeuraient la principale voie de compromission, 41 % des incidents corrigés par X-Force utilisant cette technique pour obtenir un accès initial.

100 %

Augmentation du nombre de tentatives de détournement de conversations par mois
Il y a eu deux fois plus de tentatives de détournement de conversations par mois en 2022 qu’en 2021. Les courriers indésirables menant à Emotet, Qakbot et IcedID ont fortement exploité le détournement de conversations.

52 %

Baisse des kits d’hameçonnage signalés pour récupérer des données de carte bancaire
Les kits d’hameçonnage analysés avaient pour objectif de recueillir des noms (98 %), des adresses e-mail (73 %), des adresses personnelles (66 %) et des mots de passe (58 %). Les informations de carte de crédit, ciblées dans 61 % des incidents en 2021, ont perdu leur attrait pour les acteurs de la menace. En effet, les données indiquent qu’elles étaient ciblées par seulement 29 % des kits d’hameçonnage en 2022, soit une baisse de 52 %.

62 %

Pourcentage d’attaques d’hameçonnage exploitant des pièces jointes de harponnage
Les attaquants ont privilégié les pièces jointes malveillantes, déployées par eux-mêmes ou en combinaison avec des liens ou le harponnage via des services tiers.

26 %

Part des vulnérabilités avec exploits connus en 2022
Vingt-six pour cent des vulnérabilités de 2022 avaient des exploits connus. Selon les données que X-Force a suivies depuis le début des années 1990, cette proportion a diminué ces dernières années, ce qui montre l’avantage d’un processus de gestion des correctifs bien tenu à jour.

31 %

Part des attaques mondiales ciblant la région Asie-Pacifique
L’Asie-Pacifique a conservé la première place en tant que région la plus attaquée en 2022, représentant 31 % de tous les incidents. Ce chiffre représente une augmentation de cinq points de pourcentage par rapport à la part totale d’attaques auxquelles X-Force a répondu dans la région en 2021.

Principaux vecteurs d’accès initial

En 2022, X-Force a délaissé le suivi des vecteurs d’accès initial en tant que catégories plus larges, telles que l’hameçonnage et les identifiants volés, pour se concentrer sur les techniques d’accès initial répertoriées dans le cadre MITRE ATT&CK Matrix for Enterprise. Ainsi, X-Force peut suivre les tendances importantes de manière plus granulaire sur le plan technique. Cela permet également d’obtenir des données plus facilement exploitables et comparables entre elles, en phase avec les efforts de normalisation de l’ensemble du secteur.

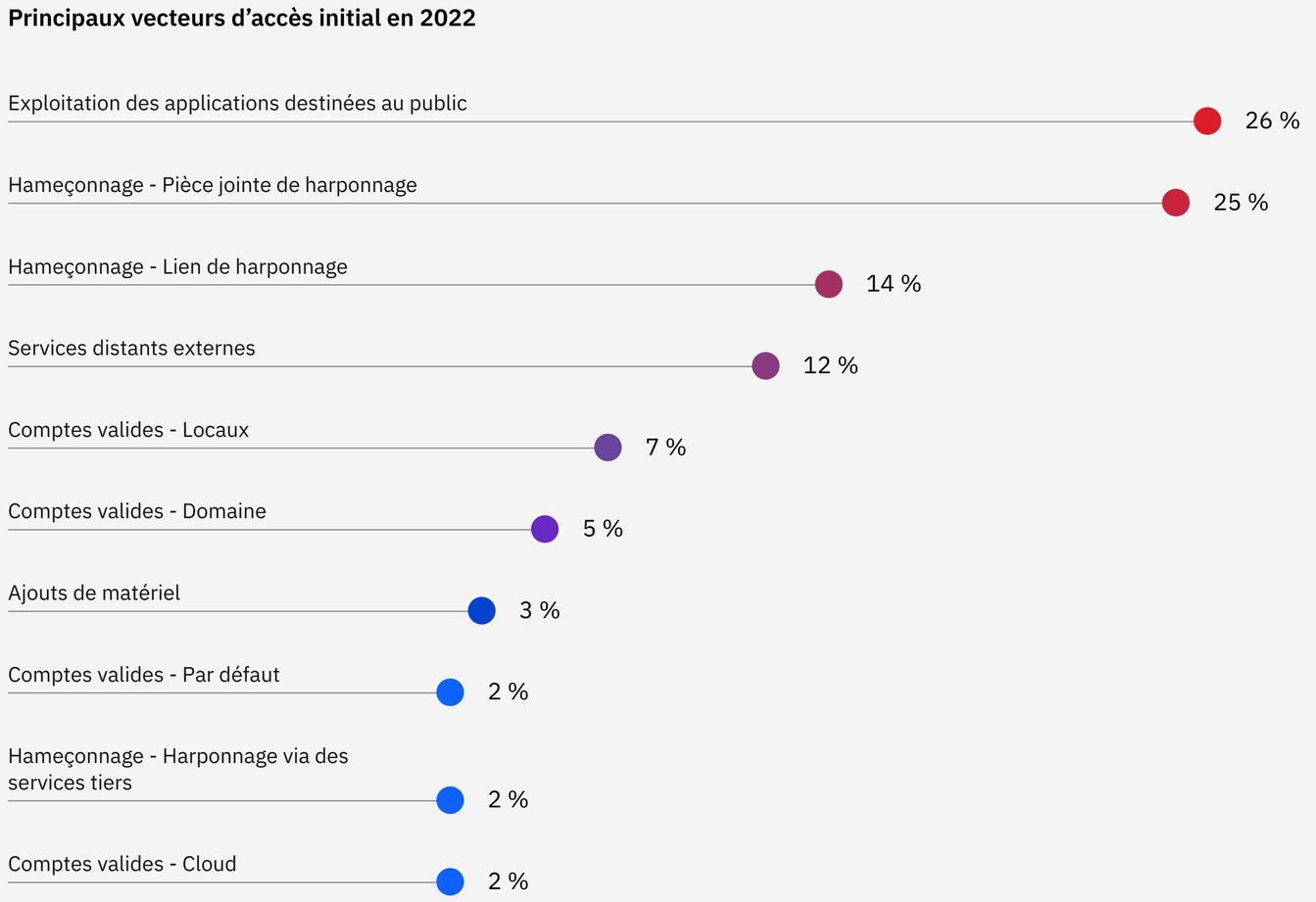


Figure 1 : principaux vecteurs d’accès initial observés par X-Force en 2022. Source : X-Force

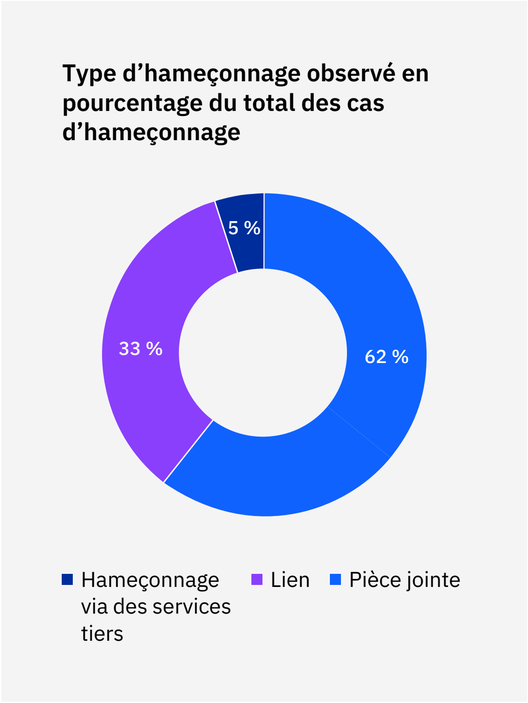


Figure 2 : types de sous-techniques d’hameçonnage en pourcentage du total des cas d’hameçonnage observés par X-Force en 2022. Source : X-Force

Hameçonnage

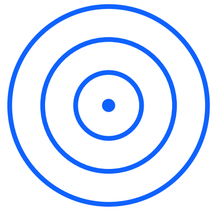
L’hameçonnage (T1566), que ce soit par pièce jointe, lien ou service tiers, reste le principal vecteur d’infection et représentait 41 % de tous les incidents corrigés par X-Force en 2022. Ce pourcentage se maintient depuis 2021, après avoir augmenté de 33 % en 2020. Si l’on considère tous les incidents d’hameçonnage, les pièces jointes de harponnage (T1566.001) ont été utilisées dans 62 % des attaques, les liens de harponnage (T1566.002) dans 33 % des attaques et le harponnage via des services tiers (T1566.003) dans 5 % des attaques. X-Force a également vu des acteurs de la menace utiliser des fichiers joints dans certaines attaques de harponnage via des services tiers ou des liens.

Les données de l’équipe IBM X-Force Red pour 2022 soulignent l’intérêt de l’hameçonnage et des identifiants mal gérés pour les acteurs de la menace. L’équipe X-Force Red a constaté qu’environ 54 % des tests d’intrusion réalisés pour ses clients en 2022 mettaient en lumière une authentification ou une gestion incorrecte des identifiants. L’équipe X-Force Red en charge des services de simulation d’adversaires a régulièrement simulé des attaques de harponnage avec des codes QR ciblant les jetons d’authentification multifacteur (MFA). De nombreuses organisations manquaient de visibilité sur les applications et les terminaux exposés par le biais de la gestion des identités et des accès et les portails d’authentification unique (SSO), tels qu’Okta.

Arrivant en deuxième position, l’exploitation d’applications destinées au public (T1190) - qui consiste à profiter d’une faiblesse d’un ordinateur ou d’un programme connecté à Internet - a été identifiée dans 26 % des incidents traités par X-Force. Ce type d’attaque, appelé « exploitation de vulnérabilité » dans les précédents rapports Threat Intelligence Index, est en baisse par rapport à 2021 (34 %).

L’utilisation de comptes valides (T1078), observée dans 16 % des incidents étudiés, arrive en troisième position. Elle concerne les cas où des pirates informatiques ont obtenu et utilisé de manière abusive des identifiants de comptes existants comme moyen d’accès. Ces incidents comprenaient des comptes cloud (T1078.004) et des comptes par défaut (T1078.001) (2 % chacun) ; des comptes de domaine (T1078.002) (5 %) ; et des comptes locaux (T1078.003) (7 %).

En tant que cible des kits d’hameçonnage, les données de carte de crédit ont connu une forte baisse, passant de 61 % en 2021 à 29 % en 2022.



Les kits d’hameçonnage durent plus longtemps et ciblent les informations identifiant la personne plutôt que les données de carte de crédit

Pour la deuxième année consécutive, IBM Security a analysé des milliers de kits d’hameçonnage du monde entier et a découvert que les déploiements de kits sont opérationnels plus longtemps et touchent plus d’utilisateurs. Les données indiquent que la durée de vie des kits d’hameçonnage observés a plus que doublé d’une année à l’autre, tandis que le déploiement médian est resté relativement faible à 3,7 jours.

Dans l’ensemble, le déploiement le plus court a duré quelques minutes et le déploiement le plus long, découvert en 2022, a duré plus de trois ans. Notre enquête a mis en lumière les points suivants :

- Le tiers des kits déployés ont duré environ 2,3 jours l’an dernier, soit plus du double par rapport à 2021, où la même proportion n’avait pas duré plus d’une journée.
- Environ la moitié de tous les kits signalés ont affecté 93 utilisateurs, alors qu’en 2021, chaque déploiement ne comptait en moyenne pas plus de 75 victimes potentielles.
- Le nombre total maximal de victimes d’une attaque par hameçonnage signalée s’élevait à un peu plus de 4 000, ceci étant toutefois une valeur extrême.
- Presque tous les kits d’hameçonnage analysés (98 %) cherchaient à recueillir des noms. Venaient ensuite les adresses e-mail (73 %), les adresses personnelles (66 %) et les mots de passe (58 %).
- En tant que cible des kits d’hameçonnage, les données de carte de crédit ont connu une forte baisse, passant de 61 % en 2021 à 29 % en 2022.
- Cette baisse indique que les hameçonneurs privilégient les informations identifiant la personne, qui leur offrent des possibilités plus nombreuses et plus malveillantes. Les informations identifiant la personne peuvent être collectées et vendues sur le dark web ou d’autres forums, ou utilisées pour mener d’autres attaques contre des cibles.

Marques les plus usurpées

Les grands noms de la technologie sont aussi les marques les plus usurpées. X-Force estime que ce changement par rapport à la liste un peu plus diversifiée de 2021 est dû à une meilleure capacité à identifier les marques pour lesquelles un kit est configuré, et pas seulement celle qu’il cible par défaut. De nombreux kits d’hameçonnage sont polyvalents et permettent de changer la marque usurpée en modifiant un paramètre simple. Par exemple, un kit peut usurper Gmail par défaut, mais une mise à jour d’une ligne le transforme en une attaque pouvant usurper Microsoft.

Les identifiants volés pour de tels services sont précieuses. L’accès aux comptes que les victimes utilisent pour gérer des volets entiers de leur présence en ligne peut permettre d’accéder à d’autres comptes. Le rapport Cloud Threat Landscape 2022 a mis en lumière le fait que les attaquants mettaient l’accent sur ce type d’accès initial. Selon le rapport, le nombre de comptes cloud annoncés à la vente sur le dark web a plus que triplé (200 %) par rapport à 2021.

Marques les plus usurpées d’une année à l’autre

	2022	2021
1	Microsoft	Microsoft
2	Google	Apple
3	Yahoo	Google
4	Facebook	BMO Harris Bank
5	Outlook	Chase
6	Apple	Amazon
7	Adobe	Dropbox
8	AOL	DHL
9	PayPal	CNN
10	Microsoft Office 365	Hotmail

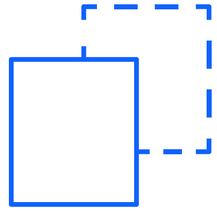
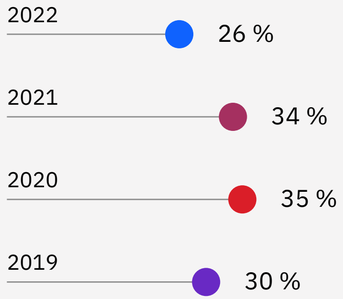


Figure 3 : ce diagramme recense les marques les plus usurpées en 2021 et 2022 et montre que les acteurs de la menace se concentrent de plus en plus sur les grandes marques technologiques. Source : données d’IBM sur les kits d’hameçonnage

Part des incidents résultant de l’exploitation de vulnérabilités au cours des quatre dernières années



Vulnérabilités

L’exploitation de vulnérabilités, rebaptisée « exploitation d’applications destinées au public (T1190) » pour le rapport de 2022, s’est classée au deuxième rang des principaux vecteurs d’infection et constitue une méthode de compromission privilégiée par les attaquants depuis 2019. Des vulnérabilités ont été exploitées dans 26 % des attaques corrigées par X-Force en 2022, contre 34 % en 2021, 35 % en 2020 et 30 % en 2019.

Toutes les vulnérabilités exploitées par les acteurs de la menace n’entraînent pas un cyber-incident. En 2022, le nombre d’incidents résultant de l’exploitation de vulnérabilités a diminué de 19 % par rapport à 2021, après avoir augmenté de 34 % par rapport à 2020. X-Force a estimé que cette évolution était due à la vulnérabilité généralisée de Log4J à la fin de l’année 2021.

L’exploitation pour l’accès est un domaine clé dans lequel l’équipe X-Force Red en charge des services de simulation d’adversaires a poursuivi ses recherches afin de simuler des menaces avancées. L’équipe s’est concentrée davantage sur la recherche de vulnérabilités pour l’exploitation des systèmes d’exploitation et des applications, afin d’élargir l’accès et d’effectuer une escalade des privilèges. Cette orientation était en grande partie due à des exercices antérieurs, avec des clients de longue date, qui ont durci les chemins d’attaque Active Directory traditionnels, et à la nécessité de rechercher de nouveaux chemins d’attaque.

Bien que les vulnérabilités soient un vecteur d’accès initial courant et que le secteur réagisse à plusieurs vulnérabilités majeures au cours d’une année donnée, toutes les vulnérabilités ne se valent pas. Il est important que les décideurs aient une vue d’ensemble du paysage des vulnérabilités et s’assurent qu’ils disposent du contexte nécessaire pour comprendre la menace réelle qu’une vulnérabilité donnée pose pour leurs réseaux.

Il y a près de 30 ans, avant l’avènement du système CVE (Common Vulnerabilities and Exposures, ou vulnérabilités et expositions communes), X-Force s’est lancé dans la création d’une base de données de vulnérabilités robuste. De nos jours, elle fait partie des bases de données les plus complètes dans le secteur de la cybersécurité. Bien que les vulnérabilités constituent un risque majeur pour la sécurité, il existe beaucoup plus de vulnérabilités signalées qu’il n’y a d’exploits. De plus, malgré l’attention du public sur les attaques zero day, le nombre réel d’attaques de ce type est éclipsé par le nombre total de vulnérabilités connues.

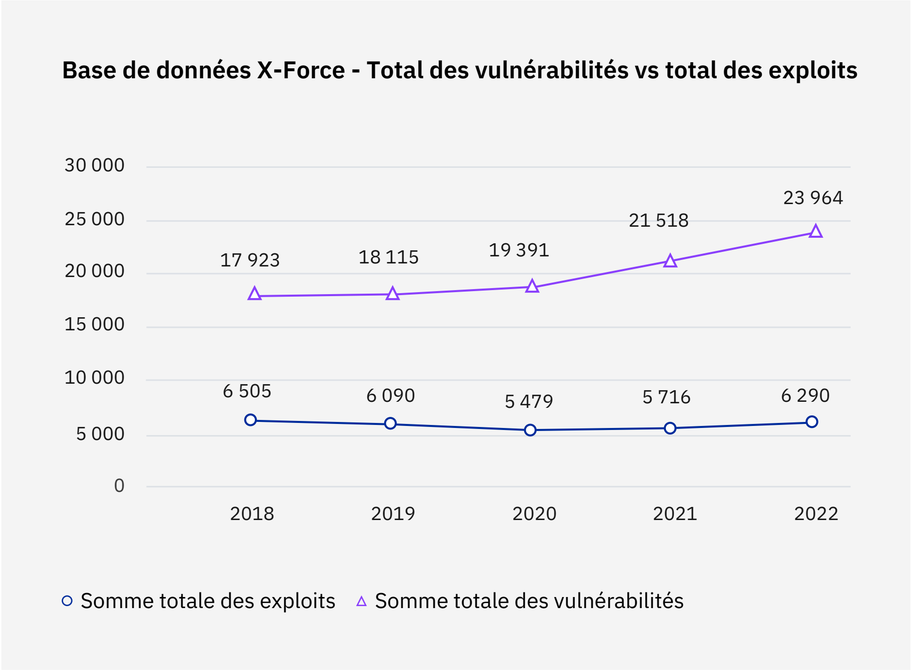


Figure 4 : vue de la base de données de vulnérabilités de X-Force montrant les vulnérabilités et les exploits au cours des cinq dernières années. Source : X-Force

Chaque année, un nombre record de vulnérabilités sont découvertes. En 2022, un total de 23 964 vulnérabilités ont fait l’objet d’un suivi, contre 21 518 en 2021. La tendance à l’augmentation des vulnérabilités d’une année à l’autre s’est poursuivie au cours de la dernière décennie. L’analyse de notre base de données des vulnérabilités a fait le bonheur des défenseurs. En effet, elle a révélé que la proportion d’exploits connus et viables par rapport aux vulnérabilités signalées a diminué ces dernières années. Elle était de 36 % en 2018, 34 % en 2019, 28 % en 2020, 27 % en 2021 et 26 % en 2022.

Ces chiffres peuvent changer avec l’exposition d’attaques zero day et d’exploits développés pour des vulnérabilités plus anciennes - parfois des années après leur identification - et il existe plusieurs explications potentielles à ce recul. À commencer par la mise en place de programmes officiels de bug bounty (programmes de récompenses aux bugs) qui ont encouragé la découverte proactive des vulnérabilités dans les applications. En outre, il existe quelques vulnérabilités très populaires et bien établies qui servent déjà de moyen d’exploitation du système pour les attaquants. Ceux-ci ont ainsi moins besoin de développer de nouveaux exploits.
La baisse observée est probablement due à une combinaison de plusieurs facteurs. Toutefois, cette baisse ne veut pas dire que l’exploitation de vulnérabilités est une menace moins sérieuse.

Alors que la proportion d’exploits par rapport aux vulnérabilités diminue, la gravité des exploits suivis par X-Force a augmenté au cours des cinq dernières années. En 2018, 58 % des vulnérabilités affichaient un score CVSS (Common Vulnerability Scoring System) moyen,

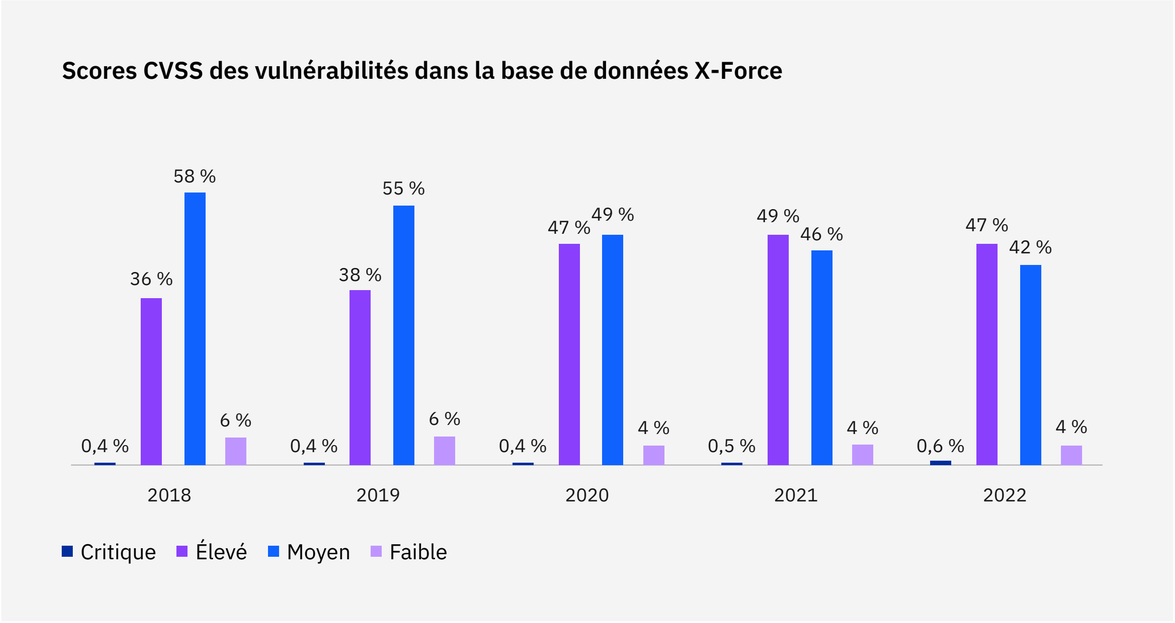


Figure 5 : base de données de vulnérabilités de X-Force montrant la gravité des vulnérabilités suivies dans notre système. Source : X-Force

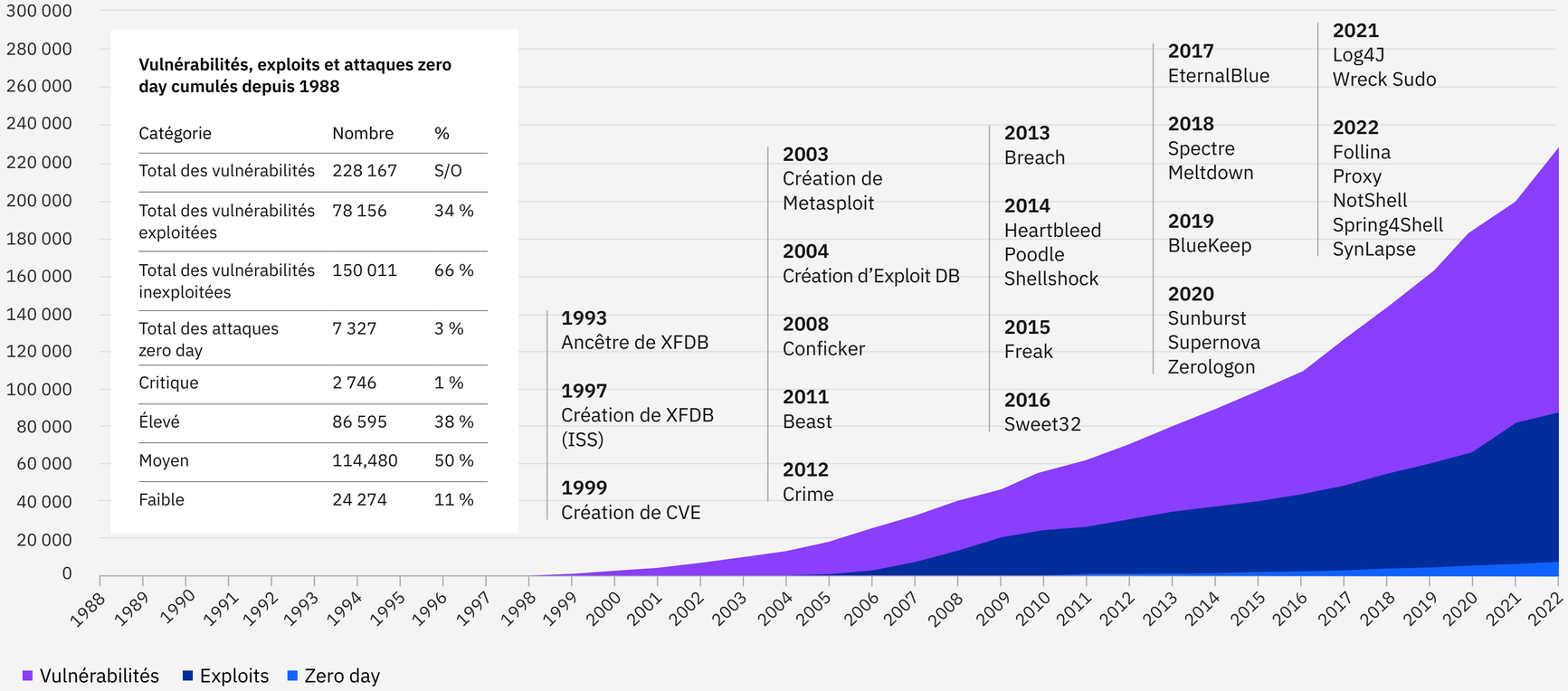
à savoir de 4,0 à 6,9 sur 10, contre un peu moins de 36 % affichant un score élevé (de 7,0 à 9,9). L’écart entre ces deux niveaux s’est inversé en 2021, et les vulnérabilités de gravité élevée représentent maintenant cinq points de pourcentage de plus que celles qui ont obtenu un score moyen.

Pourtant, de toutes les vulnérabilités que X-Force a suivies depuis 1988, 38 % ont un score élevé et seulement 1 % ont un score critique (10). La moitié des vulnérabilités suivies sont classées moyennes, les 11 % restants étant faibles, avec un score de 3,9 ou moins. Ces scores seuls ne sont pas corrélés à la gravité réelle d’une CVE, car ils ne tiennent pas compte de la façon dont l’exploitation est accomplie, ni même de l’existence ou non d’un exploit. Cependant, les scores aident les défenseurs à comparer les vulnérabilités et à prioriser leur prise en charge.
Le diagramme de la figure 6 à la page suivante permet de mettre en perspective la véritable nature du problème des vulnérabilités auquel est confronté le secteur de la cybersécurité.

Vulnérabilités de la technologie opérationnelle (TO)

Les vulnérabilités des systèmes de contrôle industriel (SCI) découvertes en 2022 ont diminué pour la première fois en deux ans, soit 457 en 2022 contre 715 en 2021 et 472 en 2020. Cela s’explique en partie par les cycles de vie des SCI et la façon dont ils sont généralement gérés et corrigés. Les attaquants savent qu’en raison des exigences en matière de temps d’arrêt minimaux, des longs cycles de vie des équipements et des logiciels plus anciens et moins pris en charge, de nombreux composants de SCI et réseaux TO demeurent exposés à des vulnérabilités plus anciennes. En général, l’infrastructure est en place pendant beaucoup plus longtemps que les postes de travail de bureau standard, ce qui prolonge la durée de vie des vulnérabilités spécifiques aux SCI au-delà de celles qui peuvent exploiter l’informatique.

Le problème de la vulnérabilité



Vulnérabilités, exploits et attaques zero day cumulés depuis 1988

Catégorie	Nombre	%
Total des vulnérabilités	228 167	S/O
Total des vulnérabilités exploitées	78 156	34 %
Total des vulnérabilités inexploitées	150 011	66 %
Total des attaques zero day	7 327	3 %
Critique	2 746	1 %
Élevé	86 595	38 %
Moyen	114,480	50 %
Faible	24 274	11 %

Figure 6 : diagramme montrant la croissance des vulnérabilités, des exploits et des attaques zero day depuis 1988. On y trouve également une chronologie des événements majeurs impliquant des vulnérabilités depuis 1993. XFDB signifie « X-Force Database » et Exploit DB signifie « Exploit Database ». Source : X-Force

Principales actions sur l’objectif

Auparavant, le rapport X-Force Threat Intelligence Index examinait la vaste catégorie des principales attaques. Pour son rapport de 2022, X-Force a divisé cette catégorie en deux catégories distinctes : les mesures spécifiques prises par les acteurs de la menace sur les réseaux ciblés, ou « action hostile sur l’objectif », et l’effet prévu ou avéré de cette action sur la victime, ou « impact ».

Selon les données des services de réponse aux incidents d’IBM Security X-Force, le déploiement de portes dérobées était l’action sur l’objectif la plus courante, se produisant dans 21 % de tous les incidents signalés. Viennent ensuite les ransomwares (17 %) et la compromission d’e-mails professionnels (Business Email Compromise ou BEC) (6 %). Les documents malveillants (maldocs), les campagnes de spam, les outils d’accès distant et l’accès au serveur représentaient chacun 5 % des incidents.

Principales actions sur l’objectif en 2022

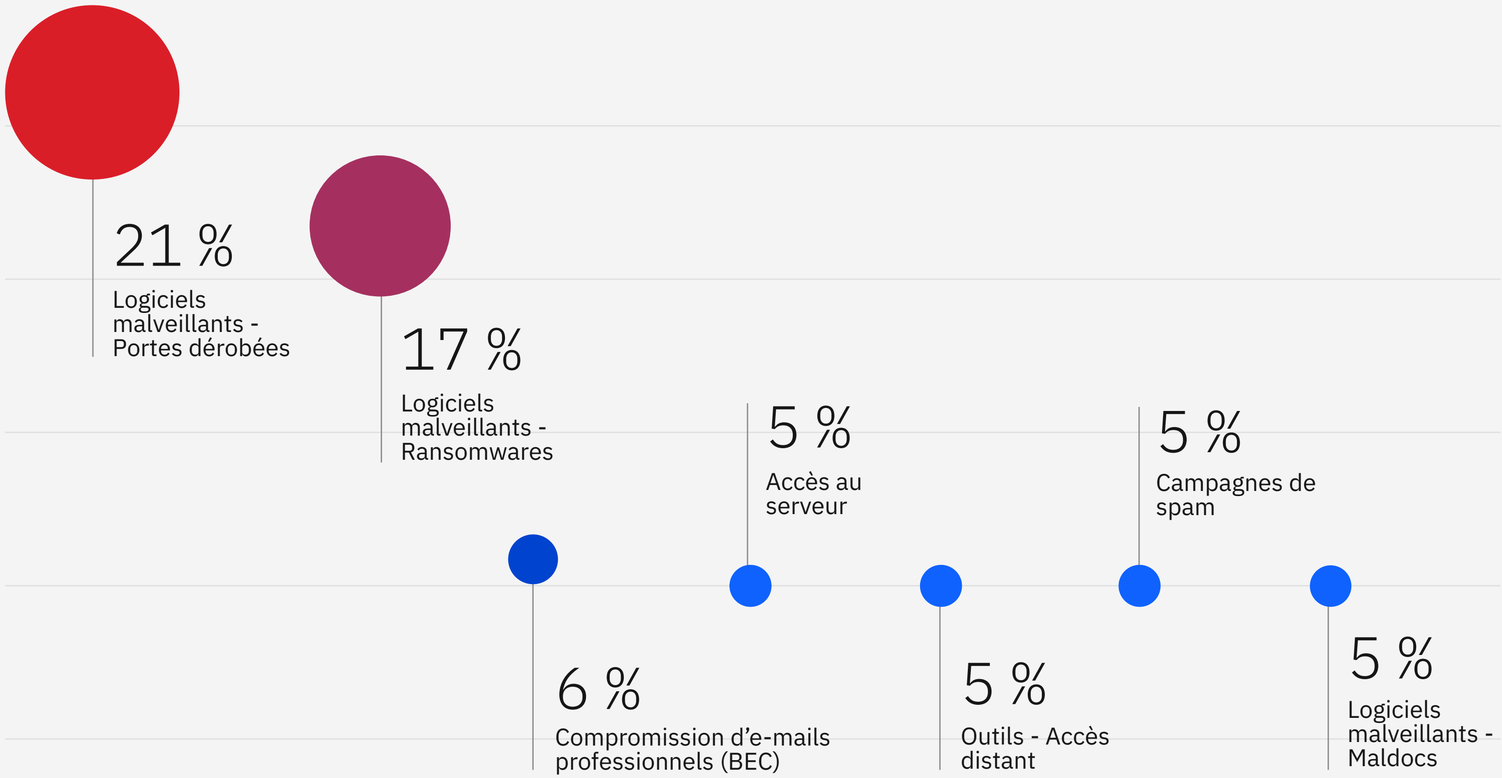


Figure 7 : principales actions sur l’objectif observées par X-Force en 2022. Source : X-Force

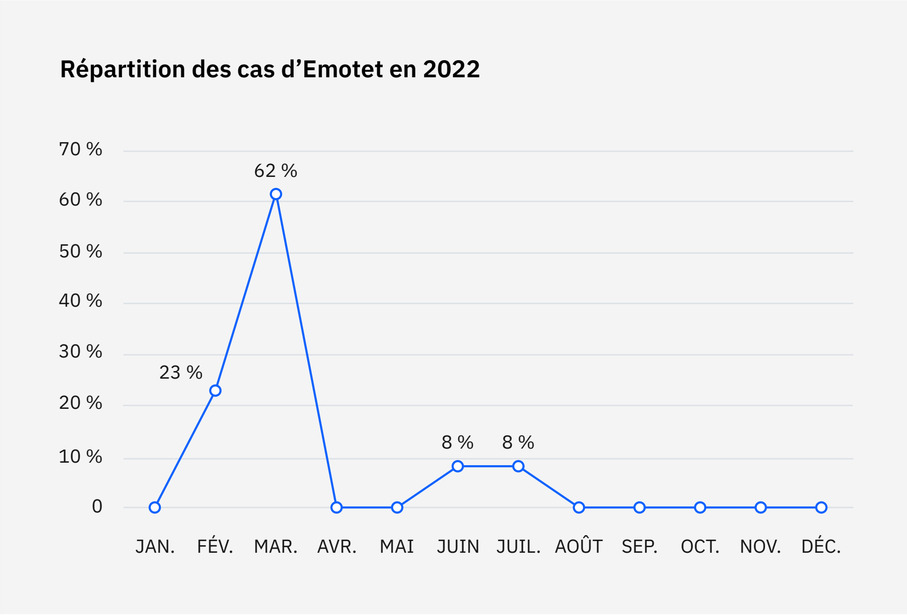


Figure 8 : diagramme montrant le pic de cas d’Emotet au début de l’année 2022. Source : X-Force

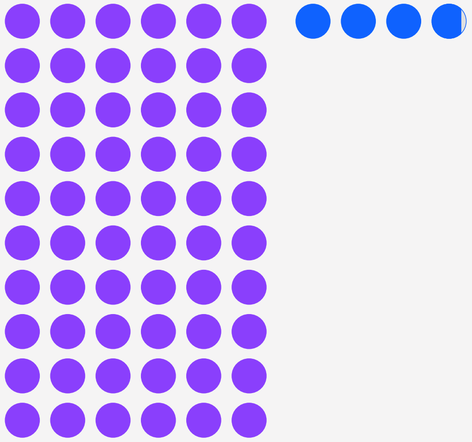
Dans les cas où un déploiement de porte dérobée a été classé comme une action sur l’objectif, il est probable que l’acteur de la menace avait d’autres intentions lorsque la porte dérobée est devenue opérationnelle. L’intervention réussie des équipes de sécurité ou des intervenants en cas d’incident a probablement empêché l’acteur de la menace d’atteindre d’autres objectifs. Les logiciels malveillants faisaient probablement partie de cette activité malveillante supplémentaire, étant donné que les deux tiers de ces cas de porte dérobée portaient la signature d’une attaque par ransomware.

Le déploiement accru de portes dérobées peut également être dû aux sommes d’argent que ce type d’accès peut générer sur le dark web. L’accès à un réseau d’entreprise compromis à partir d’un courtier d’accès initial se vend généralement pour plusieurs milliers de dollars. Ce type d’accès peut intéresser les acteurs malveillants qui souhaitent faire de l’argent rapidement en évitant les problèmes liés au maintien de l’accès, tout en se déplaçant latéralement et en exfiltrant des données de grande valeur. Les portes dérobées peuvent aussi présenter un intérêt pour les acteurs malveillants qui n’ont pas accès aux logiciels malveillants requis pour établir eux-mêmes l’accès.

En général, les courtiers d’accès initial tentent de vendre leurs accès aux enchères. Selon les observations de X-Force, les prix vont de 5 000 à 10 000 dollars. Toutefois, les prix finaux peuvent être inférieurs. D’autres sources ont signalé des accès vendus à des prix allant de 2 000 à 4 000 dollars, un accès ayant même atteint les 50 000 dollars. Par comparaison et à titre d’exemple, le prix d’une carte de crédit était nettement inférieur, avec un prix annoncé inférieur à 10 dollars.

Les portes dérobées ont conduit à un pic considérable d’infections par Emotet en février et mars. Ce pic a fortement gonflé le classement des cas de portes dérobées, car celles déployées dans ce laps de temps représentaient 47 % de toutes les portes dérobées identifiées dans le monde en 2022. Suite à la pause d’Emotet de juillet à novembre (il a ensuite repris pendant près de deux semaines à un volume beaucoup plus faible), le nombre de cas de portes dérobées a considérablement diminué.

Durée moyenne d’une attaque par ransomware



Ransomwares

Malgré une année chaotique pour certains des groupes de ransomwares les plus prolifiques, les ransomwares ont continué de perturber les opérations des organisations et constituaient la deuxième action la plus courante sur l’objectif, suivant de près les déploiements de portes dérobées. La part des incidents liés aux ransomwares est passée de 21 % en 2021 à 17 % en 2022.

Selon une étude réalisée par IBM Security X-Force, la durée moyenne des attaques par ransomware a diminué de 94,34 % entre 2019 et 2021, passant de plus de deux mois à un peu moins de quatre jours. Néanmoins, les ransomwares constituent un danger immédiat qui ne cesse de s’étendre et ne semble pas s’essouffler.

La compromission des contrôleurs de domaine est un moyen particulièrement préjudiciable que les attaquants utilisent pour distribuer leurs ransomwares sur un réseau. Un petit pourcentage (environ 4 %) des résultats des tests de pénétration réseau réalisés par X-Force Red a révélé que des erreurs de configuration dans Active Directory pouvaient exposer certaines entités à une escalade de privilèges ou à une prise de contrôle totale du domaine. En 2022, X-Force a également observé des attaques par ransomware plus agressives sur l’infrastructure sous-jacente, telle que ESXi et Hyper-V. L’impact potentiellement élevé de ces techniques d’attaque souligne l’importance de sécuriser correctement les contrôleurs de domaine et les hyperviseurs.

Variantes de ransomwares

Les groupes de ransomwares et les courtiers d’accès associés vont et viennent et X-Force a constaté une attrition régulière parmi les principaux groupes actifs dans cet espace. X-Force a identifié 19 variantes de ransomwares en 2022, contre 16 en 2021. Les variantes de LockBit représentaient 17 % du total des attaques par ransomware observées, contre 7 % en 2021. Phobos et WannaCry arrivaient tous deux en deuxième position avec 11 %. REvil, également appelé Sodinokibi, qui représentait 37 % des cas en 2021, a été détrôné par les principaux groupes. Revil et Ryuk, qui arrivait en deuxième position avec 13 % en 2021, sont tous deux passés à 3 % en 2022.

LockBit 3.0 est la dernière variante de la famille de ransomwares LockBit qui fait partie d’une opération de ransomware en tant que service (RaaS) associée à LockerGoga et MegaCortex. LockBit est opérationnel depuis septembre 2019 et LockBit 3.0 a été publié en 2022. Une partie importante du code source de LockBit 3.0 semble avoir été empruntée au ransomware BlackMatter.

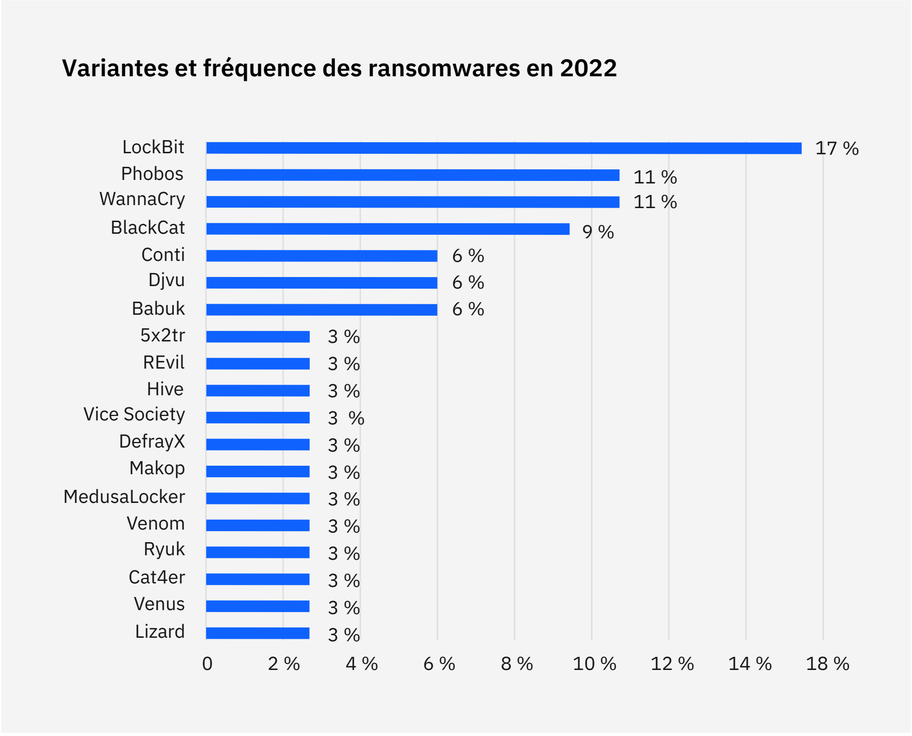


Figure 9 : variantes de ransomwares et fréquence à laquelle les services de réponse aux incidents d’IBM Security X-Force les ont observées en 2022. Source : X-Force

Les chercheurs ont découvert le ransomware Phobos au début de 2019. Sur la base des similitudes dans le code, des mécanismes de livraison, des techniques d’exploitation et des notes de rançon, Phobos a été identifié comme une variante des familles de ransomwares Crysis et Dharma identifiées auparavant. Phobos a été couramment utilisé pour des attaques à plus petite échelle, qui impliquent des demandes de rançon moindres. Les campagnes d’hameçonnage par e-mail et l’exploitation de ports RDP (Remote Desktop Protocol) vulnérables sont les principales méthodes de distribution observées pour Phobos.

WannaCry, apparu pour la première fois en 2017, se propage en utilisant EternalBlue pour exploiter la vulnérabilité du serveur Microsoft Server Message Block 1.0 (SMBv1) (MS17-010). Plusieurs cas de WannaCry ou de Ryuk observés par X-Force en 2022 résultaient d’infections datant d’il y a trois à cinq ans. Se produisant sur des équipements anciens non corrigés, ces incidents soulignent l’importance d’un nettoyage approprié après de tels événements.

Compromission d’e-mails professionnels (BEC)

La compromission d’e-mails professionnels (Business Email Compromise ou BEC) a conservé sa troisième place en 2022, avec 6 % des incidents auxquels X-Force a répondu. Ce chiffre est légèrement inférieur à celui de 2021 (8 % des attaques) et de 2020 (9 % et cinquième place). La compromission d’e-mails professionnels a détrôné l’accès au serveur, qui arrivait en deuxième position en 2021. Ce type d’attaque se produit lorsqu’un agresseur accède à un serveur à des fins inconnues. En 2022, ces attaques ont été classées de manière plus granulaire, en fonction du type d’accès obtenu par les attaquants. Des liens de harponnage ont été utilisés dans la moitié des attaques BEC auxquelles X-Force a répondu. Les pièces jointes malveillantes et l’utilisation abusive de comptes valides ont été utilisées pour permettre des tentatives de BEC dans 25 % des cas chacune.

Principaux impacts

X-Force a également examiné de plus près l'effet des incidents sur les organisations victimes, afin de mieux comprendre l'impact recherché par les acteurs de la menace à travers des incidents auxquels X-Force a répondu. Grâce à ces informations, les organisations sont en mesure de mieux comprendre les effets les plus courants afin de planifier plus efficacement les interventions en cas d'incidents potentiels à l'avenir.

L'analyse a révélé que plus d'un incident sur quatre visait à extorquer des fonds aux organisations ciblées, ce qui en fait le principal impact observé dans les incidents corrigés par X-Force. Les cas d'extorsion observés étaient le plus souvent le fruit de ransomwares ou de compromissions d'e-mails professionnels et comprenaient souvent l'utilisation d'outils d'accès distant, de cryptomineurs, de portes dérobées, de téléchargeurs et de web shells.

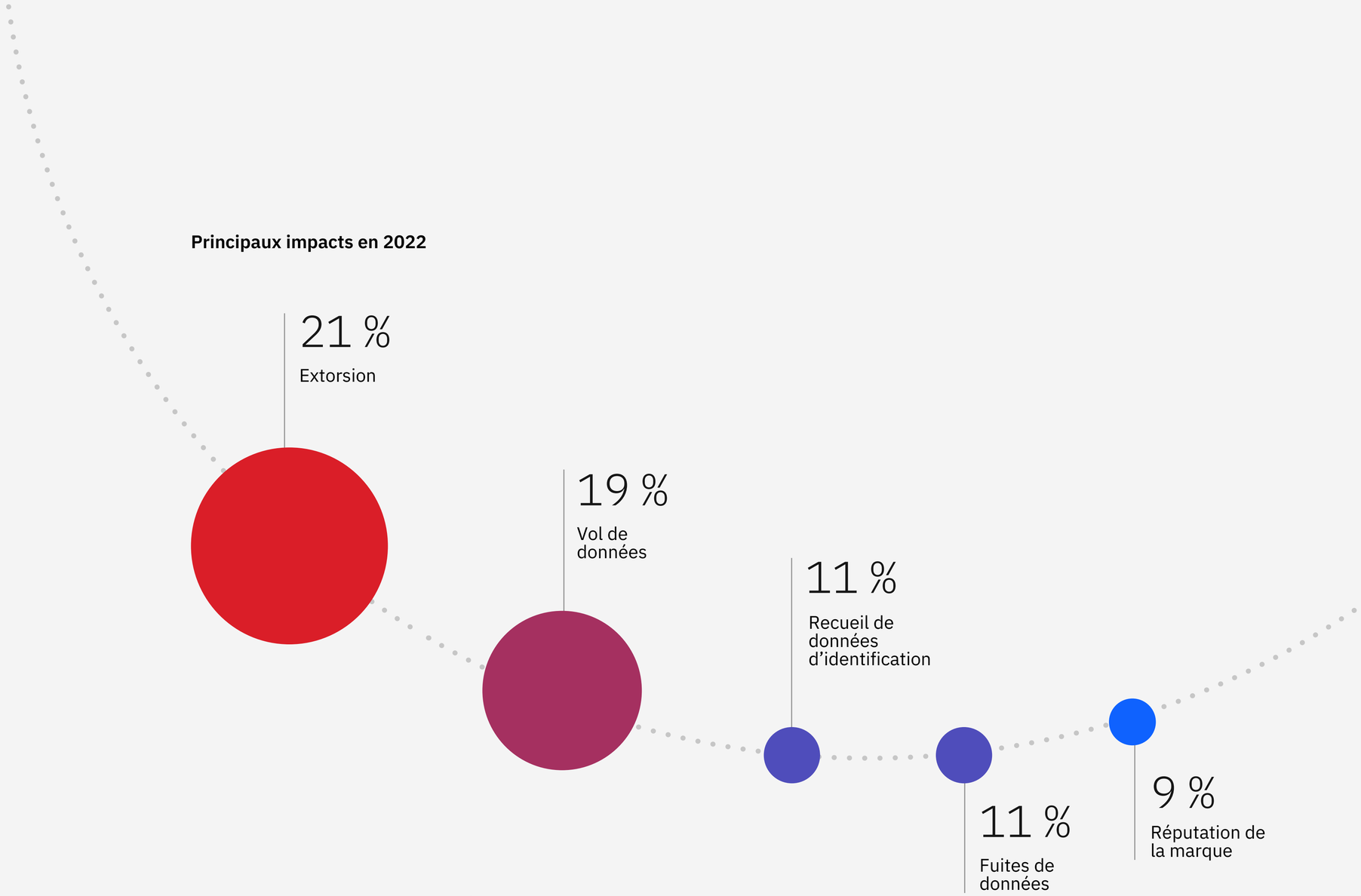


Figure 10 : principaux impacts observés par X-Force lors de ses interventions de RI en 2022. Source : X-Force

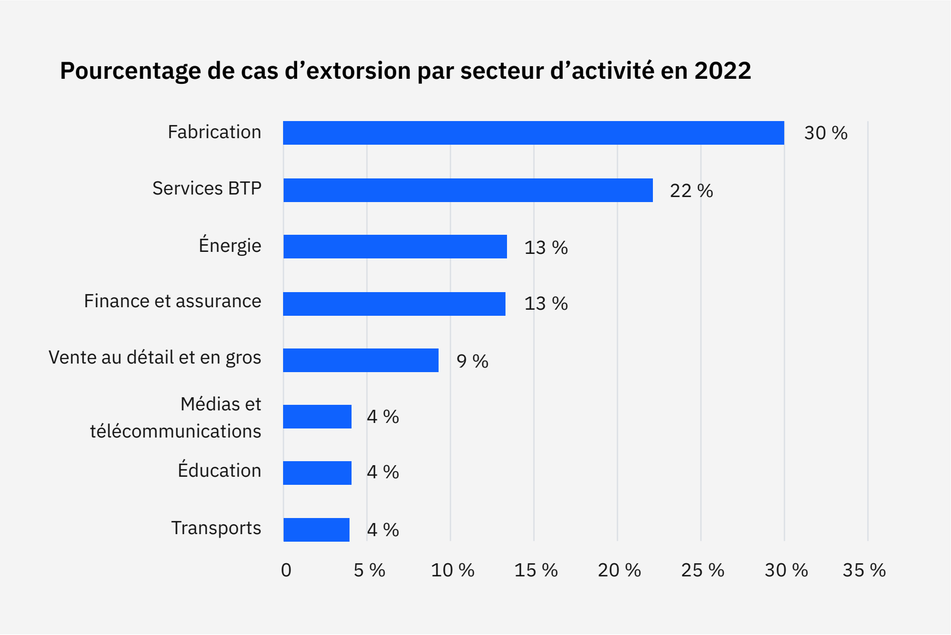


Figure 11 : pourcentage de cas d’extorsion par secteur d’activité observés par X-Force lors de ses interventions de RI en 2022. Les chiffres ayant été arrondis, leur somme n’est pas égale à 100 %.
Source : X-Force

Le vol de données arrive en deuxième position et représente 19 % de tous les incidents corrigés par X-Force. Le recueil de données d’identification ayant conduit au vol de noms d’utilisateur et de mots de passe et ayant nécessité des mesures d’atténuation appropriées représentait 11 %. Les incidents où X-Force pouvait identifier des informations ciblées réellement divulguées après avoir été volées étaient moins fréquents que le vol de données à 11 %. Les incidents affectant la réputation de la marque, tels que la perturbation des services que les organisations fournissent à leurs clients, représentaient 9 % des incidents (voir l’annexe pour la liste complète des impacts suivis par X-Force). Les incidents qui ont eu un impact sur la réputation de la marque des organisations ciblées étaient principalement des attaques par déni de service distribué (DDoS). Celles-ci sont aussi souvent utilisées pour faire chanter les victimes afin qu’elles paient pour mettre fin à l’attaque.

Développements marquants dans l'extorsion en ligne[1-9]

Année	Événement	Tactique
2013	Cryptolocker, l'une des premières épidémies majeures de ransomware	Chiffrement de données
2014	DDoS 4 Bitcoin, Armada Collective	DDoS aléatoire
2015	Avec le ransomware Chimera arrive la menace de fuite de données volées en ligne	Double extorsion
2017-2018	BitPaymer et SamSam	Big game hunting (ou chasse au gros gibier)
2020	Attaque par ransomware de Vastaamo	Triple extorsion

Extorsion

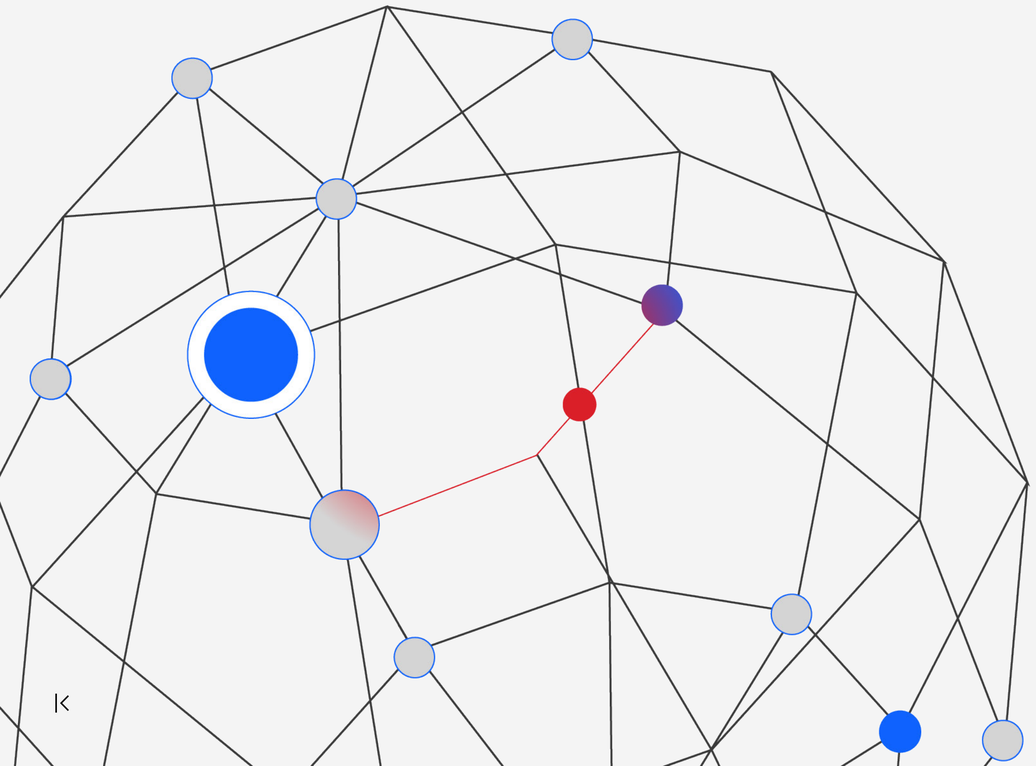
Bien qu'à l'heure actuelle l'extorsion soit le plus souvent associée aux ransomwares, les campagnes d'extorsion ont inclus diverses méthodes pour exercer une pression sur leurs cibles. Ces méthodes incluent notamment les menaces d'attaques DDoS, le chiffrement de données et, plus récemment, des menaces de double et de triple extorsion combinant plusieurs éléments précédemment observés.

Une autre tactique qu'au moins un groupe de ransomwares a testée à partir de 2022 consistait à rendre les données volées plus accessibles aux victimes en aval. En permettant aux victimes secondaires d'identifier plus facilement leurs données lors d'une fuite de données, les opérateurs cherchent à renforcer la pression exercée sur l'organisation ciblée en premier lieu par le groupe de ransomwares ou un affilié. En 2023, X-Force s'attend à ce que les acteurs de la menace utilisent une notification améliorée ou nouvelle des victimes en aval afin d'augmenter les coûts potentiels d'une intrusion sur le plan juridique et de la réputation.

Souvent, les défenseurs et les victimes de cyberattaques se concentrent sur les impacts observés qu'a subis l'organisation. Cependant, il importe de tenir compte des intentions des acteurs de la menace, de leurs capacités et de leur évolution au fil du temps. Cette approche permet de mieux discerner comment les capacités pourraient évoluer à l'avenir. Compte tenu des options d'extorsion toujours plus nombreuses et de l'objectif principal de gain financier des acteurs de ransomwares, l'équipe X-Force estime que les acteurs de la menace vont continuer de faire évoluer et de développer leurs méthodes d'extorsion pour trouver de nouvelles façons de faire pression sur les victimes pour qu'elles paient.

07

Activités cybernétiques liées à la guerre en Ukraine



Les cyberactivités parrainées par l'État russe suite à son invasion de l'Ukraine n'ont pas, au moment de cette publication, entraîné les attaques généralisées et à fort impact redoutées à l'origine par les entités gouvernementales occidentales. Cependant, la Russie a déployé un nombre sans précédent de wipers (effaceurs) contre des cibles en Ukraine, ce qui souligne son investissement continu dans les capacités destructrices des logiciels malveillants. En outre, l'invasion a conduit au regain d'opérations d'hacktivisme entreprises par des groupes sympathisants de l'un ou l'autre camp, ainsi qu'à une réorganisation du paysage cybercriminel de l'Europe de l'Est.

Compte tenu des capacités avancées avérées de la Russie en matière de cyberattaques contre les infrastructures critiques depuis 2015, les agences internationales de cybersécurité ont émis un avertissement en avril 2022. L'avertissement faisait mention de cyber-opérations potentiellement importantes et de perturbations connexes en Ukraine et ailleurs. X-Force a évalué les menaces les plus importantes qui sont apparues, y compris le retour de l'hacktivisme et de wipers, ainsi que des changements importants dans le monde de la cybercriminalité. La plupart de ces opérations ciblaient des entités basées en Ukraine, en Russie et dans les pays voisins, mais certaines se sont également étendues à d'autres régions.

Par ailleurs, les défenseurs ont tiré parti des progrès réalisés en matière de détection, de réponse et de partage de l'information qui ont été développés au cours des dernières années. Une grande proportion des tentatives précoces d'attaque par wiper ont été rapidement identifiées, analysées et rendues publiques. Ces attaques comprenaient au moins huit wipers identifiés, ainsi qu'une cyberattaque russe qui visait le réseau électrique ukrainien et qui a été découverte et déjouée en avril 2022.

Dans le cyberespace, les effets les plus largement ressentis de la guerre en cours proviennent de groupes hacktivistes autoproclamés qui soutiennent les intérêts nationaux ukrainiens ou russes. De nombreux groupes se sont formés depuis l'invasion russe et opèrent contre les réseaux russes et ukrainiens pour marquer des points politiques. Killnet est l'un des groupes les plus prolifiques favorables à la Russie. Il a revendiqué des attaques DDoS contre des services publics, des ministères, des aéroports, des banques et des compagnies d'énergie basés dans des États membres de l'Organisation du traité de l'Atlantique Nord (OTAN), des pays alliés en Europe, ainsi qu'au Japon et aux États-Unis. Les entités qui correspondent au profil de ciblage de Killnet devraient s'assurer que des mesures d'atténuation des attaques DDoS sont en place, par exemple en faisant appel aux services d'un fournisseur tiers d'atténuation des attaques DDoS.

Chronologie de certains événements hacktivistes en 2022

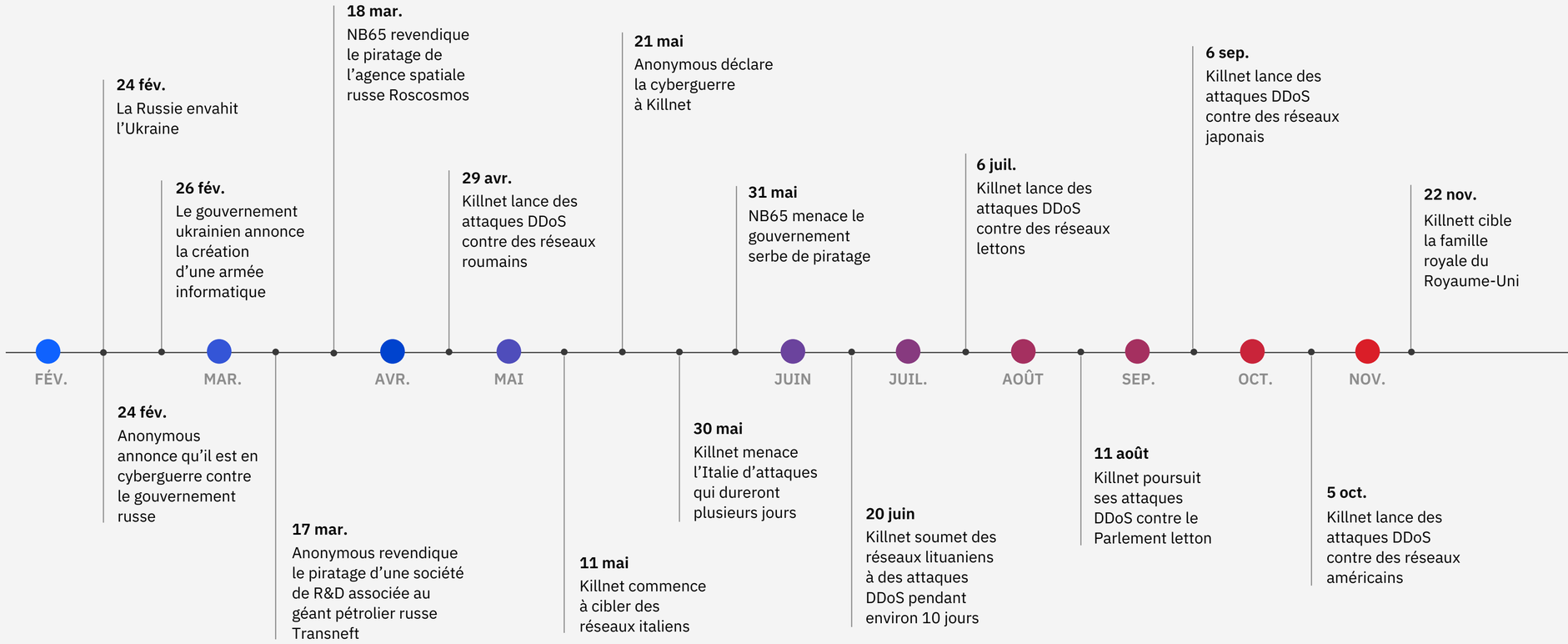


Figure 12 : image montrant les événements hacktivistes observés jusqu'ici dans le cadre du conflit en Ukraine. Source : analyse X-Force de rapports de sources ouvertes

Wipers utilisés dans le cadre de la guerre en Ukraine

La guerre en Ukraine se distingue par l'utilisation de plusieurs familles de wipers déployées contre de multiples cibles en succession rapide et à une échelle jamais vue auparavant, ainsi que par l'utilisation de logiciels malveillants parallèlement à des opérations militaires cinétiques.

Ces déploiements incluent au moins neuf nouveaux wipers : AcidRain, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, DoubleZero, AwfulShred, OrcShred et SoloShred. Ces wipers ont été principalement utilisés contre les réseaux ukrainiens avant l'invasion initiale et jusqu'aux premiers stades de la guerre, principalement de janvier à mars 2022. Bien que les wipers aient été utilisés dans le passé, il s'agissait principalement de campagnes indépendantes contre un ensemble limité de cibles. Cependant, les exceptions notables que sont WannaCry et NotPetya, qui se propagent sans discernement après avoir touché leurs victimes initiales, soulèvent des inquiétudes quant à la propagation plus large de ces wipers ou à leur réutilisation pour des opérations malveillantes ailleurs.

X-Force estime que les acteurs de cybermenaces parrainés par l'État russe constituent toujours des menaces importantes pour les réseaux informatiques et les infrastructures critiques dans le monde entier. Ce jugement est basé sur des cyber-opérations russes de longue date visant des réseaux ukrainiens, européens, de l'OTAN et américains, et des attaques lancées par des groupes russes depuis 2015.

Bouleversement parmi les groupes de cybercriminels russes

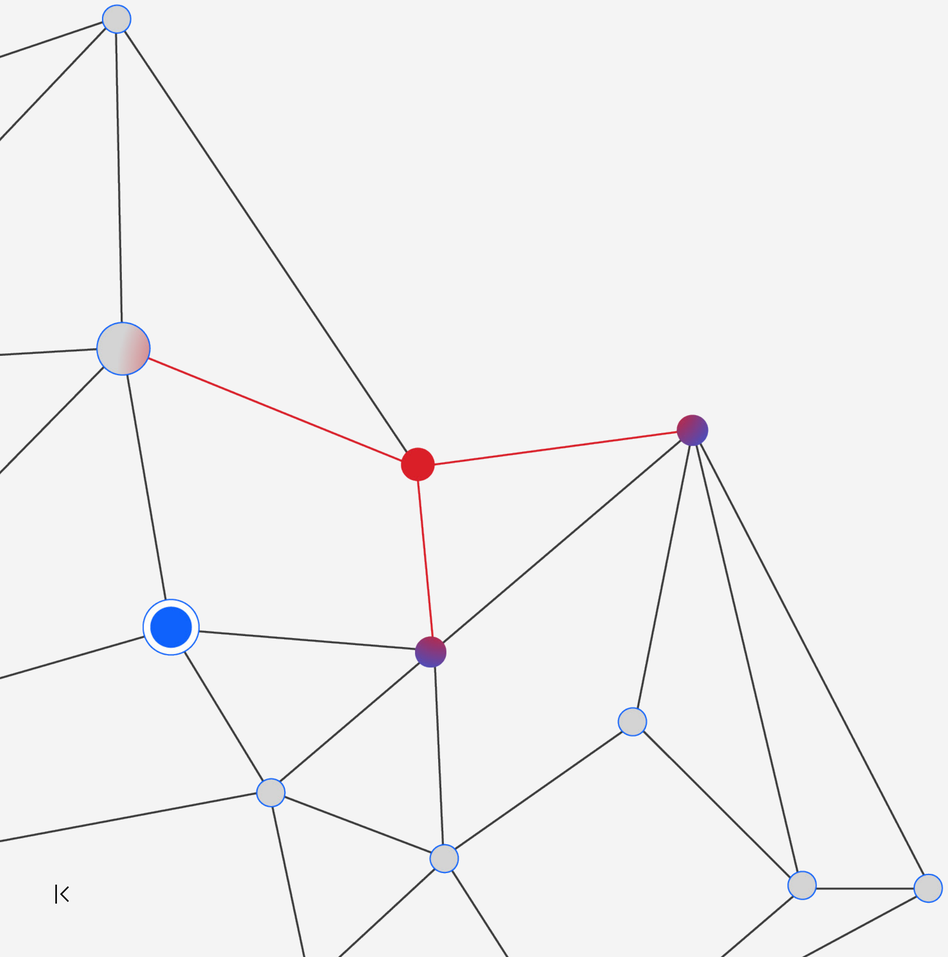
2022 fut une année mouvementée pour ITG23, l'un des plus importants groupes de cybercriminels russes, principalement connu pour avoir développé le cheval de Troie bancaire Trickbot et le logiciel malveillant Conti. Le groupe a subi une série de fuites très médiatisées au début de l'année 2022, après avoir publiquement soutenu l'implication de la Russie dans la guerre. Appelées ContiLeaks et TrickLeaks, ces fuites ont entraîné la publication de milliers de messages de discussion et la divulgation malveillante d'informations personnelles (doxing) de nombreux membres du groupe. X-Force a été en mesure de prouver que l'ITG23 s'est lancé dans des attaques systématiques à partir de la mi-avril et au moins jusqu'à la mi-juin 2022 , ce qui constitue un changement sans précédent, car le groupe n'avait jamais ciblé l'Ukraine auparavant.

En outre, le groupe a apparemment retiré deux de ses familles de logiciels malveillants les plus en vue, Trickbot et Bazar, et a mis fin à son opération de ransomware Conti. Selon diverses sources, un remaniement important du personnel pourrait se produire, le groupe se scindant en plusieurs factions et certains membres passant à autre chose.

Le retrait de Trickbot et Bazar, qui représentaient un nombre important d'infections en 2021, a provoqué un vide qui a été rapidement comblé par des familles de logiciels malveillants telles que Emotet, IcedID, Qakbot et Bumblebee. Avant de le retirer, ITG23 déployait encore le ransomware Conti à une cadence élevée et celui-ci représentait un tiers de toutes les interventions sur ransomwares réalisées par X-Force au premier trimestre de 2022.

Le groupe a également publié une nouvelle version de son logiciel malveillant Anchor, une porte dérobée furtive que le groupe déployait habituellement contre des cibles de premier plan. La version améliorée découverte par X-Force, et nommée AnchorMail, dispose d'un nouveau mécanisme de communication avec le serveur de commandement et de contrôle (C2) basé sur la messagerie électronique. Le serveur C2 utilise les protocoles SMTP (Simple Mail Transfer Protocol Secure) et IMAPS (Internet Message Access Protocol Secure), et le logiciel malveillant communique avec le serveur en envoyant et en recevant des e-mails spécialement conçus.

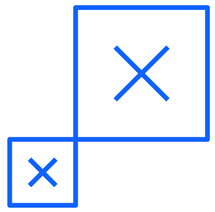
Paysage des logiciels malveillants



Hausse des vers propagés par les clés USB

Après que X-Force ait observé des tentatives d'infection par Raspberry Robin affectant des organisations à la mi-mai 2022, le ver énigmatique a commencé à se propager rapidement dans les réseaux des victimes au travers d'utilisateurs partageant des clés USB (Universal Serial Bus). Les infections ont grimpé au début du mois de juin et, début août, Raspberry Robin atteignait un pic, avec 17 % des tentatives d'infection observées par X-Force. Ce pic a été observé dans les secteurs du pétrole et du gaz, de la fabrication et des transports. Le taux de tentatives d'infection de 17 % dans ces secteurs est considérable, puisque moins de 1 % des clients X-Force au total ont observé ce logiciel malveillant. X-Force a également constaté une activité accrue de Raspberry Robin entre septembre et novembre 2022.

La propagation de vers via les clés USB est rendue possible par l'ingénierie sociale et nécessite un accès physique, que ce soit par un utilisateur légitime ou par d'autres moyens, à un réseau ou à un terminal pour l'infecter avec succès. X-Force vous conseille de vérifier que vos outils de sécurité bloquent les logiciels malveillants diffusés par clés USB connus, de réaliser une formation de sensibilisation à la sécurité et de désactiver les fonctions d'exécution automatique pour tout support amovible. Dans les environnements particulièrement sensibles, tels que les environnements de TO ou les environnements physiquement isolés, il est plus sûr d'interdire l'utilisation des clés USB. Si vous devez autoriser leur utilisation, outre la mise en œuvre des suggestions précédentes, contrôlez rigoureusement le nombre approuvé d'appareils portables à utiliser dans votre environnement.



Rust gagne en popularité

Le langage de programmation Rust n'a cessé de gagner en popularité auprès des développeurs de logiciels malveillants en 2022, grâce à sa prise en charge multiplateforme et à ses faibles taux de détection antivirus par rapport à d'autres langages plus courants. Semblable au langage Go, il s'accompagne également d'un processus de compilation plus alambiqué, ce qui peut rendre son analyse plus chronophage pour les rétro-ingénieurs. Plusieurs développeurs de ransomwares ont publié des versions Rust de leurs logiciels malveillants, notamment BlackCat, Hive, Zeon et, plus récemment, RansomExx. De plus, X-Force a analysé un crypteur ITG23 écrit en Rust, ainsi que la famille de portes dérobées et de téléchargeurs CargoBay. La popularité croissante de Rust témoigne de la volonté de l'écosystème des ransomwares d'innover pour échapper à la détection.

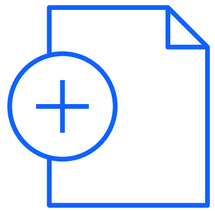
Vidar InfoStealer

X-Force a noté un afflux soudain de logiciels malveillants Vidar InfoStealer qui a commencé en juin 2022 et s'est poursuivi jusqu'au début de l'année 2023. Observé pour la première fois en 2018, Vidar est un cheval de Troie voleur de données, distribué comme logiciel malveillant en tant que service (MaaS). Le cheval de Troie est généralement exécuté par les utilisateurs qui cliquent sur des liens ou des pièces jointes malveillants dans des spams malveillants (malspam). En raison de son vaste ensemble de fonctionnalités, Vidar peut être utilisé pour récupérer une grande variété d'informations sur l'appareil, notamment des informations de carte de crédit, des noms d'utilisateur, des mots de passe et des fichiers, ainsi que pour prendre des captures d'écran du bureau de l'utilisateur. Vidar peut également voler des portefeuilles de crypto-monnaie Bitcoin et Ethereum.

Les attaques par l'intermédiaire d'un voleur de données (info stealer) sont généralement motivées par des raisons financières. Les données volées sont analysées et toute information précieuse est rassemblée et organisée dans une base de données.

Cette base de données peut ensuite être vendue sur le dark web ou via l'application de messagerie privée Telegram. Les acteurs de la menace peuvent utiliser ces informations pour commettre divers types de fraude, comme demander des prêts bancaires ou des cartes de crédit, acheter des articles en ligne ou faire des réclamations d'assurance maladie frauduleuses.

Ils peuvent utiliser des identifiants de connexion compromis pour accéder à des comptes d'entreprise et à des services distants. L'utilisation d'un voleur de données coûte environ 250 dollars par mois en moyenne, et les utilisateurs déploient le logiciel malveillant de leur choix. X-Force voit régulièrement des places de marché tenter de vendre des accès dérobés à l'aide de logiciels malveillants voleurs de données à un prix allant de 10 à 75 dollars. Lorsque l'accès a été obtenu, les acteurs de la menace peuvent facilement utiliser les privilèges du compte piraté comme point de départ pour lancer d'autres activités malveillantes.



Évolution des mécanismes de diffusion des logiciels malveillants

De plus en plus, les logiciels malveillants sont distribués via des documents Microsoft Office malveillants, généralement joints à des e-mails d'hameçonnage. Les développeurs de logiciels malveillants ont créé ces documents qui contiennent des macros conçues pour exécuter des logiciels malveillants lorsque le document est ouvert. L'utilisation de macros à cette fin est devenue si répandue que les produits Microsoft Office ont commencé à inclure des avertissements de sécurité lors de l'ouverture de documents prenant en charge les macros. À partir de juillet 2022, Microsoft bloquait l'exécution des macros par défaut dans les documents reçus par courrier électronique ou téléchargés sur Internet.

Au fur et à mesure que les défenseurs renforçaient leurs capacités de détection et de prévention, les acteurs de la menace ont abandonné Visual Basic Application (VBA) au profit des macros Excel 4.0, un format de macro plus ancien dans Microsoft Excel. Les documents Excel malveillants sont utilisés depuis un certain temps. Cependant, la plupart des mécanismes de sécurité ont été développés autour des macros VBA dans les documents Excel. Pendant un certain temps, les macros Excel 4.0 offraient un bon moyen d'échapper à la détection. À peu près à la même époque, certains acteurs de la menace ont commencé à envoyer des liens dans un e-mail menant vers un site d'injecteur (dropper) pour télécharger les documents malveillants plutôt que de les envoyer en pièce jointe. Microsoft ayant apporté des modifications pour permettre aux administrateurs de désactiver les macros Excel 4.0 et de bloquer l'exécution des macros téléchargées à partir d'Internet, les acteurs de la menace ont été contraints de changer à nouveau de tactique.

Après les changements apportés par Microsoft, de nombreux auteurs de logiciels malveillants utilisent encore des documents Microsoft Office compatibles avec les macros, mais des groupes sophistiqués ont adopté une chaîne d'infection plus complexe. Ces nouvelles tactiques impliquent une combinaison de fichiers HTML contenant un code binaire ou un fichier compressé protégé par un mot de passe. Ces fichiers contiennent également une image ISO qui peut contenir un fichier LNK, un fichier CMD ou d'autres types de fichiers peu susceptibles d'être envoyés à un destinataire d'e-mail ou téléchargés sur Internet. D'autres incluent l'injection de modèles à distance ou l'exploitation de vulnérabilités. CVE-2021-40444, une vulnérabilité d'exécution de code à distance dans Microsoft HTML (MSHTML), en est un exemple. Un composant logiciel est utilisé pour le rendu des pages web dans Microsoft Windows afin d'exécuter le logiciel malveillant, plutôt que de s'appuyer sur des macros.

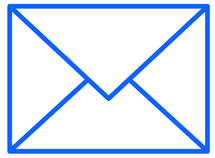
Les données relatives aux courriers indésirables mettent en évidence la menace des ransomwares et illustrent une fois de plus les tendances macroéconomiques

X-Force a analysé les tendances en matière d'hameçonnage et de courriers indésirables pour mieux comprendre leur efficacité globale et leur utilisation par les acteurs de la menace. L'enquête a révélé que des courriers indésirables ont été utilisés régulièrement tout au long de l'année pour diffuser des logiciels malveillants, tels qu'Emotet, Qakbot, IcedID et Bumblebee, qui conduisent souvent à des infections par ransomware.

Logiciels malveillants[10-18]	**Ransomwares**
Trickbot	*Conti*
Bazarloader	*Conti*, Diavol
IcedID	*Conti*, Quantum
Bumblebee	*Conti*, Diavol, Quantum
Emotet	*Conti*, BlackCat, Quantum
Qakbot	*REvil*, *Conti*, Black Basta
SocGholish	LockBit

Les données de ce tableau couvrent la période allant de fin 2021 à la publication de ce rapport. L'italique indique que le logiciel malveillant ou le ransomware a été vu en 2022, mais qu'il n'a pas été observé par X-Force depuis au moins octobre 2022.

X-Force a constaté une recrudescence de Qakbot en septembre 2022, qui utilisait la contrebande HTML pour compromettre les victimes. Ces infections sont liées à une vaste activité post-compromission, notamment la reconnaissance, la collecte d'informations et le déploiement de charges utiles supplémentaires. Les infections par Qakbot non contrôlées tout au long de 2022 ont conduit à de multiples infections par Black Basta. X-Force a constaté que les attaques par ransomware revendiquées sur le site de fuite de données du groupe Black Basta avaient nettement diminué pendant l'interruption de l'activité d'hameçonnage de Qakbot au cours de l'été 2022. X-Force s'attend à ce que la reprise de l'activité de Qakbot coïncide avec un nombre plus élevé de victimes de ransomwares.



Contournement des macros

Face aux changements apportés par Microsoft concernant les macros à partir d'octobre 2021, l'utilisation de fichiers ISO et LNK est apparue comme une tactique importante pour infecter les organisations. Cette tactique comprend à la fois la livraison directe de leurs charges utiles par le biais de ces fichiers conteneurs, ainsi que le brouillage des fichiers prenant en charge les macros au sein de ceux-ci.

- Les fichiers ISO et les fichiers compressés sont utilisés pour contourner l'attribut MOTW (mark of the web) utilisé par Microsoft et aider les cibles à activer les macros malveillantes. Alors que les fichiers ISO ou compressés semblent avoir été téléchargés depuis Internet, la pièce jointe prenant en charge les macros ne l'est pas, ce qui permet aux acteurs de la menace de poursuivre cette attaque.
- Un autre moyen de contourner les restrictions relatives aux macros consiste à inclure des charges utiles directement dans les fichiers LNK qui, lorsque l'on clique dessus, lancent des commandes arbitraires utilisées principalement pour télécharger ou charger les étapes suivantes. Avant le début de l'année 2022, une seule campagne, en février 2021, avait utilisé cette tactique. X-Force a constaté sa récurrence fin février-mars 2022 et la voit désormais régulièrement.

Parmi les autres tendances détectées par X-Force dans les campagnes de spam des acteurs de la menace, figurent l'utilisation accrue d'archives compressées chiffrées comme pièces jointes et le détournement de conversations, comme expliqué ici.

- Les extensions compressées chiffrées, que les logiciels antivirus ont plus de mal à détecter et à signaler comme malveillantes, ont été découvertes plus fréquemment en 2022. Le nombre moyen de courriers indésirables comportant de telles pièces jointes livrés par semaine a été multiplié par neuf en 2022, par rapport aux données recueillies entre avril et décembre 2021.
- Le détournement de conversations, dans lequel les acteurs de la menace s'insèrent dans des fils de discussion existants, est une tactique de longue date utilisée pour accroître la légitimité des courriers indésirables et inciter plus efficacement les victimes à s'engager. Cette tactique a connu une hausse marquée en 2022 - par rapport à la majorité de l'année 2021 - et s'est atténuée au printemps. Selon X-Force, cette tendance est due en grande partie aux courriers indésirables Emotet.

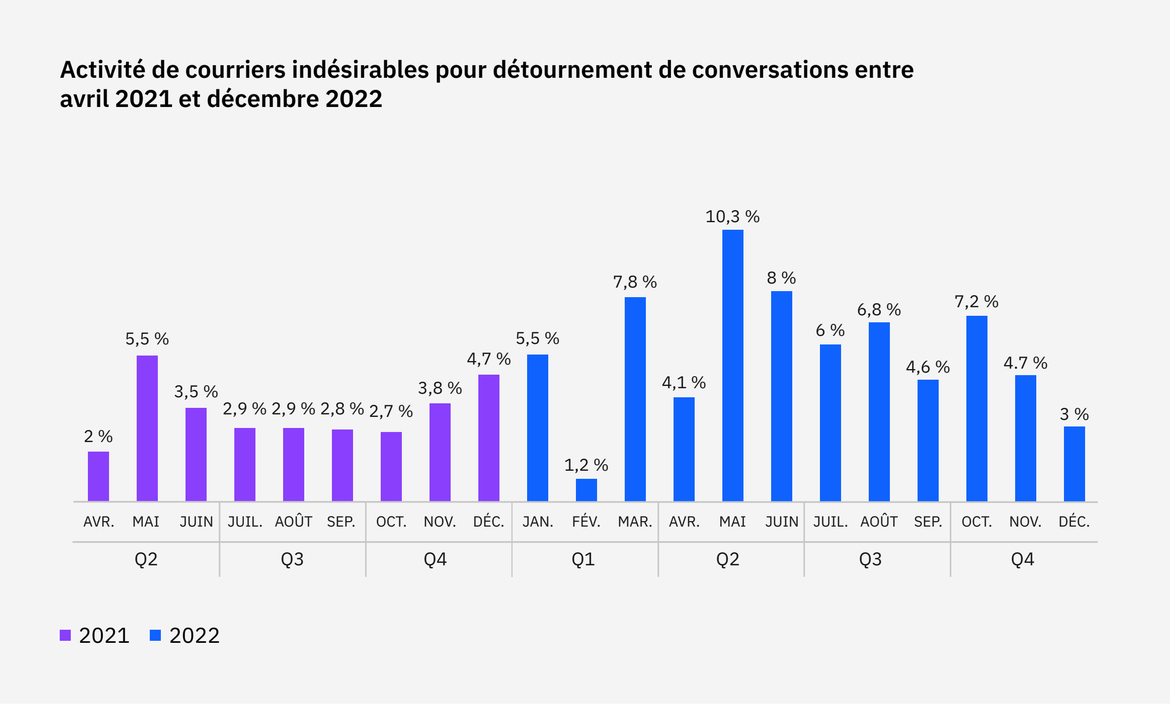


Figure 13 : les pourcentages correspondent au nombre total de tentatives de détournement de conversations détectées dans les données X-Force depuis avril 2021. Source : X-Force

– Après son démantèlement en janvier 2021, le botnet Emotet a fait son retour en novembre de la même année. Il a poursuivi son activité en 2022, a fait une pause de près de quatre mois à partir de la mi-juillet et est revenu pendant près de deux semaines en novembre 2022.

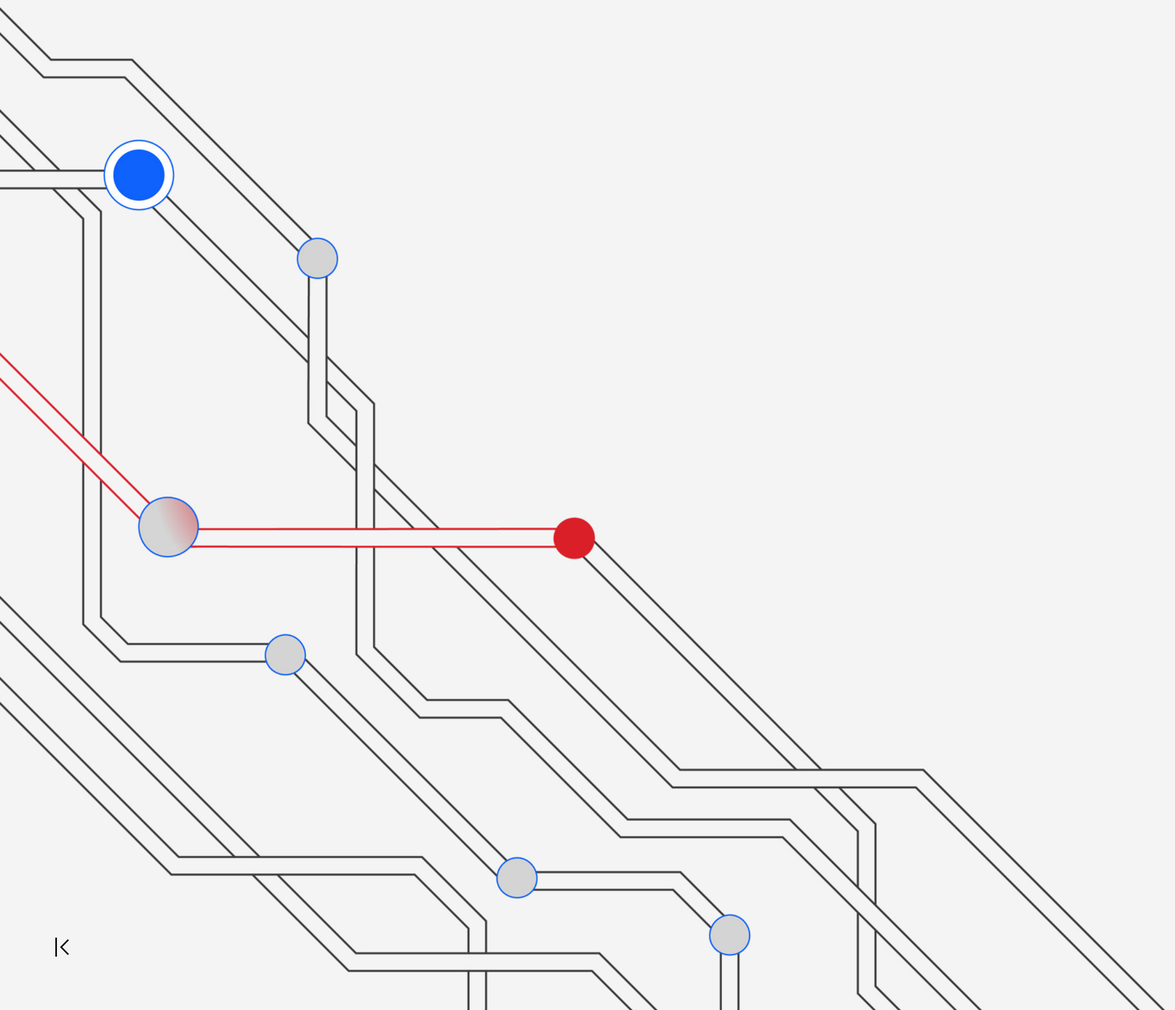
– Les données montrent qu'il y a eu environ deux fois plus de tentatives régulières par mois en 2022 par rapport aux données disponibles depuis avril 2021. Le détournement de conversations a connu une évolution instable jusqu'en mai 2022 et son déclin au cours de la seconde moitié de l'année correspond plus ou moins à l'inactivité d'Emotet.

– Les courriers indésirables menant à Emotet, Qakbot et IcedID ont fortement exploité le détournement de conversations. Le retour d'Emotet en novembre 2021 a contribué à une augmentation irrégulière jusqu'en mai 2022. La baisse générale observée dans la seconde moitié de l'année correspond à la pause d'Emotet de juillet à octobre et à son bref retour en novembre 2022.

– Il est difficile d'effectuer le suivi du détournement de conversations et de le distinguer clairement des cas où des acteurs ajoutent simplement un en-tête de réponse à un courrier indésirable, et cela risque de s'aggraver. Par exemple, certains acteurs de la menace ont commencé à supprimer les en-têtes de ligne d'objet « Re : », probablement parce qu'ils sont conscients que ces en-têtes peuvent être utilisés pour suivre leur activité.

09

Menaces sur la TO et les systèmes de contrôle industriel



Menaces sur la technologie opérationnelle

L'année 2022 a été marquée par la découverte de deux nouveaux logiciels malveillants spécifiques à la TO, à savoir Industroyer2 et INCONTROLLER, également connu sous le nom de PIPEDREAM, et la divulgation de nombreuses vulnérabilités de la TO appelées OT : ICEFALL. Le contexte des cybermenaces liées à la TO s'élargit considérablement et les propriétaires et exploitants de ces actifs doivent être parfaitement conscients de l'évolution du paysage.

X-Force a examiné de plus près les données sur les attaques réseaux et la RI relatives à la TO afin de mieux comprendre comment les acteurs de la menace cherchent à compromettre les clients des secteurs qui exploitent la TO. Les données relatives aux attaques réseaux montrent que les attaques par force brute, l'utilisation de normes de chiffrement insuffisantes et dépassées et les mots de passe faibles ou par défaut sont des signes d'alerte courants dans les environnements informatiques et de TO de ces secteurs.

Parmi les données relatives aux attaques réseaux propres au système de contrôle industriel (SCI), les alertes indiquant des tentatives probables d'attaques par force brute étaient les plus courantes, suivies de près par les alertes de chiffrement faible. Les alertes de chiffrement faible les plus courantes concernaient l'utilisation continue de la norme TLS (Transport Layer Security) 1.0, une méthode de chiffrement dépassée et peu sûre, rendue obsolète en mars 2021. Bien que le gouvernement américain recommande une reconfiguration pour utiliser TLS 1.2 ou 1.3, les directives du National Institute of Standards and Technology (NIST) abordent de manière plus approfondie la réalité du terrain. Dans cette réalité, les systèmes plus anciens peuvent être contraints d'utiliser des versions plus faibles de chiffrement pour continuer de fonctionner. Les alertes relatives aux mots de passe faibles ou par défaut sont également significatives, d'autant plus qu'il s'agit.

de vulnérabilités de base qui facilitent la tâche des auteurs d'attaques par force brute. Le balayage généralisé et probablement systématique des vulnérabilités internes et externes constituait la tentative d'attaque la plus courante contre les secteurs qui exploitent la TO. Les données ont révélé que les anciennes vulnérabilités et menaces sont toujours d'actualité. Un groupe de vulnérabilités découvertes en 2021 par Cisco Talos dans le logiciel de surveillance Advantech R-SeeNet a déclenché une petite majorité des alertes de balayage de vulnérabilités dans les secteurs qui exploitent la TO en 2022. Ces vulnérabilités pourraient permettre aux attaquants d'exécuter du code ou des commandes arbitraires.

La seconde vulnérabilité la plus courante, cependant, remonte à 2016. Il s'agit d'une vulnérabilité de type « contournement de filtre » dans l'application Trihedral VTScada, CVE-2016-4510, qui pourrait permettre à des utilisateurs non authentifiés d'envoyer des requêtes HTTP pour accéder à des fichiers. Les types d'attaques, tels que WannaCry et Conficker, qui continuent de représenter des menaces importantes pour la TO, soulignent par ailleurs les risques liés aux anciennes menaces.

La fabrication continue d'être le secteur exploitant la TO le plus ciblé

Si l'on examine le sous-ensemble d'incidents dans les secteurs qui exploitent la TO, on constate que le secteur manufacturier était le secteur le plus attaqué en 2022, selon les données. Il a été la cible de 58 % des incidents que X-Force a corrigés. Le déploiement de portes dérobées était la principale action sur l'objectif, représentant 28 % des incidents dans ce secteur. Les acteurs de ransomwares, en particulier, trouvent dans ce secteur une cible attrayante, probablement en raison de la faible tolérance de ces organisations aux temps d'arrêt.

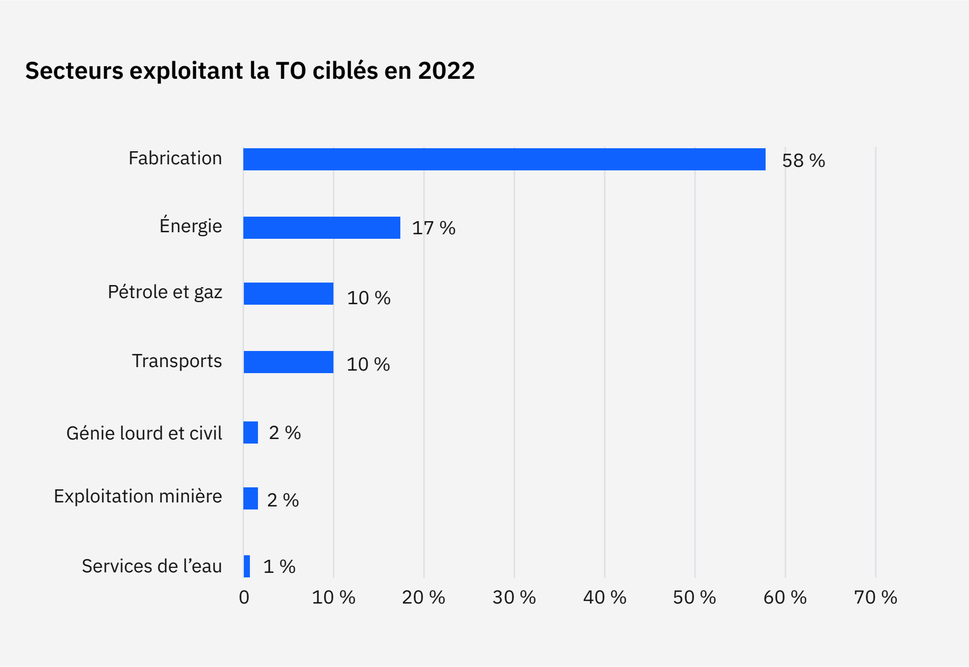


Figure 14 : pourcentage de cas de RI par secteur exploitant la TO, auxquels X-Force a répondu en 2022.
Source : X-Force

Si l'on examine les vecteurs d'accès initial lors des incidents survenus dans les secteurs exploitant la TO, le harponnage représente 38 % des incidents, notamment l'utilisation de pièces jointes (22 %), l'utilisation de liens (14 %) et le harponnage en tant que service (2 %). L'exploitation d'applications destinées au public arrive en deuxième position (24 %), suivant la tendance générale du secteur. Avec 20 % des incidents, la détection de portes dérobées est également en tête dans ces secteurs. Viennent ensuite les ransomwares (19 %). L'extorsion occupe également une place de choix, avec 29 % des incidents, suivie de près par le vol de données, avec 24 %.

L'absence de segmentation adéquate entre les réseaux de TO et les réseaux informatiques constitue une autre vulnérabilité majeure exploitée dans le domaine de la TO. L'équipe X-Force Red en charge des services de simulation d'adversaires cible régulièrement les faiblesses de la segmentation pour accéder à des environnements TO isolés. Cela inclut notamment les serveurs de saut, les postes de travail d'opérateur à double résidence et les serveurs de reporting, tels que les historiens de données qui exposent les services web et SQL de la TO aux réseaux informatiques de l'entreprise. Une segmentation adéquate de ces parties de vos réseaux et une surveillance étroite des communications entre elles peuvent assurer la sécurité des actifs.

Tendances géographiques

Pour la deuxième année consécutive, la région Asie-Pacifique occupe la première place en tant que région la plus attaquée en 2022, avec 31 % des incidents auxquels le service X-Force IR a répondu. L'Europe suit de près avec 28 % des attaques, puis l'Amérique du Nord avec 25 %. L'Asie-Pacifique et l'Europe affichaient des pourcentages d'incidents plus élevés, avec respectivement une hausse de cinq et de quatre points de pourcentage par rapport aux chiffres de 2021. En revanche, au Moyen-Orient, le pourcentage a chuté de 14 à 4 %.

Incidents par région entre 2020 et 2022

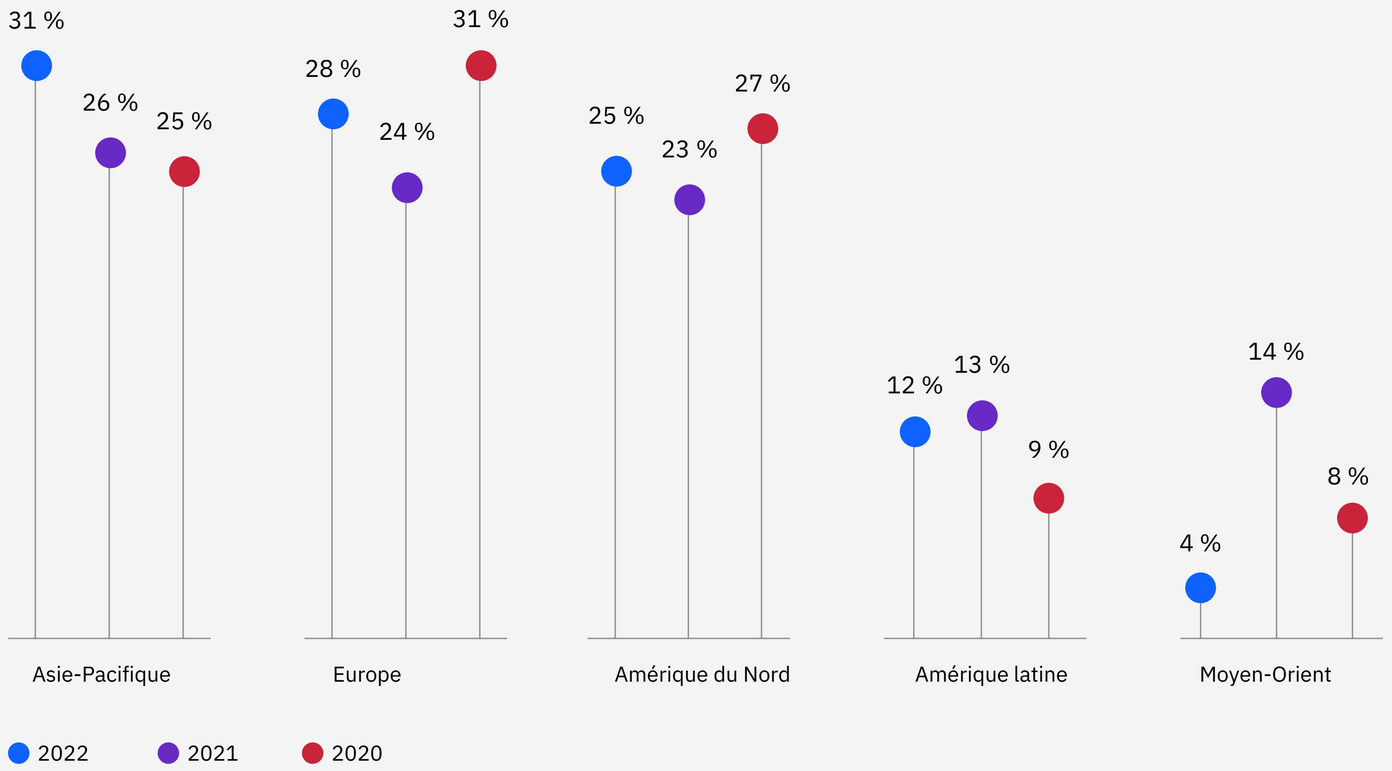


Figure 15 : proportion de cas de RI par région auxquels X-Force a répondu entre 2020 et 2022. Source : X-Force

N° 1 | Asie-Pacifique

La région Asie-Pacifique, en particulier le Japon, a été l'épicentre du pic d'Emotet en 2022. Bien qu'elle ne soit pas directement liée à la guerre en Europe, la recrudescence des cas d'Emotet au Japon a coïncidé avec l'invasion de l'Ukraine par la Russie, qui, selon d'autres chercheurs de la communauté de la cybersécurité, a contribué à une importante activité d'Emotet à l'époque. Des campagnes de spam ont été identifiées dans plusieurs secteurs, la plupart des cas se produisant dans les secteurs de la fabrication, des finances et des assurances. Emotet est diffusé principalement par le biais de campagnes de spam qui utilisent des titres accrocheurs.

Le secteur de la fabrication arrive en tête de liste des secteurs attaqués dans cette région, avec 48 % des incidents, suivi de loin par le secteur des finances et des assurances avec 18 %.

Le harponnage par pièce jointe est le principal vecteur d'infection (40 %) dans cette région, suivi par l'exploitation des applications destinées au public (22 %). Les cas de services distants externes et les liens de harponnage sont à égalité en troisième place, à 12 %.

Le déploiement de portes dérobées était l'action la plus courante sur l'objectif, avec 31 % des incidents dans la région. Les ransomwares arrivaient en deuxième position (13 %) et, les documents malveillants (maldocs), en troisième position (10 %). L'extorsion constituait l'impact le plus courant, observé dans 28 % des cas. L'impact sur la réputation de la marque arrivait en deuxième position avec 22 % et le vol de données, en troisième position avec 19 %.

Le Japon représentait 91 % des incidents en Asie-Pacifique, les Philippines représentant 5 %, et l'Australie, l'Inde et le Vietnam représentant 1,5 % chacun.

Dans la région Asie-Pacifique, le secteur de la fabrication était le secteur le plus attaqué, avec 48 % des incidents.

N° 2 | Europe

À partir de mars 2022, juste après l'invasion de l'Ukraine par la Russie, le déploiement de portes dérobées a connu une forte croissance en Europe. Il représentait 21 % des cas dans la région, contre 11 % pour les ransomwares. Les outils d'accès distant ont été identifiés dans 10 % des incidents auxquels X-Force a répondu. En ce qui concerne l'impact sur les clients, 38 % des cas observés par X-Force en Europe étaient liés à l'extorsion, 17 % au vol de données et 14 % au recueil de données d'identification. L'Europe était la région la plus touchée par l'extorsion, représentant 44 % de tous les cas d'extorsion observés.

L'exploitation d'applications destinées au public était le principal vecteur d'infection utilisé contre les entreprises européennes, représentant 32 % de tous les incidents corrigés par X-Force dans la région, dont plusieurs ont conduit à des infections par ransomware. L'utilisation de comptes locaux valides arrivait en deuxième position avec 18 %, suivie des liens de harponnage à 14 %, en forte baisse par rapport aux 42 % de 2021. Cette diminution des liens de harponnage peut être due à une meilleure sensibilisation des utilisateurs, à de meilleurs moyens de protection de la messagerie ou à des mesures plus efficaces de détection des logiciels malveillants après leur installation.

Les services professionnels, aux entreprises et aux consommateurs sont à égalité avec le secteur des finances et des assurances en tant que secteurs les plus attaqués, chacun représentant 25 % des incidents auxquels X-Force a répondu. Le secteur de la fabrication arrivait en deuxième position avec 12 % des incidents, tandis que les secteurs de l'énergie et de la santé se partageaient la troisième place avec 10 %.

Le Royaume-Uni a été le pays le plus attaqué en Europe, avec 43 % des incidents. L'Allemagne représentait 14 % des incidents, le Portugal 9 %, l'Italie 8 % et la France 7 %. X-Force a également répondu à un plus petit nombre d'incidents en Norvège, au Danemark, en Suisse, en Autriche, en Grèce, au Groenland, en Espagne et en Serbie.

Le Royaume-Uni a été le pays le plus attaqué en Europe, avec 43 % des incidents.

N° 3 | Amérique du Nord

X-Force a observé une légère augmentation du nombre d'incidents en Amérique du Nord, avec 23 % de tous les incidents en 2021 contre 25 % en 2022.

Les entreprises du secteur de l'énergie se sont hissées en tête de la liste des victimes en Amérique du Nord, représentant 20 % de toutes les attaques auxquelles X-Force a répondu en 2022. Le secteur de la fabrication et le secteur du commerce de détail et de gros se partagent la deuxième place avec 14 % des incidents chacun. Alors que le commerce de détail et de gros occupaient une place similaire en 2021, les chiffres pour la fabrication représentaient une baisse de 50 % par rapport à 2021. Les services professionnels, aux entreprises et aux consommateurs arrivaient en troisième position en 2022 avec 12 %, dans un contexte de hausse des ransomwares et autres incidents liés aux logiciels malveillants.

Les principaux vecteurs d'infection identifiés étaient l'exploitation d'applications destinées au public (35 %) et les pièces jointes de harponnage (20 %). Les incidents liés aux ransomwares représentaient 23 % des cas, dont quelques-uns résultaient de la détection d'infections persistantes de WannaCry ou Ryuk remontant à 2018 ou 2019, ce qui souligne l'importance d'un nettoyage approprié après de tels événements. Dans la région, les botnets représentaient 12 % des cas, les portes dérobées et les attaques BEC se partageant la troisième position avec 10 % chacune.

Si l'on examine l'impact le plus important des acteurs de la menace, le recueil de données d'identification a pris la pole position avec 25 % des incidents auxquels X-Force a répondu en Amérique du Nord. Les fuites et les vols de données arrivaient ex aequo en deuxième position avec 17 % chacun, tandis que l'extorsion représentait 13 % des cas.

Les États-Unis représentaient 80 % des attaques dans la région, contre 20 % pour le Canada.

Les entreprises les plus fréquemment attaquées en Amérique du Nord étaient des entreprises du secteur de l'énergie, avec 20 % des cas.

N° 4| Amérique latine

Pour les besoins du rapport, IBM considère que l'Amérique latine comprend le Mexique, l'Amérique centrale et l'Amérique du Sud.

Les incidents en Amérique latine se sont écartés des tendances mondiales. Occupant la deuxième place en 2021, le commerce de détail et de gros était en 2022 le secteur le plus attaqué, avec 28 % des incidents corrigés par X-Force. Le secteur des finances et des assurances était le deuxième secteur le plus ciblé avec 24 % des cas, suivi du secteur de l'énergie avec 20 % des cas.

Les ransomwares devançaient les autres types d'attaque en Amérique latine, représentant 32 % des incidents auxquels X-Force a répondu. Le déploiement de portes dérobées constituait la deuxième action sur l'objectif la plus fréquente, avec 16 % des cas, tandis que les attaques BEC et le détournement de conversations arrivaient ex aequo en troisième position, avec 11 % chacun. L'extorsion et le vol de données étaient les impacts les plus fréquemment observés dans la région (27 % des cas), les pertes financières comptant pour 20 % des cas. La destruction et les fuites de données occupaient la troisième place, avec 13 % des cas chacune.

Les principaux vecteurs d'accès initial étaient les services distants externes (30 %) et l'exploitation d'applications destinées au public (20 %). La compromission de type « drive-by », les ajouts de matériel, les comptes de domaine valides, les comptes locaux valides et les pièces jointes de harponnage représentaient chacun 10 % des cas.

Le Brésil représentait 67 % de tous les cas auxquels X-Force a répondu en Amérique latine, la Colombie 17 % et le Mexique 8 %. Le Pérou et le Chili se partageaient les 8 % restants.

En Amérique latine, le Brésil représentait 67 % des cas auxquels X-Force a répondu.

N° 5 | Moyen-Orient et Afrique

Pour les besoins du rapport, IBM considère que le Moyen-Orient et l'Afrique comprennent le Levant, la Péninsule arabique, l'Égypte, l'Iran et l'Irak, ainsi que l'ensemble du continent africain.

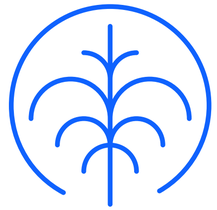
Le déploiement de portes dérobées a été détecté dans 27 % des cas auxquels X-Force a répondu dans cette région en 2022. Les ransomwares et les vers représentaient le deuxième type d'attaque le plus courant, avec 18 % des cas chacun. L'extorsion et les pertes financières représentaient chacune la moitié des impacts identifiés dans les incidents survenus dans cette région en 2021.

Les liens de harponnage ont été utilisés pour l'accès initial dans deux tiers des incidents corrigés par X-Force au Moyen-Orient et en Afrique, le tiers restant correspondant aux supports amovibles.

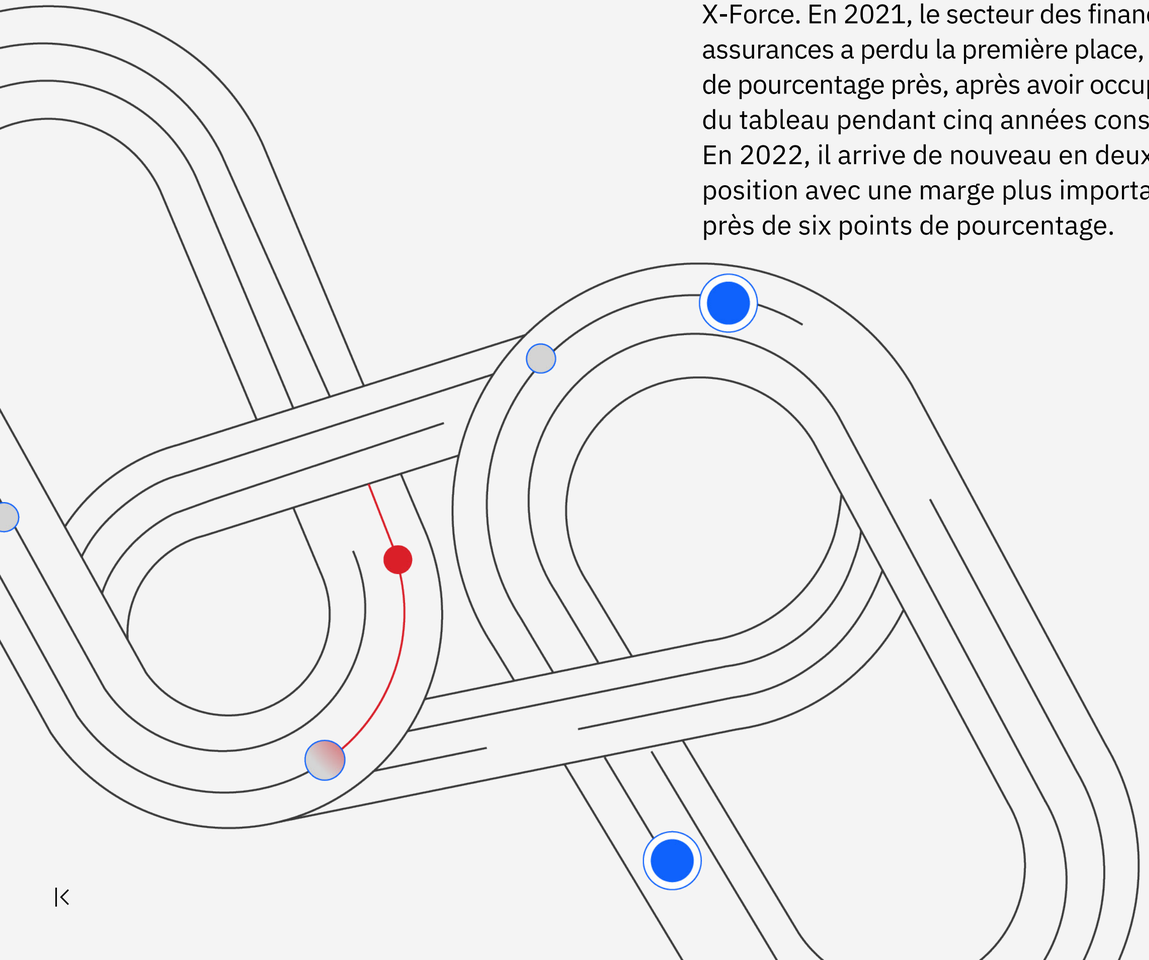
En 2022, le secteur des finances et des assurance était le secteur le plus ciblé au Moyen-Orient et en Afrique, avec 44 % des incidents, ce qui représente une légère baisse par rapport à 2021 (48 %). Les services professionnels, aux entreprises et aux consommateurs représentaient 22 % des attaques, tandis que les secteurs de la fabrication et de l'énergie se partageaient la troisième place avec 11 % chacun.

L'Arabie saoudite représentait les deux tiers des cas de la région auxquels X-Force a répondu. Les autres cas étaient répartis entre le Qatar, les Émirats arabes unis et l'Afrique du Sud.

L'attaque la plus courante dans cette région était le déploiement de portes dérobées avec 27 % des incidents.



Tendances sectorielles



Pour la deuxième année consécutive, le secteur de la fabrication était le secteur le plus attaqué, selon les données de réponse aux incidents de X-Force. En 2021, le secteur des finances et des assurances a perdu la première place, à un point de pourcentage près, après avoir occupé le haut du tableau pendant cinq années consécutives. En 2022, il arrive de nouveau en deuxième position avec une marge plus importante de près de six points de pourcentage.

Part des attaques par secteur 2018 – 2022

Secteur	2022	2021	2020	2019	2018
Fabrication	24,8 %	23,2	17,7	8	10
Finances et assurances	18,9 %	22,4	23	17	19
Services professionnels, aux entreprises et aux consommateurs	14,6 %	12,7	8,7	10	12
Énergie	10,7 %	8,2	11,1	6	6
Commerce de détail et de gros	8,7 %	7,3	10,2	16	11
Éducation	7,3 %	2,8	4	8	6
Santé	5,8 %	5,1	6,6	3	6
Secteur public	4,8 %	2,8	7,9	8	8
Transports	3,9 %	4	5,1	13	13
Médias et télécommunications	0,5 %	2,5	5,7	10	8

24,8 %

des interventions de RI de X-Force concernaient le secteur de la fabrication.

N° 1 | Fabrication

Le secteur de la fabrication était le secteur le plus attaqué, avec une marge légèrement supérieure à celle de 2021. En 2022, des portes dérobées ont été déployées dans 28 % des incidents, battant les ransomwares, qui sont apparus dans 23 % des incidents corrigés par X-Force. Le pic d'infections par Emotet a boosté le pourcentage de déploiements de portes dérobées. Certains de ces cas auraient pu conduire à des attaques par ransomware, entre autres activités plus malveillantes, mais ils ont été identifiés suffisamment tôt pour être corrigés.

Les pièces jointes de harponnage et l'exploitation d'applications destinées au public sont les deux principaux vecteurs d'infection, avec 28 % chacune. Les services distants externes arrivent en deuxième position (14 %), tandis que les liens de harponnage et les comptes par défaut valides étaient à égalité en troisième position (10 %).

L'extorsion était le principal impact sur les entreprises de fabrication, dans 32 % des cas. Les fabricants ne tolèrent guère les temps d'arrêt, et cette intolérance fait de l'extorsion une stratégie lucrative pour les attaquants. Le vol de données arrive en deuxième position, avec 19 % des incidents, suivi par les fuites de données (16 %). La région Asie-Pacifique a connu le plus grand nombre d'incidents dans le secteur de la fabrication, avec environ 61 % des cas. L'Europe et l'Amérique du Nord sont ex aequo en deuxième position avec 14 %, suivies de l'Amérique latine avec 8 % et du Moyen-Orient et de l'Afrique avec 4 %.

18,9 %

des interventions de RI de X-Force concernaient le secteur des finances et des assurances.

N° 2 | Finances et assurances

Le secteur des finances et des assurances représentait moins d'une attaque sur cinq à laquelle X-Force a répondu en 2022, ce qui lui a valu la deuxième place. Ce pourcentage indique une légère baisse au cours des dernières années, car d'autres secteurs ont commencé à attirer l'attention des attaquants, en particulier le secteur de la fabrication.

Les entreprises du secteur des finances et des assurances ont tendance à devancer les entreprises des autres secteurs en termes de transformation digitale et d'adoption du cloud. Les attaquants doivent donc redoubler d'efforts pour réussir leurs attaques contre ces entreprises.

Les attaques par porte dérobée représentaient l'action sur l'objectif la plus couramment observée (29 %), suivies par les ransomwares et les maldocs (11 % chacun). Les pièces jointes de harponnage constituaient le principal vecteur d'infection et étaient utilisées dans 53 % des attaques contre ce secteur. L'exploitation d'applications destinées au public arrivait en deuxième position avec 18 % des attaques, et les liens de harponnage constituaient le vecteur d'accès initial dans 12 % des incidents.

L'Europe a connu le plus grand nombre d'attaques contre les entreprises du secteur des finances et des assurances, avec environ 33 % de l'ensemble des attaques, l'Asie-Pacifique arrivant juste derrière avec environ 31 %. L'Amérique latine représentait environ 15 % des incidents auxquels X-Force a répondu, l'Amérique du Nord et le Moyen-Orient et l'Afrique représentant environ 10 % chacun.

14,6 %

des interventions de RI de X-Force concernaient le secteur des services professionnels, aux entreprises et aux consommateurs.

N° 3 | Services professionnels, aux entreprises et aux consommateurs

Le secteur des services professionnels comprend les cabinets-conseil, les sociétés de gestion et les cabinets d'avocats. Ces services représentaient 52 % des victimes de ce segment. Les services aux entreprises comprennent les entreprises informatiques et technologiques et les agences de relations publiques, de publicité et de communication. Celles-ci représentaient 37 % des victimes. Les services aux consommateurs, qui englobent les constructeurs de maisons, l'immobilier, les arts, les divertissements et les loisirs, représentaient 11 % des incidents. Ensemble, ils forment la catégorie des services professionnels, aux entreprises et aux consommateurs du rapport X-Force Threat Intelligence Index 2023.

Les services professionnels, aux entreprises et aux consommateurs ont été le plus souvent victimes d'attaques par ransomware et par porte dérobée, avec 18 % des cas chacun. Les deux principaux vecteurs d'infection étaient l'exploitation d'applications destinées au public et les services distants externes (23 % chacun). Les pièces jointes de harponnage et les comptes locaux valides étaient chacun à l'origine de 15 % des incidents.

L'extorsion était l'impact le plus courant dans 28 % des incidents, avec le vol de données, le recueil de données d'identification et les fuites de données représentant chacun 17 % des incidents. L'Europe représentait 47 % des incidents auxquels X-Force à répondu, suivie de l'Amérique du Nord avec 33 %, l'Asie-Pacifique avec 10 %, le Moyen-Orient et l'Afrique avec 7 % et l'Amérique latine avec 3 %.

10,7 %

des interventions de RI de X-Force concernaient le secteur de l'énergie.

N° 4 | Énergie

Les entreprises du secteur de l'énergie, y compris les compagnies d'électricité et les compagnies pétrolières et gazières, représentaient le quatrième secteur le plus attaqué - comme en 2021 - avec 10,7 % des attaques. L'exploitation des applications destinées au public était le vecteur d'infection le plus courant (40 %). Les liens de harponnage et les services distants externes représentaient chacun 20 % des cas. Les botnets constituaient l'action sur l'objectif la plus fréquente avec 19 % des cas, les ransomwares et les attaques BEC se partageant la deuxième place avec 15 % des cas.

Le vol de données et l'extorsion ont été constatés dans 23 % des cas, suivis par le recueil de données d'identification et les infections par botnet (15 % chacun). Parmi tous les incidents auxquels X-Force a répondu dans le monde, les entreprises d'Amérique du Nord étaient les principales victimes, avec 46 %, contre 23 % pour l'Europe et l'Amérique latine, et un peu moins de 5 % pour l'Asie-Pacifique, le Moyen-Orient et l'Afrique.

Le secteur de l'énergie reste sous la pression de diverses forces mondiales, en particulier celles exacerbées par la guerre en Ukraine et la façon dont elle a affecté un commerce mondial de l'énergie déjà instable.

8,7 %

des interventions de RI de X-Force concernaient le secteur du commerce de détail et de gros.

N° 5 | Commerce de détail et de gros

Les détaillants sont responsables de la vente de biens aux consommateurs et aux grossistes. Les grossistes sont généralement responsables du transport et de la distribution de ces biens directement des fabricants aux détaillants ou directement aux consommateurs. Le secteur du commerce de détail et de gros était le cinquième secteur le plus ciblé, selon les données de X-Force IR, occupant ainsi la même place qu'en 2021.

Le vecteur d'accès initial le plus courant dans les attaques contre le commerce de détail et de gros était les e-mails de harponnage contenant un lien malveillant (33 %). Les services distants externes compromis, le harponnage par pièce jointe malveillante et les ajouts de matériel représentaient chacun 17 % des incidents.

Les ransomwares, les portes dérobées et les attaques BEC constituaient les actions les plus courantes des attaquants, chacune représentant 19 % des activités. Des vers ont été identifiés dans 10 % des cas. Les organisations ont été victimes d'extorsion dans 50 % des cas, et de recueil de données d'identification et de pertes financières dans 25 % des cas. L'Amérique du Nord et l'Amérique latine ont connu le plus grand nombre de cas (39 % chacune), contre 22 % pour l'Europe.

7,3 %

des interventions de RI de X-Force concernaient le secteur de l’éducation.

N° 6 | Éducation

Les incidents dans le secteur de l’éducation ont impliqué des portes dérobées dans 20 % des attaques auxquelles X-Force a répondu. Les ransomwares, les logiciels publicitaires et les courriers indésirables représentaient chacun 13 % des cas. L’exploitation d’applications destinées au public était le vecteur d’accès initial le plus souvent observé (42 % des cas), suivi par les pièces jointes de harponnage (25 %). L’hameçonnage via un service, l’hameçonnage via un lien et l’hameçonnage via un compte local ou cloud valide représentaient chacun 8 % des vecteurs d’accès initial. Avec 25 % chacun, les impacts étaient le vol de données, la fuite de données, l’extorsion et la reconnaissance. L’Asie-Pacifique représentait 67 % des cas, l’Amérique du Nord 27 % et l’Amérique latine 6 %.

5,8 %

des interventions de RI de X-Force concernaient le secteur de la santé.

N° 7 | Santé

Figurant parmi les 10 premiers secteurs d'activité les plus touchés, les soins de santé ont affiché un recul et sont passés de la sixième place en 2021 à la septième place en 2022. Au cours des trois dernières années, le secteur de la santé a représenté environ 5 à 6 % des incidents auxquels X-Force a répondu. Les attaques par porte dérobée représentaient 27 % des cas, contre 18 % pour les web shells. Les logiciels publicitaires, les attaques BEC, les cryptomineurs, les chargeurs, les outils de reconnaissance et de balayage et les outils d'accès distant représentaient chacun 9 % des cas. La reconnaissance était le principal impact observé (50 %), tandis que le vol de données et le cryptominage ont été identifiés dans 25 % des cas chacun.

Les cibles basées en Europe représentaient 58 % des incidents, les 42 % restants correspondant à des cibles en Amérique du Nord.

4,8 %

des interventions de RI de X-Force concernaient le secteur public.

N° 8 | Secteur public

Le secteur public est également une cible privilégiée des attaques par porte dérobée, avec 25 % des cas recensés par X-Force IR. Les attaques DDoS représentaient également un quart des cas. Les nombreuses informations sensibles contenues dans les réseaux du secteur public sont une cible fréquente des campagnes de cyber-espionnage. Ces informations peuvent comprendre de vastes bases de données d'informations identifiant la personne et autres informations susceptibles d'être utilisées par des groupes parrainés par des États ou vendues à des fins lucratives par des cybercriminels. Les maldocs ont été identifiés dans 17 % des cas, tandis que les cryptomineurs, les outils de recueil de données d'identification, les ransomwares et les web shells représentaient les 83 % restants.

Dans ce secteur, X-Force a pu relier les incidents à des cybercriminels, à des menaces internes ayant entraîné la destruction de données, à des hacktivistes et à des groupes d'attaquants parrainés par des États et menant des activités d'espionnage, chaque catégorie occupant une part égale.

L'exploitation d'applications destinées au public et les pièces jointes de hameçonnage étaient les principaux vecteurs d'infection (40 % chacun), tandis que l'utilisation de comptes par défaut valides représentait 20 % des incidents. Les organismes publics de la région Asie-Pacifique ont été les plus visés (50 % des cas), devançant l'Europe (30 %) et l'Amérique du Nord (20 %).

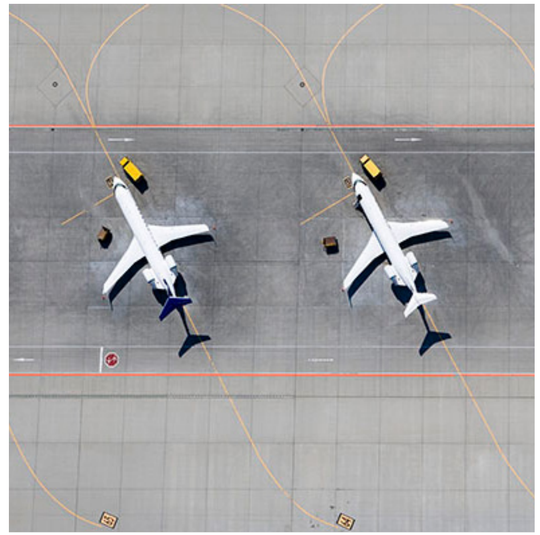
3,9 %

des interventions de RI de X-Force concernaient le secteur des transports.

N° 9 | Transports

Après avoir occupé la septième place en 2021, le secteur des transports a été relégué à la neuvième place qu'il occupait en 2020. Toutefois, ce secteur représentait toujours à peu près le même pourcentage d'incidents auxquels X-Force a répondu. L'hameçonnage était le vecteur d'accès initial le plus courant dans 51 % des cas, avec une répartition égale entre les liens, les pièces jointes et le harponnage en tant que service. L'utilisation de comptes locaux valides représentait 33 % des vecteurs d'accès initial, les comptes cloud valides servant de point d'entrée dans 17 % des cas. L'accès au serveur et le déploiement d'outils d'accès distant constituaient les principales actions sur l'objectif (25 % chacun), suivis par les campagnes de spam, les ransomwares, les portes dérobées et les dégradations (13 % chacun).

Le vol de données était l'impact le plus fréquent (50 % des cas), l'extorsion et l'atteinte à la réputation de la marque représentant chacune 25 % des cas. Les sociétés de transport européennes étaient les plus visées (62 % des cas), un peu plus de 37 % revenant à l'Asie-Pacifique en deuxième position.



0,5 %

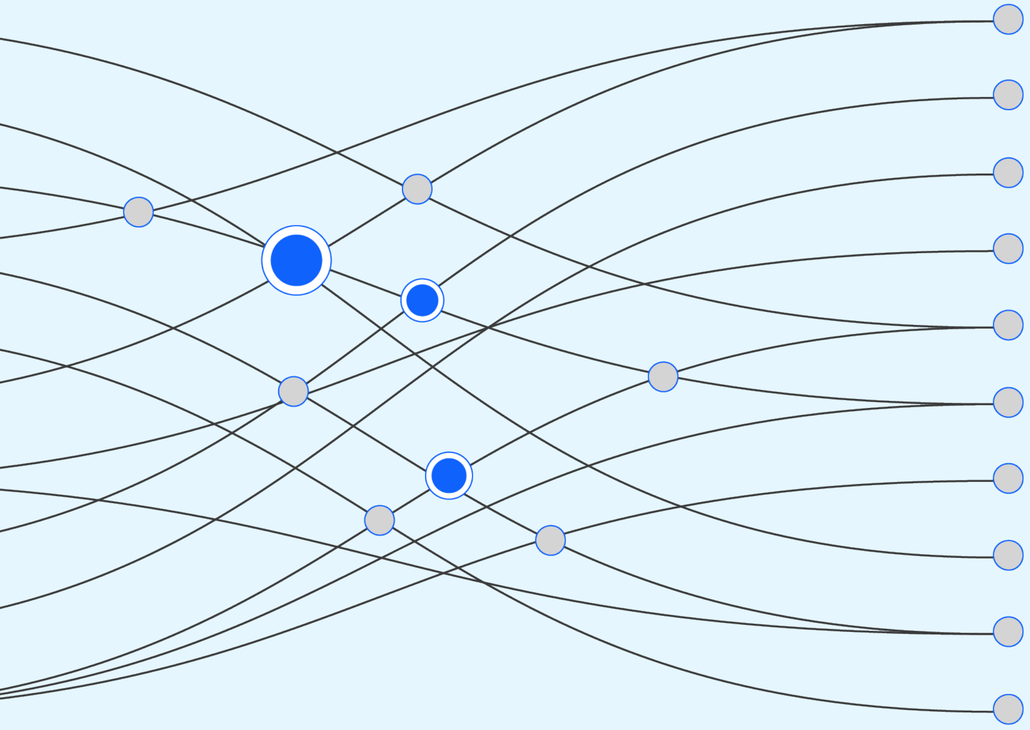
des interventions de RI de X-Force concernaient le secteur des médias et des télécommunications.

N° 10 | Médias et télécommunications

Les médias et les télécommunications représentaient une petite fraction des incidents auxquels X-Force a répondu, arrivant en dernière position pour la deuxième année consécutive. Les vecteurs d'infection observés comprenaient l'utilisation abusive de services distants externes, tels que les VPN et autres mécanismes d'accès, et les comptes de domaine valides. Ces vecteurs ont conduit à des attaques par ransomware. Les actions observées dans ces cas comprenaient le déploiement de ransomwares et d'outils d'exfiltration de données. Ces actions, à leur tour, ont conduit au vol, à la fuite, à la destruction et à l'extorsion de données.

12

Recommandations



Voici les mesures que nous vous recommandons de prendre pour sécuriser votre organisation contre les menaces malveillantes, notamment celles évoquées dans ce rapport.

Gérez vos actifs : « Que possédons-nous ? Que protégeons-nous ? Quelles données sont essentielles à notre entreprise ? ». Ce sont les premières questions auxquelles toute équipe de sécurité doit répondre pour mettre en place une défense efficace. De même, il convient de prioriser la découverte des actifs dans votre périmètre, de comprendre votre exposition aux attaques d'hameçonnage et de réduire ces surfaces d'attaque pour favoriser une sécurité globale. Enfin, les organisations doivent étendre leurs programmes de gestion des actifs pour inclure le code source, les données d'identification et d'autres données qui pourraient déjà exister sur Internet ou sur le dark web.

Apprenez à connaître votre adversaire : alors que de nombreuses organisations ont une vision globale du contexte des menaces, X-Force leur recommande d'adopter une vision qui met l'accent sur les acteurs spécifiques de la menace qui sont les plus susceptibles de cibler leur secteur, leur organisation et leur région. Il s'agit notamment de comprendre comment les acteurs de la menace opèrent, d'identifier leur niveau de sophistication et de savoir quelles tactiques, techniques et procédures les attaquants sont le plus susceptibles d'utiliser.

Gérez la visibilité : une fois qu'elles en savent plus sur les adversaires les plus susceptibles d'attaquer, les organisations doivent s'assurer qu'elles disposent d'une visibilité appropriée sur les sources de données à même d'indiquer la présence d'un attaquant. Pour stopper les attaquants avant qu'ils ne causent des perturbations, il est essentiel de maintenir la visibilité aux points clés de l'organisation et de veiller à ce que les alertes soient générées et traitées rapidement.

Remettez en question les hypothèses : les organisations doivent partir du principe qu'elles ont déjà été compromises. Ce faisant, les équipes peuvent continuellement réexaminer les points suivants :

- Comment les attaquants peuvent s'infiltrer dans leurs systèmes
- Quel est le niveau d'efficacité de leurs capacités de détection et de réponse face aux tactiques, techniques et procédures émergentes
- Les difficultés auxquelles pourraient se heurter un adversaire potentiel visant à compromettre vos données et systèmes les plus critiques

Les équipes de sécurité les plus performantes effectuent régulièrement des tests offensifs - chasse aux menaces, tests de pénétration et tests red team basés sur des objectifs - afin de détecter ou de valider les voies d'attaques opportunistes dans leurs environnements.

Agissez sur la base des informations à votre disposition : exploitez les renseignements sur les menaces à tous les niveaux. L'exploitation efficace des renseignements sur les menaces vous permettra d'analyser les voies d'attaques courantes et d'identifier les principales possibilités d'atténuer les attaques courantes, tout en vous permettant de développer des possibilités de détection ultra-fiables. L'exploitation des renseignements sur les menaces doit aller de pair avec la compréhension de vos adversaires et de leur mode de fonctionnement.

Soyez prêt : les attaques sont inévitables, pas l'échec ! Les organisations doivent élaborer des plans de réponse aux incidents adaptés à leur environnement. Ces plans doivent être régulièrement mis à l'épreuve et modifiés en fonction de l'évolution de l'organisation, afin d'améliorer les délais de réponse, de résolution et de reprise.

Le fait de pouvoir compter sur les services d'un prestataire de services de RI réputé permet de réduire le temps nécessaire pour rassembler des intervenants qualifiés en vue d'atténuer l'attaque. En outre, il est essentiel d'inclure votre prestataire de services de RI dans l'élaboration et le test de votre plan de réponse, car cela contribue à une réponse plus efficace. Les meilleurs plans de RI prévoient une réponse interorganisationnelle, intègrent des parties prenantes en dehors du service informatique et testent les lignes de communication entre les équipes techniques et la direction générale. Enfin, en testant votre plan dans le cadre d'un exercice cyber range immersif à haute pression, vous améliorerez grandement votre capacité à répondre à une attaque.

Renforcez la sécurité en prenant les mesures suivantes :

- [ ] Gérez vos actifs
- [ ] Apprenez à connaître votre adversaire
- [ ] Gérez la visibilité
- [ ] Remettez en question les hypothèses
- [ ] Agissez sur la base des informations à votre disposition
- [ ] Soyez prêt

À propos de nous

IBM Security X-Force

IBM Security X-Force est une équipe de spécialistes du piratage informatique, d'intervenants, de chercheurs et d'analystes spécialisés dans les menaces. Notre portefeuille X-Force comprend des produits et services offensifs et défensifs, alimentés par une vision à 360 degrés des menaces.

À l'ère des cyberattaques incessantes, du tout-connecté et des mandats réglementaires croissants, les organisations ont besoin d'une approche de sécurité ciblée. X-Force pense que la menace doit être le point central. Grâce à des tests de pénétration, à la gestion des vulnérabilités et à des services de simulation d'adversaires, l'équipe de hackers de X-Force Red endosse le rôle de cybercriminels pour trouver les failles de sécurité exposant vos actifs les plus importants. Grâce aux services de préparation, de détection et de réponse aux incidents, ainsi que de gestion de crise, l'équipe X-Force IR sait où les menaces peuvent se cacher et comment les arrêter. Les chercheurs de X-Force créent des techniques offensives pour détecter et prévenir les menaces, tandis que les analystes de X-Force collectent et traduisent les données sur les menaces en informations exploitables pour réduire les risques.

Grâce à une compréhension approfondie de la façon dont les cybercriminels pensent, élaborent des stratégies et frappent, X-Force peut vous aider à prévenir, détecter, répondre et récupérer des incidents et à vous concentrer sur les priorités de votre entreprise.

Si votre organisation a besoin d'aide pour renforcer sa posture de sécurité, planifiez une consultation individuelle avec un spécialiste d'IBM Security X-Force.

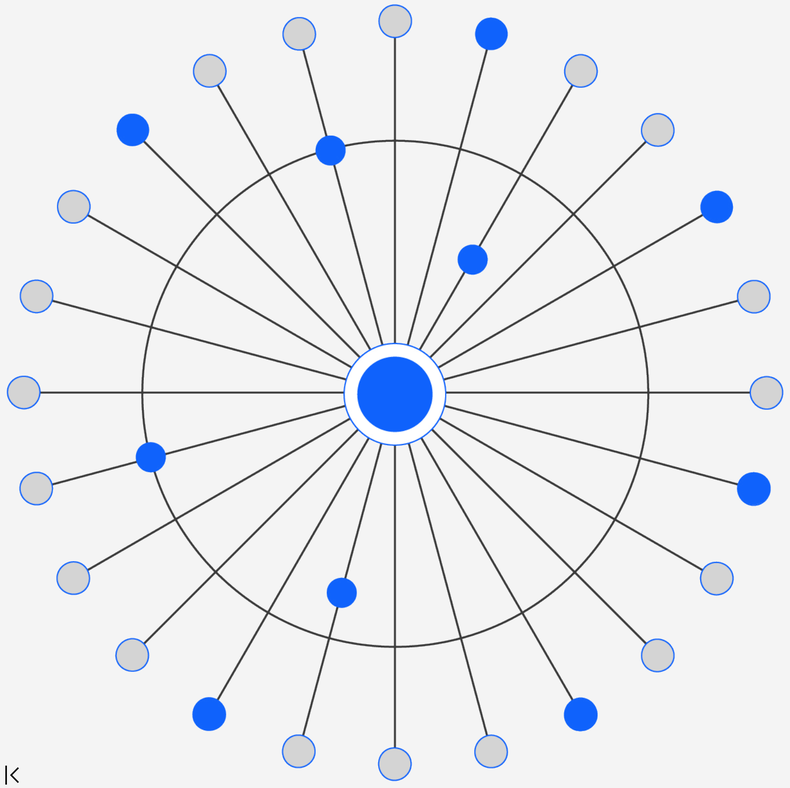
Planifier un entretien →

IBM Security

IBM Security s'adapte à votre environnement en constante évolution et travaille avec vous pour vous maintenir sur la bonne voie. Grâce à nos capacités dynamiques d'IA et d'automatisation, nous vous aidons à toujours conserver une longueur d'avance et à agir plus vite et avec plus de précision. Soyez sûr de prendre les bonnes décisions aujourd'hui et demain grâce aux conseils de notre équipe digne de confiance, composée de spécialistes leaders du secteur. Prévision des menaces ou protection des données ; collaboration avec d'autres fournisseurs ou dans le monde entier ; quelle que soit la direction que prend votre organisation, IBM Security peut vous aider à atteindre des objectifs commerciaux ambitieux, tout en explorant de nouvelles technologies essentielles et en vous aidant à minimiser les menaces inattendues.

En savoir plus →

Contributeurs



Michael Worley
Christopher Caridi
Michelle Alvarez
Karlina Bakken
Yannick Bedard
Michele Brancati
Christopher Bedell
Joshua Chung
Scott Craig
Joseph DiRe
John Dwyer
Emmy Ebanks
Richard Emerson
Charlotte Hammond
Kevin Henson
Guy-Vincent Jourdan
Vio Onut
Mitch Mayne
Dave McMillen
Kat Metrick
Scott Moore
Golo Mühr
Andy Piazza
Benjamin Shipley
Christopher Thompson
Ole Villadsen
Reginald Wong
John Zorabedian

Annexe

Liste des impacts

Impacts	Impacts
Botnet	Minage de cryptomonnaie
Réputation de la marque	Espionnage
Recueil de données d’identification	Extorsion
Destruction de données	Pertes financières
Fuites de données	Arrêt de la production (TO)
Vol de données	Reconnaissance

1. *A timeline of the biggest ransomware attacks*, CNET, 15 novembre 2021
2. *International action against DD4BC cybercriminal group*, Europol, 12 janvier 2016
3. *DD4BC, Armada Collective, and the Rise of Cyber Extortion*, Recorded Future, 7 décembre 2015
4. *A Brief History of Ransomware*, Varonis, 10 novembre 2015
5. *Inside Chimera Ransomware - the first 'doxingware' in wild*, MalwardBytes Labs, 8 décembre 2015
6. *Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware*, Crowdstrike, 14 novembre 2018
7. *Operators of SamSam Continue to Receive Significant Ransom Payments*, Crowdstrike, 11 avril 2018
8. *Triple Extortion Ransomware: The DDoS Flavour*, PacketLabs, 12 mai 2022
9. *They Told Their Therapists Everything. Hackers Leaked It All*, Wired, 4 mai 2021
10. *BazarCall to Conti Ransomware via Trickbot and Cobalt Strike*, The DFIR Report, 1er août 2021
11. *Diavol Ransomware*, The DFIR Report, 13 décembre 2021
12. *Quantum Ransomware*, The DFIR Report, 25 avril 2022
13. *Bumblebee Loader Linked to Conti and Used In Quantum Locker Attacks*, Kroll, 6 juin 2022
14. *This isn't Optimus Prime's Bumblebee but it's Still Transforming*, Proofpoint, 28 avril 2022
15. *Understanding REvil: REvil Threat Actors May Have Returned (Updated)*, Unit 42, 3 juin 2022
16. *AdvIntel's State of Emotet aka "SpmTools" Displays Over Million Compromised Machines Through 2022*, AdvIntel, 13 septembre 2022
17. *Back in Black: Unlocking a LockBit 3.0 Ransomware Attack*, NCC Group, 19 août 2022
18. *Back in Black: Unlocking a LockBit 3.0 Ransomware Attack*, NCC Group, 19 August 2022

Compagnie IBM France
17 avenue de l'Europe
92275 Bois-Colombes Cedex

Produit aux États-Unis d'Amérique
Février 2023