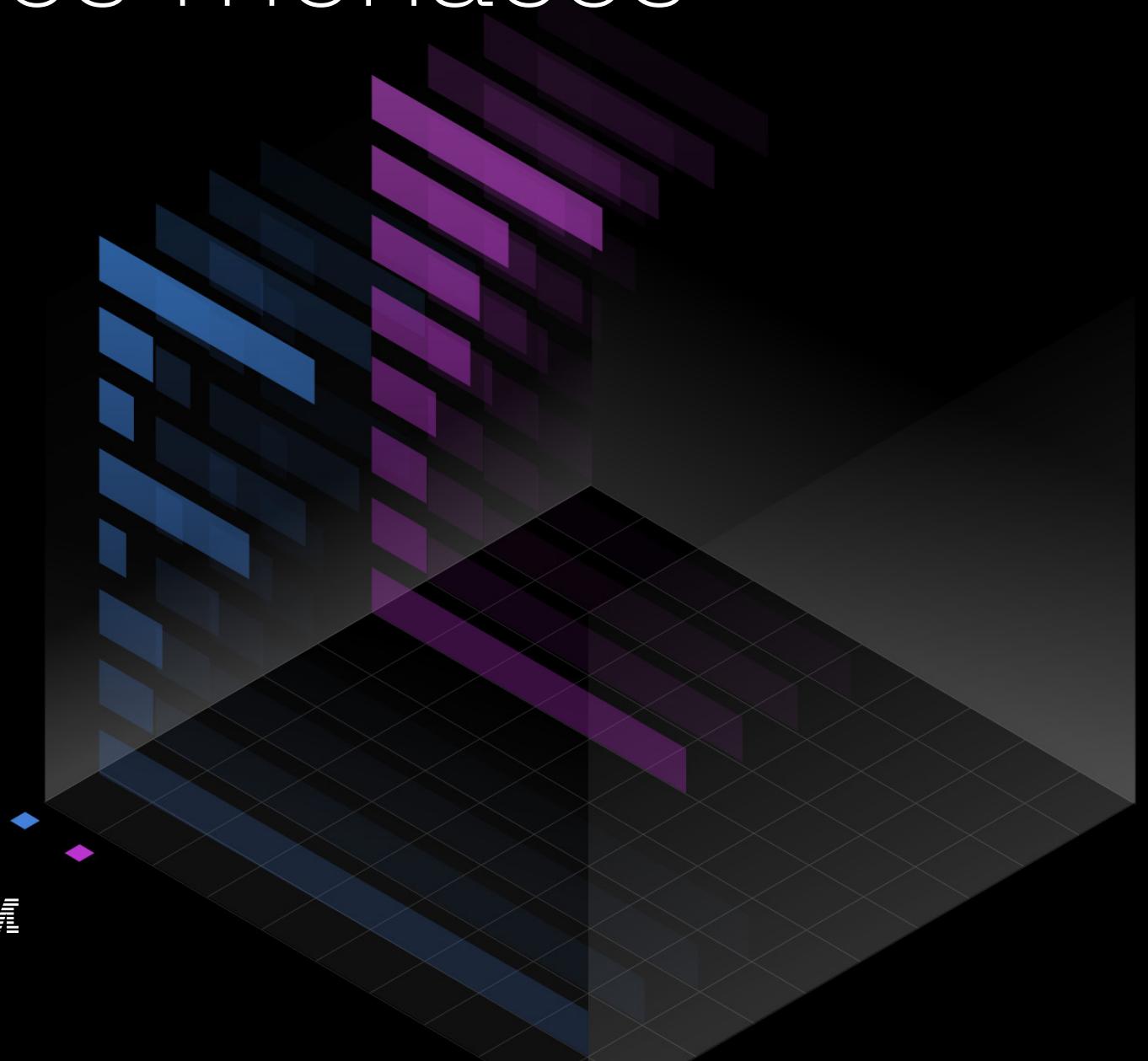




Rapport X-Force de veille des menaces 2021



IBM

Sommaire

Introduction	03
Synthèse	05
Principales attaques de 2020	07
Cyberattaquants avancés	14
Menaces contre l'OT et les ICS	18
Principales marques usurpées	20
Nouvelles menaces dues aux logiciels malveillants	22
Cybercriminalité financière	26
Tendances géographiques et sectorielles	28
Regards sur l'avenir	47
Recommandations pour la résilience	48
À propos d'IBM Security X-Force	49
Contributeurs	50

Synthèse

L'année 2020 a sans aucun doute été l'une des plus importantes sur le plan des conséquences et des changements ces derniers temps : une pandémie mondiale, des bouleversements économiques qui ont impacté la vie de millions de personnes, des troubles sociaux et politiques. Ces événements ont eu des répercussions profondes sur les entreprises, nombre d'entre elles opérant un virage majeur en commençant à fonctionner avec des équipes distantes ou dispersées géographiquement.

Dans le cybermonde, les extraordinaire circonstances de 2020 ont ouvert des brèches où les cybercriminels se sont engouffrés pour exploiter les faiblesses des réseaux de communication. Elles ont aussi dévoilé des cibles riches de promesses au sein des chaînes d'approvisionnement et des infrastructures stratégiques. L'année s'est terminée comme elle avait commencé, avec la découverte d'une menace aux implications mondiales qui nécessitait de réagir et de trouver des solutions rapidement. Une attaque largement attribuée à un acteur piloté par un État-nation, exploitant une [porte dérobée dans un logiciel de surveillance de réseau](#) pour attaquer des organisations gouvernementales et des entreprises du secteur privé, a démontré que le risque imputable à des tiers doit être anticipé, mais ne peut pas être prédit.

Pour aider à relever les défis de cette époque, IBM Security X-Force évalue le contexte des cybermenaces, aide les entreprises à comprendre l'évolution des menaces et les risques qui en découlent, et leur apprend à hiérarchiser les initiatives de cybersécurité. Outre l'exceptionnel travail de veille des menaces que nous fournissons aux clients, nous analysons la masse des données que nous recueillons pour publier notre document X-Force Threat Intelligence Index, un bilan annuel du contexte des menaces et de son évolution.

Parmi les tendances que nous avons suivies, les ransomware, ou rançongiciels, ont poursuivi leur progression pour devenir le type de menace numéro un. Ils représentent 23 % des événements de sécurité traités par X-Force en 2020. Pour extorquer des paiements, les attaquants utilisant les ransomware ont fait monter la pression grâce à un mode opératoire mixte, combinant le cryptage des données et la menace de les divulguer sur des sites publics. Le succès de ces stratégies a permis à un seul gang d'emboîcher plus de 123 millions de dollars en 2020¹, selon les estimations de X-Force.

Le secteur manufacturier a subi une avalanche de ransomware et d'autres attaques en 2020. Pris dans son ensemble, le secteur manufacturier a été le deuxième le plus ciblé, après le secteur de la finance et des assurances. Il avait été le huitième secteur le plus attaqué en 2019. X-Force a découvert des attaquants sophistiqués qui utilisaient des campagnes ciblées de harponnage (spear phishing) dans leurs attaques contre des entreprises manufacturières et des ONG participant à la [chaîne d'approvisionnement du vaccin contre le COVID-19](#).

1. Toutes les sommes indiquées dans ce rapport sont exprimées en dollars américains.

Les agresseurs avaient en outre peaufiné leurs logiciels malveillants, en particulier ceux qui ciblaient Linux, le code open source qui prend en charge l'infrastructure cloud et le stockage de données stratégiques. L'analyse d'Intezer a révélé en 2020 56 nouvelles familles de logiciels malveillants ciblant Linux, soit un niveau d'innovation bien supérieur à celui des autres types de menaces.

Il y a des raisons d'espérer que 2021 sera une meilleure année. Les tendances sont notoirement difficiles à prévoir, mais il existe cependant une constante sur laquelle nous pouvons compter : le changement. La résilience face au va-et-vient des défis en matière de cybersécurité exige des renseignements exploitables et une vision stratégique de l'avenir, garantissant une sécurité plus ouverte et plus connectée.

Fidèle à un esprit dont le postulat est que la communauté fait la force, IBM Security est heureux de proposer X-Force Threat Intelligence Index, son indice de veille des menaces pour 2021. Les résultats de ce rapport ont pour objectif d'aider les équipes de sécurité, les professionnels de la gestion des risques, les décideurs, les chercheurs, les médias et d'autres acteurs à comprendre la nature des menaces de l'année écoulée et à se préparer à celles qui vont leur emboîter le pas.



Introduction

IBM Security X-Force s'est appuyé sur des milliards de points de données recueillis auprès de ses clients et de sources publiques entre janvier et décembre 2020 pour analyser les types d'attaques, les vecteurs d'infection et les comparaisons à l'échelon planétaire et par secteurs d'activité. Nous vous présentons ici quelques-unes des principales conclusions du X-Force Threat Intelligence Index.

23 %

Part des ransomware dans les attaques Les ransomware ont été la méthode d'attaque la plus populaire en 2020, représentant 23 % de tous les incidents traités et résolus par IBM Security X-Force.

Plus de 123 millions de dollars

Estimation des gains générés par les meilleurs ransomware Selon une estimation basse de X-Force, les cyberattaquants exploitant le ransomware Sodinokibi (également connu sous le nom de REvil) ont à eux seuls engrangé au moins 123 millions de dollars en 2020 et dérobé environ 21,6 téraoctets de données.

25 %

Part de la principale vulnérabilité utilisée dans les attaques au premier trimestre 2020 Les cyberattaquants ont exploité une faille Citrix de type traversée de répertoire, mettant à profit cette vulnérabilité dans 25 % de toutes les attaques au cours des trois premiers mois de l'année, pour un total de 8 % des attaques en 2020.

35 %

Part des attaques par analyse et exploitation des vulnérabilités dans les principaux vecteurs d'infection L'analyse et l'exploitation des vulnérabilités sont devenues le premier vecteur d'infection en 2020, dépassant le hameçonnage (phishing) qui était le principal vecteur en 2019.

N° 2

Classement du secteur manufacturier parmi les secteurs les plus attaqués Le secteur manufacturier a été le deuxième secteur le plus attaqué en 2020, alors qu'il n'occupait que la huitième place en 2019, et n'a été dépassé que par les services financiers.

5 heures

Durée des vidéos de formation aux attaques sur un serveur de groupe de menaces Des erreurs opérationnelles commises par des attaquants de l'État-nation iranien ont permis aux chercheurs de X-Force de découvrir environ 5 heures de vidéo sur un serveur incorrectement configuré, et ainsi d'avoir un aperçu de leurs techniques.

Plus de 100

Cadres ciblés par une campagne de hameçonnage de précision À la mi-2020, X-Force a découvert une campagne mondiale de hameçonnage qui a atteint plus de 100 cadres de haut rang occupant des rôles de management et d'approvisionnement pour un groupe de travail chargé d'acheter des équipements de protection individuelle (EPI) dans la lutte contre le COVID-19.

49 %

Taux de croissance des vulnérabilités liées aux ICS, 2019-2020 Les vulnérabilités liées aux systèmes de contrôle industriel (ICS) découvertes en 2020 ont augmenté de 49 % en un an par rapport à 2019.

56

Nombre de nouvelles familles de logiciels malveillants ciblant Linux Le nombre de nouvelles familles de logiciels malveillants ciblant Linux découvertes en 2020 était de 56, un chiffre record. Ce chiffre représente une augmentation de 40 % sur un an par rapport à 2019.

31 %

Part des pays européens attaqués L'Europe a été la région géographique la plus attaquée en 2020, avec 31 % des attaques observées par X-Force, suivie de l'Amérique du Nord (27 %) et de l'Asie (25 %).

Principales attaques de 2020

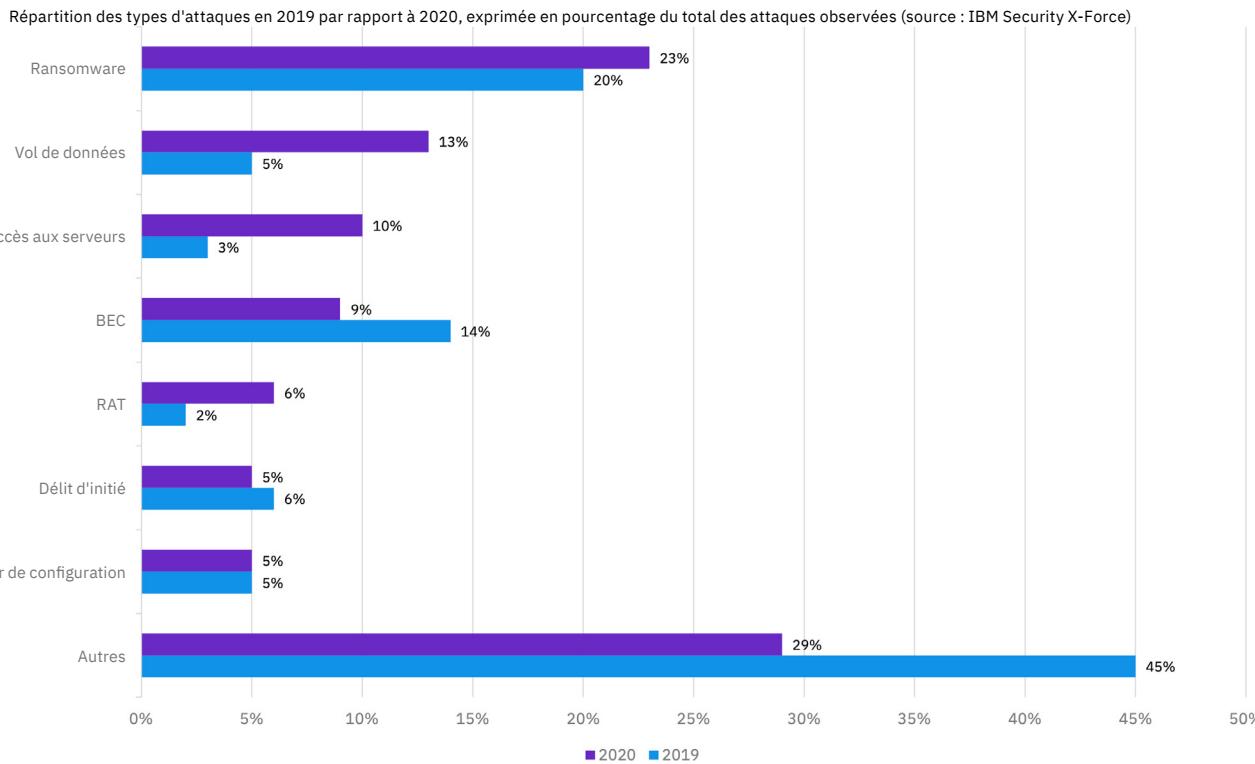
Une bonne compréhension du contexte des attaques peut aider les équipes de sécurité à hiérarchiser les ressources, à rechercher les scénarios les plus probables et à identifier les changements dans les techniques des attaquants.

Les sous-sections suivantes fournissent des indications sur les principales tendances des attaques identifiées par X-Force en 2020 : les attaques par ransomware arrivent indéniablement à la première place, suivies de loin par le vol de données et les attaques par accès aux serveurs. En ce qui concerne les vecteurs d'attaque initiaux, l'analyse et l'exploitation se sont classées premières en 2020, suivies du hameçonnage (phishing) et du vol d'identifiants.²

Les 3 principaux types d'attaques	Les 3 principaux vecteurs d'attaque initiaux
1. Ransomware (23 % des attaques)	1. Analyse et exploitation (35 % des attaques contre 30 % en 2019)
2. Vol de données (augmentation de 160 % depuis 2019)	2. Hameçonnage (33 % des attaques contre 31 % en 2019)
3. Accès aux serveurs (augmentation de 233 % depuis 2019)	3. Vol d'identifiants (18 % des attaques contre 29 % en 2019)

Figure 1

Principaux types d'attaque : comparatif entre 2020 et 2019



2. Les termes « attaques » et « incidents » sont utilisés de manière interchangeable dans ce rapport. Un incident désigne le cas où une entreprise appelle en urgence l'équipe X-Force Incident Response, avec pour conséquence l'ouverture d'une enquête et/ou la remédiation d'une attaque ou d'une attaque suspectée.

L'activité des ransomware a explosé

Les attaques par ransomware ont représenté 23 % de tous les incidents observés dans les engagements de X-Force en 2020, contre 20 % l'année précédente, une hausse qui laisse à penser qu'un nombre croissant de cybercriminels jugent les ransomware rentables.

Les cyberattaquants ont mené des attaques par ransomware principalement en accédant aux environnements choisis comme victimes via un protocole informatique à distance, le vol d'identifiants ou le hameçonnage. Tous ces vecteurs d'attaque ont déjà été exploités de la même manière pour installer des ransomware au cours des années précédentes.

Les cyberattaquants réussissent en outre mieux leurs attaques en élargissant leurs chaînes d'attaque. Selon les observations de X-Force, les groupes exploitant les ransomware qui ont le mieux réussi en 2020 ont privilégié la création de cartels de ransomware sous forme de service (RaaS) et l'externalisation des aspects clés de leurs opérations à des cybercriminels spécialisés dans différents aspects d'une attaque.

59 % des attaques par ransomware ont utilisé une double stratégie d'extorsion, selon les données X-Force de réponse aux incidents. Toutefois, comme les entreprises ont la possibilité d'effectuer une reprise à partir de sauvegardes et ainsi de ne pas payer la rançon, les attaquants ont changé de tactique, ne se contentant plus de chiffrer les données et d'empêcher d'y accéder. Désormais, ils dérobent aussi les données, puis menacent de divulguer les données sensibles en cas de refus de paiement de la rançon. Certains fournisseurs de ransomware ont même organisé des enchères sur le dark web pour vendre les informations sensibles subtilisées à leurs victimes.

De ce fait, selon son estimation la plus prudente, X-Force évalue le revenu total des rançons obtenues par Sodinokibi à 123 millions de dollars en 2020, grâce à l'utilisation de ces tactiques d'extorsion. Les développeurs de ransomware ont, en résumé, trouvé un moyen de contourner l'échappatoire que représentaient les sauvegardes pour les entreprises, car ils peuvent brandir la menace de la divulgation des données comme levier pour extorquer des paiements.

La crainte d'une atteinte à la réputation suite à une divulgation de données sensibles peut causer des préjudices importants à l'entreprise et à ses clients, avec pour conséquences des poursuites et de lourdes amendes réglementaires, en plus des coûts d'une reprise qui demande beaucoup de temps. Lorsque les attaquants par ransomware diffusent publiquement des données sensibles sur des sites de divulgation, ces violations de sécurité sont souvent relayées par les médias, ce qui aggrave l'atteinte à la réputation découlant de ces attaques. En analysant les violations de sécurité rendues publiques, X-Force a calculé qu'elles ont été composées à 36 % de divulgations de données suite à des attaques par ransomware en 2020.

Sodinokibi, le type de ransomware le plus courant

Les deux principaux types de ransomware observés par X-Force en 2020 étaient Sodinokibi (22 % des incidents dus aux ransomware) et Nefilim (11 %). Tous deux combinaient le vol de données avec des attaques par ransomware.

Les autres types de ransomware fréquemment observés par X-Force ont été RagnarLocker (7 %), Netwalker (7 %), Maze (7 %), Ryuk (7 %) et EKANS (4 %), tandis que les 42 % restants des attaques par ransomware se comptaient de petits échantillons d'autres types de ransomware tels que Egregor, CLOP, Medusa et autres.

59 %

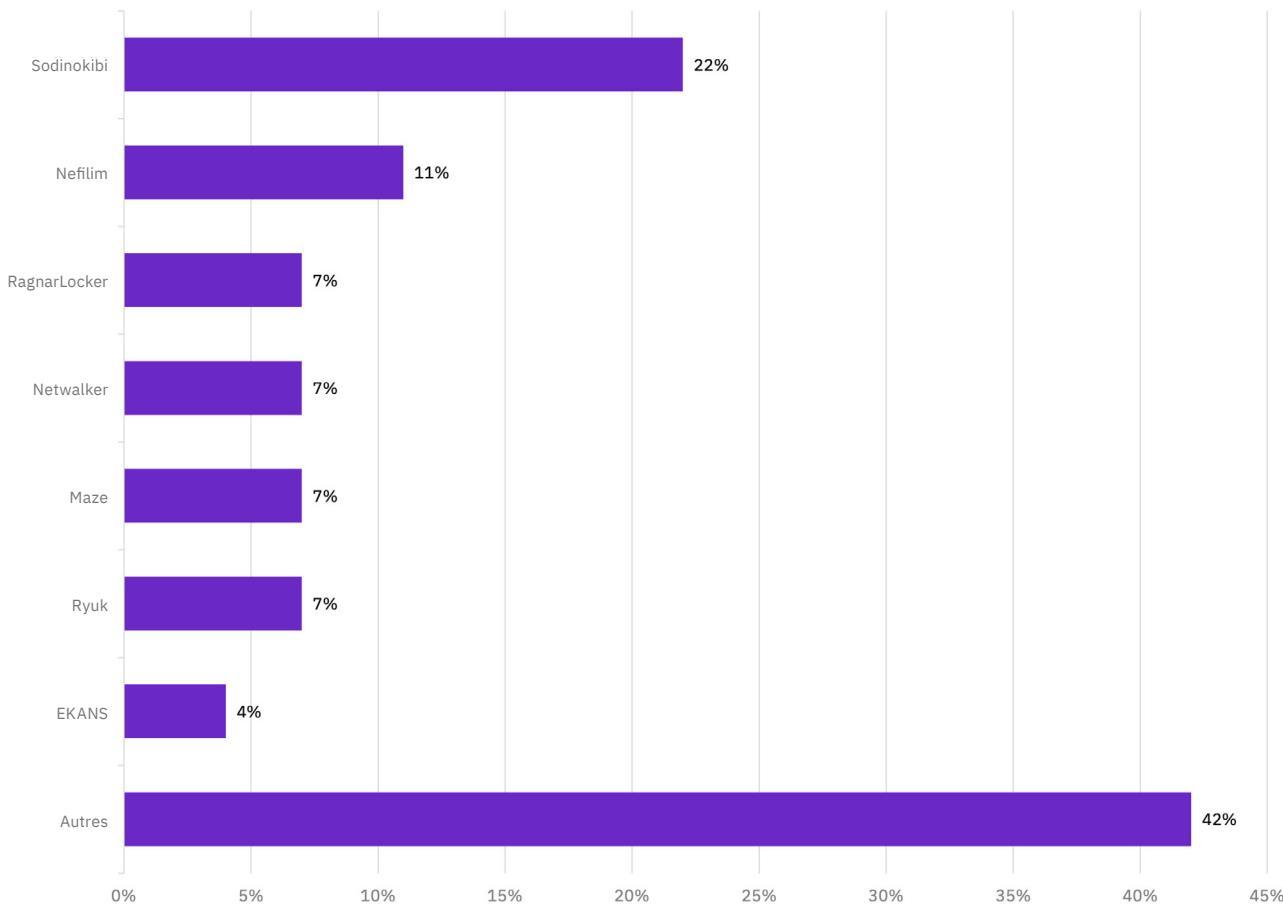
des attaques par ransomware ont utilisé une double stratégie d'extorsion

Plus de 123 millions de dollars

Estimation des bénéfices réalisés par les utilisateurs de Sodinokibi en 2020

Figure 2**Principaux types de ransomware**

Répartition en pourcentage des types de ransomware observés en 2020 (source : IBM Security X-Force)



Sodinokibi étant le type de ransomware le plus fréquemment observé par X-Force en 2020, nous avons rassemblé une quantité appréciable de données et d'indications sur ces attaques et les avons suivies de près : non seulement les attaques de Sodinokibi contre les clients IBM, mais toutes les attaques revendiquées par le groupe.

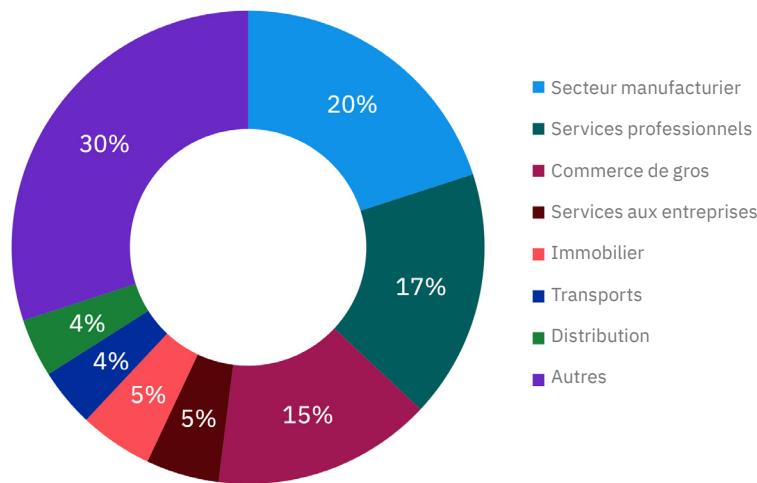
Plusieurs tendances ont émergé de nos recherches :

- Les attaques par le ransomware Sodinokibi ont culminé en juin ou juillet 2020, puis ont de nouveau augmenté après une brève accalmie en août et septembre, sans doute due à la disponibilité des cyberattaquants, aux vacances et aux obligations liées à d'autres emplois.
- Le secteur manufacturier, les services professionnels et la vente en gros ont été les les plus fréquemment ciblés par Sodinokibi, probablement parce que ses utilisateurs ont estimé que les entreprises de ces secteurs avaient une faible tolérance aux temps d'indisponibilité - peut-être plus que d'habitude pendant la pandémie - ou hébergeaient des données particulièrement sensibles. (*voir la Figure 3*)
- Les demandes de rançon de Sodinokibi avaient tendance à représenter de 1 à 5 % des revenus annuels totaux de l'entreprise victime, et dans un cas, avaient atteint 42 millions de dollars.

Figure 3

Attaques du ransomware Sodinokibi par secteur d'activité

Répartition en pourcentage par secteur d'activité des attaques du ransomware Sodinokibi observées en 2020
(source : IBM Security X-Force)



Le ransomware Sodinokibi en chiffres

Régions géographiques les plus ciblées

1. États-Unis (58 %)
2. Royaume-Uni (8 %)
3. Australie (5 %)
4. Canada (3 %)

Revenus estimés Total en 2020 : 123 millions de dollars + en août 2020 uniquement : 55 millions de dollars

Estimation du volume total de données dérobées : 21,6 téraoctets

Près des deux tiers des victimes de Sodinokibi en 2020 ont payé une rançon et environ 43 % ont vu leurs données divulguées, selon les estimations de X-Force.

Recommandations pour répondre à une attaque par ransomware

La préparation est fondamentale : Mettez en œuvre et répétez un plan de réponse en cas d'attaque par ransomware, y compris les attaques d'extorsion mixte par ransomware et vol de données.

Protégez vos données en les sauvegardant hors ligne : Les sauvegardes peuvent permettre à votre entreprise d'opérer une reprise rapide et indépendante en cas d'attaque par ransomware.

Mettez en œuvre une défense en profondeur : Utilisez une approche à multiples facettes, par exemple l'authentification multifactorielle sur chaque point d'accès d'un réseau, la bonne visibilité des nœuds finaux, la traque proactive des menaces, la réalisation de tests de pénétration réguliers pour identifier les points faibles d'un réseau, et la correction et l'atténuation rapides des vulnérabilités connues.

Le guide définitif des ransomware

[Inscrivez-vous pour télécharger le livre blanc >](#)

Vol de données

Le vol de données, par lequel un attaquant s'empare des données sensibles des victimes, a représenté 13 % des attaques résolues par X-Force en 2020, soit une augmentation significative par rapport aux 5 % d'attaques de ce type constatées en 2019.

Une rafale d'attaques basées sur le logiciel malveillant Emotet, en septembre et octobre 2020, explique en grande partie l'augmentation significative des attaques par vol de données. Ces attaques d'Emotet, qui ont eu lieu principalement en Asie, ont représenté 46 % de l'activité de vols de données traités par X-Force en 2020.

Le secteur manufacturier a subi le plus gros des attaques par vol de données en 2020, avec 33 % de tous les vols. Le secteur de l'énergie est arrivé en deuxième position, avec 21 % des attaques, et la finance et les assurances en troisième position, avec 17 % des attaques.

Attaques par accès aux serveurs

Les attaques par accès aux serveurs ont été le troisième type d'attaque le plus courant en 2020, soit 10 % de toutes les attaques traitées par X-Force Incident Response en 2020. Dans une attaque par accès au serveur, un cyberattaquant obtient un accès non autorisé au serveur d'une victime, soit en exploitant des identifiants de serveur volés, soit en exploitant une vulnérabilité ou par d'autres moyens.

Près de 36 % des attaques par accès au serveurs observées par X-Force Incident Response en 2020 visaient le secteur de la finance et des assurances, mais les services aux entreprises (14 %), le secteur manufacturier (7 %) et la santé (7 %) ont été eux aussi durement touchés.

C'est la réussite de l'exploitation de CVE-2019-19781, une faille Citrix de type traversée de répertoire, qui a renforcé les attaques par accès aux serveurs.

Vulnérabilité Citrix CVE-2019-19781

Les données X-Force indiquent que 15 % des incidents survenus au cours du premier semestre 2020 étaient directement liés à la vulnérabilité Citrix CVE-2019-19781, soit 15 fois plus que toute autre vulnérabilité. Cette vulnérabilité, révélée en décembre 2019, affecte Citrix Application Delivery Controller (ADC), Citrix Gateway et NetScaler Gateway. La vulnérabilité permet à un attaquant d'exécuter du code arbitraire sur un serveur Citrix vulnérable.

L'exploitation en chiffres de la faille CVE-2019-19781

- 59 % de tous les incidents en janvier 2020
- 25 % de tous les incidents au premier trimestre 2020
- 15 % de tous les incidents au premier semestre 2020
- 8 % du total des incidents traités par X-Force en 2020
- Plus de 25 000 serveurs Citrix vulnérables connus

La vulnérabilité Citrix exploitée par de nombreux groupes

X-Force a identifié de nombreux groupes d'attaquants qui ont mis à profit la vulnérabilité CVE-2019-19781 en 2020, notamment des groupes sponsorisés par des États ainsi que des cybercriminels à motivation financière. Ces avantages sont notamment :

- [Hive0088](#) (aussi appelé APT41, présumé affilié à l'État chinois)
- [ITG07](#) (aussi appelé Chafer, présumé affilié à l'État iranien)
- [Utilisateurs du ransomware Sodinokibi](#) (aussi appelé REvil)
- [Utilisateurs du ransomware Maze](#)

En accédant aux systèmes grâce à cette vulnérabilité, les attaquants ont dans divers cas installé des chevaux de Troie d'accès à distance (RAT) tels qu'Adwind, déployé les logiciels malveillants intermédiaires Trickbot et Cobalt Strike, et même déployé des ransomware, notamment Sodinokibi et Maze. Certains attaquants l'ont également utilisé pour accéder aux réseaux pour exécuter des attaques par ransomware.

Les 10 vulnérabilités les plus exploitées en 2020

Nous vous présentons ici la liste des 10 principales vulnérabilités exploitées en 2020. Il convient de noter que seules deux des vulnérabilités de cette liste ont été divulguées en 2020, ce qui souligne la menace persistante posée par les vulnérabilités anciennes. Tout au long de 2020, les cyberattaquants ont davantage tendu à exploiter une vulnérabilité de 2019 ou d'une année antérieure, probablement parce qu'il était difficile d'exploiter un grand nombre des vulnérabilités révélées en 2020 et de corriger les vulnérabilités anciennes rencontrées par de nombreuses entreprises.

1. **CVE-2019-19781** : Citrix Application Delivery Controller
2. **CVE-2018-20062** : Vulnérabilité de type RCE (exécution de code à distance) dans NoneCMS ThinkPHP
3. **CVE-2006-1547** : ActionForm dans Apache Software Foundation (ASF) Struts
4. **CVE-2012-0391** : Composant ExceptionDelegator dans Apache Struts
5. **CVE-2014-6271** : Injection de commande GNU Bash
6. **CVE-2019-0708** : Vulnérabilité « Bluekeep » de type RCE (exécution de code à distance) dans les services Bureau à distance de Microsoft
7. **CVE-2020-8515** : Injection de commande Draytek Vigor
8. **CVE-2018-13382 et CVE-2018-13379** : Autorisation incorrecte et traversée de répertoire dans Fortinet FortiOS
9. **CVE-2018-11776** : Vulnérabilité de type RCE (exécution de code à distance) dans Apache Struts
10. **CVE-2020-5722** : HTTP : Injection SQL dans Grandstream UCM6200

Principaux vecteurs d'infection

Impulsées par l'exploitation intensive de CVE-2019-19781, l'analyse et l'exploitation des vulnérabilités sont devenues le vecteur d'infection initial le plus couramment utilisé par les cyberattaquants, soit 35 % de tous les incidents comportant un vecteur d'attaque connu³ traité par X-Force. En comparaison, l'analyse et l'exploitation n'étaient le vecteur d'infection que dans 30 % des attaques de l'année précédente.

Les attaques par analyse et exploitation ne nécessitent généralement que peu de ressources et peuvent être automatisées et mises à l'échelle pour cibler une grande variété de victimes, ce qui peut expliquer pourquoi ce vecteur a connu un volume aussi élevé en 2020. En plus de la vulnérabilité de traversée de répertoire dans Citrix, les attaques par analyse et exploitation en 2020 incluaient le ciblage de la vulnérabilité Heartbleed, des protocoles de gestion vulnérables ou mal configurés et l'exploitation de la vulnérabilité cryptographique CVE-2017-9248.

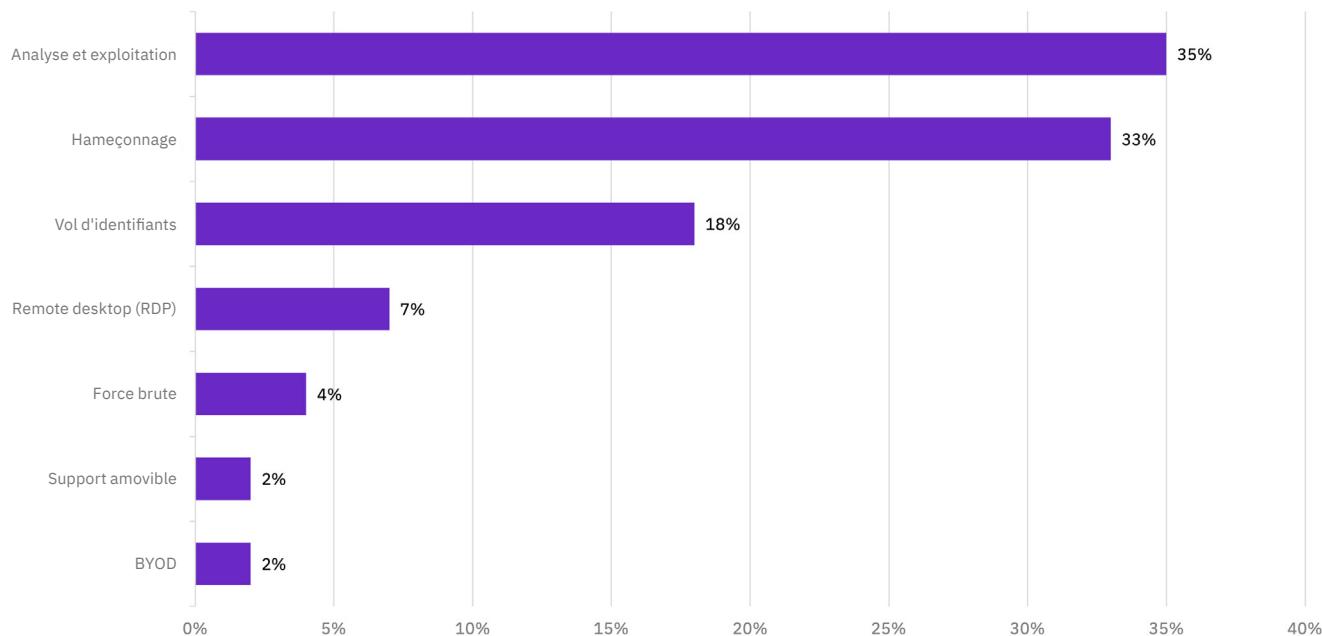
Le hameçonnage (phishing) a été le deuxième vecteur d'infection le plus couramment utilisé, dans 33 % des attaques, en légère hausse par rapport à 31 % l'an dernier. Ces chiffres font penser que les modifications des techniques des attaquants et les mécanismes de défense contre le hameçonnage sont restés synchrones.

Le vol d'identifiants n'a représenté que 18 % des attaques, soit une baisse significative par rapport aux 29 % de l'année dernière. Ces résultats suggèrent que les cyberattaquants ont préféré utiliser les techniques d'analyse et d'exploitation pour de nombreux compromis en 2020, probablement en raison de leur taux de réussite plus élevés.

Figure 4

Les principaux vecteurs d'attaque initiaux

Répartition en pourcentage des sept vecteurs d'attaque initiaux observés par IBM Security X-Force Incident Response en 2020
(source : IBM Security X-Force)



3. Plusieurs incidents n'avaient pas de vecteur d'attaque connu et ne sont donc pas inclus dans ces données.

Cyberattaquants avancés

Tout au long de 2020, X-Force s'est aperçu que certains groupes d'attaquants commettaient des erreurs opérationnelles, se trahissant ainsi involontairement et lui fournissant des informations précieuses. Dans d'autres cas, le suivi des cyberattaquants avancés a permis de recueillir des informations précieuses sur les menaces en lien avec le COVID-19, révélant notamment que les agresseurs ciblaient la distribution des vaccins et continuaient à mettre à profit la pandémie pour piéger les utilisateurs par hameçonnage.

Des groupes d'attaquants iraniens pris la main dans le sac

En septembre 2020, les analystes de X-Force ont découvert une infrastructure associée à l'activité de hameçonnage Hive0082. Hive0082, également appelé Silent Librarian, COBALT DICKENS ou TA407, cible activement les établissements universitaires mondiaux depuis au moins 2013, malgré de multiples [divulgations publiques](#) de son activité.

L'activité de septembre 2020 ne différait pas beaucoup des opérations précédentes. Cependant, les opérateurs avaient oublié des métadonnées générées par les outils utilisés pour usurper les pages de connexion valides des ressources académiques ciblées. Plus précisément, les chercheurs de X-Force ont noté l'utilisation continue de l'extension Chrome « SingleFile » dans ces campagnes. Cette extension peut enregistrer l'horodatage de la machine copiant un site Web. Plusieurs des sites Web usurpés utilisés dans cette campagne contenaient des horodatages « Iran Daylight Time », une erreur probable de la part de l'opérateur de Hive0082. (*voir la Figure 5*)

Figure 5

Activité de hameçonnage de Hive0082

Métadonnées de la page Web usurpée par Hive0082, montrant un horodatage iranien (source : IBM Security X-Force)

```
</script>
<!--
Page saved with SingleFile
url: [REDACTED]
saved date: Mon Apr 08 2019 13:20:57 GMT+0430 (Iran Daylight Time)
-->
```

Dans un autre exemple, les erreurs d'un autre groupe d'attaquants sponsorisé par l'État iranien connu et suivi par X-Force sous le nom d'ITG18 ont fourni un aperçu sans précédent de ses opérations. Le groupe a des antécédents d'erreurs de sécurité opérationnelle, en particulier des erreurs de base de configuration de serveur qui, dans le passé, ont entraîné la divulgation de leurs victimes et, dans un cas, l'entrée d'un ransomware sur l'un de ses serveurs d'exploitation.

En mai 2020, X-Force a découvert un autre serveur incorrectement configuré appartenant à ITG18 et qui contenait plus de 40 gigaoctets de fichiers vidéo et de données. Les vidéos détaillaient la marche à suivre et la technologie utilisées par ITG18 pour effectuer ses opérations de reconnaissance contre les comptes compromis. Les vidéos contenaient également des métadonnées sur ses opérations qui ont révélé par inadvertance l'infrastructure VPN d'ITG18, les numéros de téléphone des attaquants et plusieurs tentatives de hameçonnage infructueuses contre des cibles du gouvernement américain.

Figure 6

Compte AOL de formation d'ITG18

Une configuration erronée du serveur d'ITG18 a révélé le numéro de téléphone de l'attaquant, associé à un compte AOL utilisé pour la formation (source : IBM Security X-Force)

The screenshot shows a user interface for managing an AOL account. On the left, there's a sidebar with icons for 'Informations personnelles', 'Sécurité du compte' (which is selected), 'Activité récente', 'Préférences', and 'Aide'. The main content area has a large title 'Aol.' at the top. Below it, a section titled 'Sécurité du compte' contains 'Mode de connexion' (password activated) and 'Numéros de téléphone' (redacted). A small red box highlights the first digit of the phone number '+98'.

Les informations acquises suite aux erreurs opérationnelles commises par ces deux groupes ont permis aux analystes X-Force de veille des menaces d'avertir les cibles de l'activité en cours, de mieux comprendre les techniques de formation et les méthodologies de vol de mots de passe, et d'identifier l'infrastructure utilisée en temps réel pour réaliser des activités malveillantes. Ces connaissances, à leur tour, nous ont permis de mieux protéger et d'avertir une grande variété d'entreprises susceptibles de constituer des victimes potentielles.

Campagnes de hameçonnage en lien avec le COVID-19

Au cours de ses recherches continues sur la cyberactivité liée au coronavirus, X-Force a découvert diverses campagnes de hameçonnage en rapport avec le COVID-19, menées par des cyberattaquants avancés et ciblant la chaîne d'approvisionnement des vaccins anti-COVID-19.

Attaques contre la chaîne du froid des vaccins

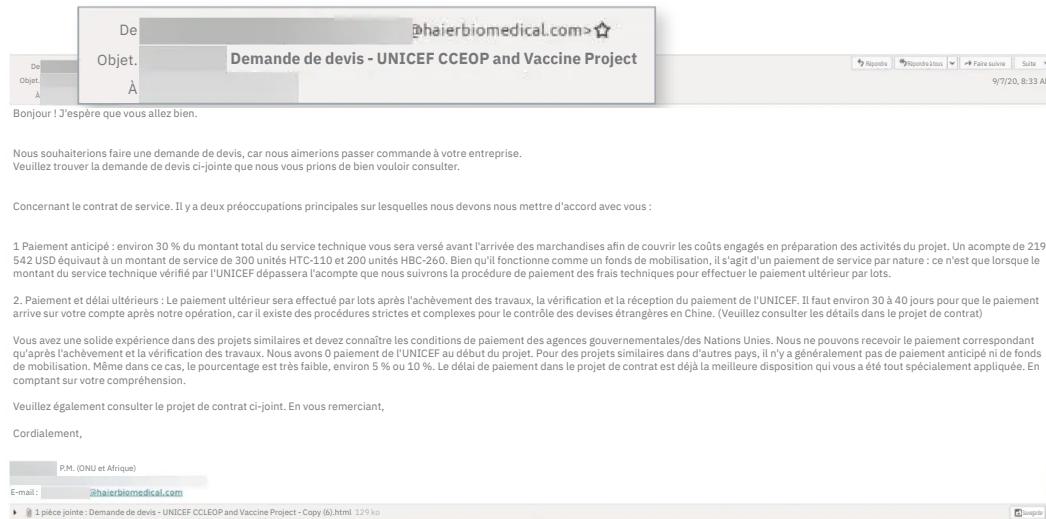
En octobre 2020, X-Force Threat Intelligence a observé une vague d'emails de hameçonnage ciblant des individus, des entreprises et des entités supranationales susceptibles d'être intéressés par les technologies de distribution sécurisée d'un vaccin contre le COVID-19. L'activité détectée avait imité la plateforme CCEOP (Cold Chain Equipment Optimization Platform) de l'UNICEF (Fonds des Nations Unies pour l'enfance) et de Gavi Vaccine Alliance, utilisée pour la distribution des vaccins dans le monde. Bien qu'ils n'aient pas été identifiés à l'heure actuelle, des agresseurs parrainés par un État-nation étaient probablement à l'origine de ces attaques.

Il s'agissait d'une campagne de hameçonnage bien calibrée, conçue par un attaquant qui cherchait vraisemblablement à obtenir des informations approfondies sur les processus de transport et de distribution d'un vaccin COVID-19, grâce à la collecte d'identifiants. Les cibles comprenaient la direction générale de la fiscalité et de l'union douanière de la Commission européenne, ainsi que des entreprises de différents secteurs : énergie, industrie manufacturière, création de sites Web et solutions de sécurité Internet et logicielles. Il s'agit d'entreprises internationales dont le siège se trouve en Allemagne, en Italie, en Corée du Sud, en République tchèque, sur les territoires de la très grande Europe et à Taïwan.

Figure 7

Hameçonnage visant le vaccin COVID-19

Exemple d'email de hameçonnage utilisé dans les attaques contre la chaîne du froid des vaccins anti-COVID-19 (source : IBM Security X-Force)



Attaques contre la chaîne d'approvisionnement des EPI

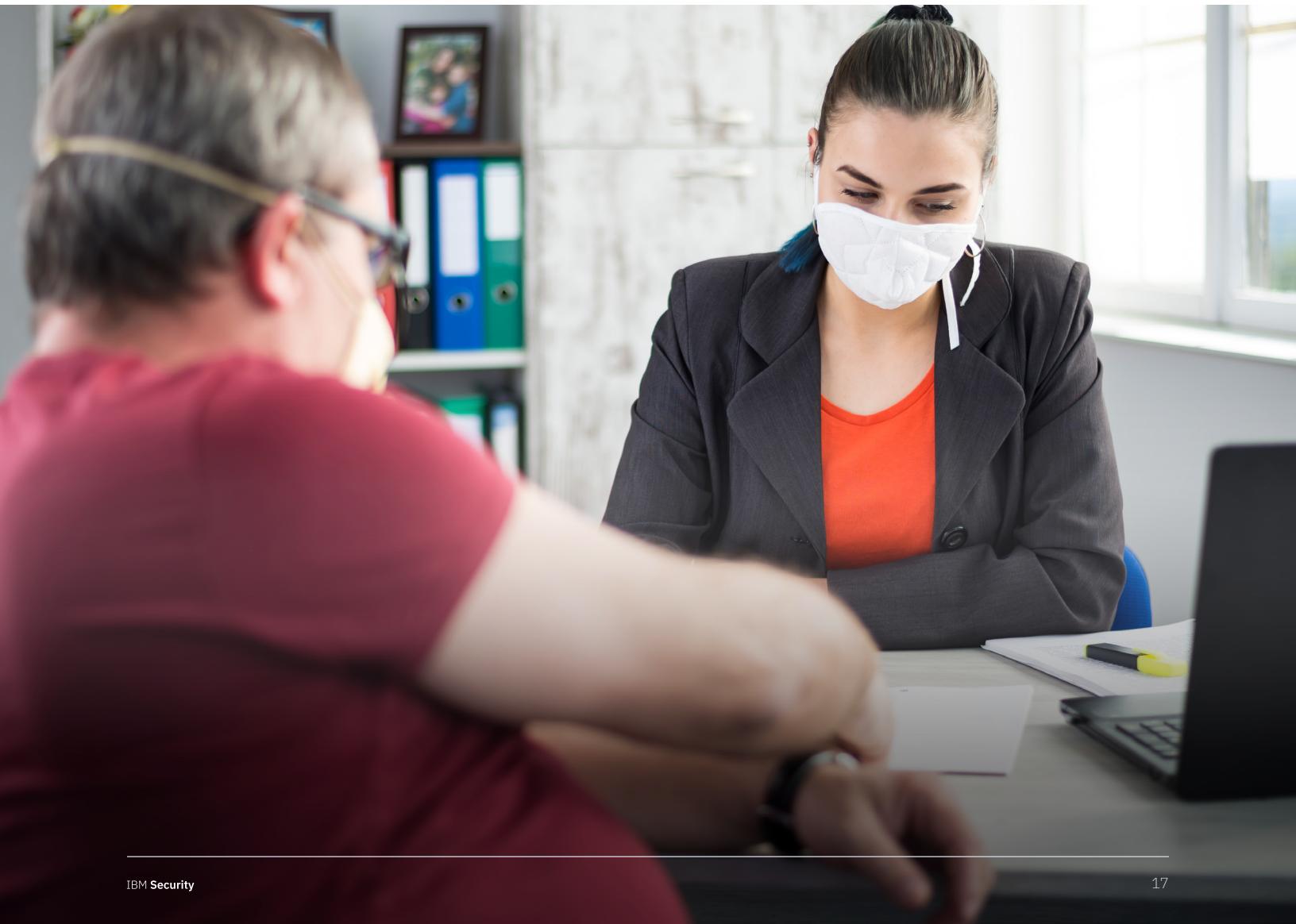
En mai 2020, les travaux de recherche de X-Force ont révélé une attaque contre une multinationale allemande associée à un groupe de travail mixte du gouvernement allemand et du secteur privé, chargée de l'achat d'équipements de protection individuelle (EPI). Cette découverte montre le fonctionnement d'une campagne au ciblage précis, mettant à profit la course à l'approvisionnement en EPI essentiels.

Les attaquants à l'origine de cette campagne ont ciblé plus de 100 cadres de haut rang occupant des rôles de management et d'approvisionnement au sein de cette organisation et de son écosystème de partenaires tiers. Dans l'ensemble, X-Force a observé environ 40 entreprises ciblées dans cette campagne. Compte tenu du ciblage étendu de cette chaîne d'approvisionnement, il est probable que d'autres membres du groupe de travail puissent être des cibles d'intérêt de cette campagne malveillante, nécessitant une vigilance accrue.

Campagne ciblant l'Ukraine

En outre, entre la mi-mars et la mi-avril 2020, X-Force a découvert des fichiers .docx malveillants attribués en toute probabilité à une activité continue suspectée de la part de Hive0051 (aussi appelé [Gamaredon](#)). Cette nouvelle activité semble être cohérente avec le mode opératoire bien établi de Hive0051, qui se concentre sur le ciblage d'entités basées en Ukraine.

Le contenu des fichiers de documents malveillants que nous avons découverts utilisait un mélange de leurre prenant pour thème le COVID-19 et la géopolitique, avec une usurpation d'entités gouvernementales et d'ONG ukrainiennes. Il est fort probable que ce groupe mettait à profit les développements géopolitiques en cours et les préoccupations liées à l'épidémie de COVID-19 pour exploiter la population nationale ukrainienne ou des entités ayant un intérêt significatif pour les développements régionaux.



Menaces ciblant l'OT et les ICS

Les menaces visant l'OT, ou technologie d'exploitation, peuvent avoir des effets bien concrets : déversements de produits chimiques, dysfonctionnements de machines ou même accidents de véhicules. X-Force donne par conséquent la priorité à la recherche et à l'analyse sur la technologie d'exploitation, en se basant sur ses sources de données propriétaires pour fournir une perspective unique des menaces visant les entreprises qui utilisent des réseaux d'OT.

Pour examiner les tendances des attaques contre l'OT en 2020, les analystes de X-Force ont étudié des incidents survenus dans des entreprises du secteur manufacturier, du gaz et du pétrole, des transports, des services publics, du BTP et de l'exploitation minière et qui étaient susceptibles d'affecter les réseaux d'OT.

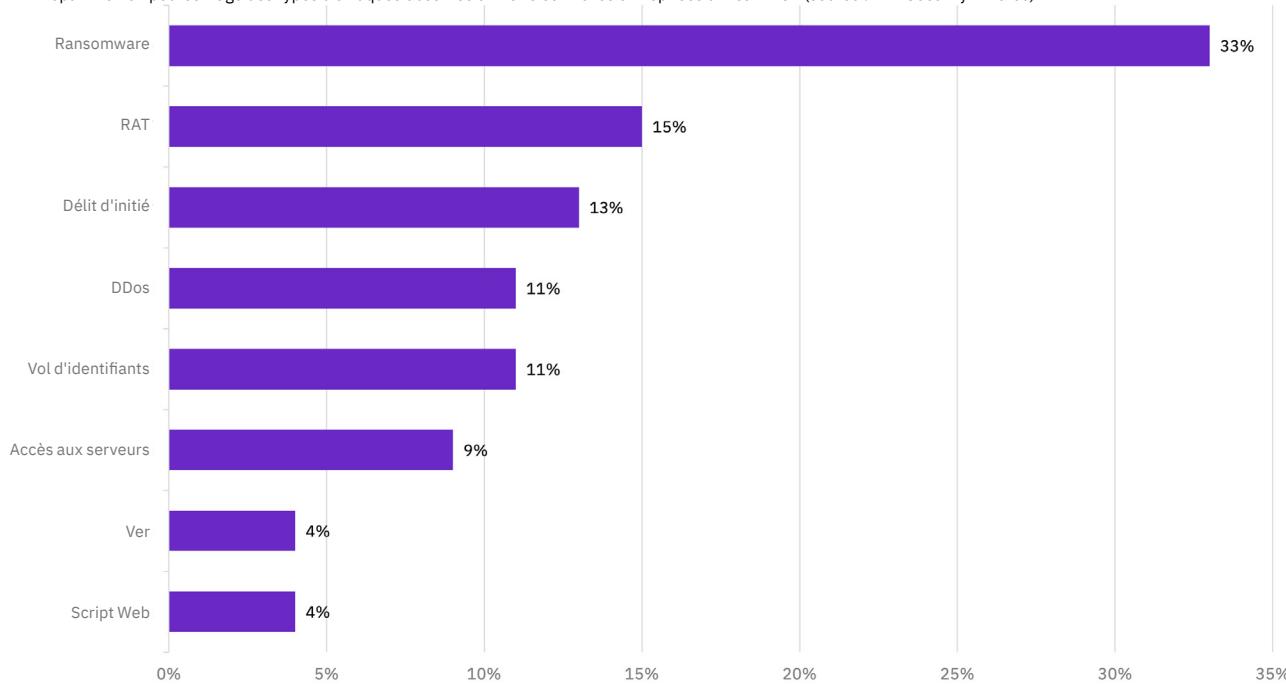
Ransomware

Les attaques par ransomware ont été la menace la plus courante pour l'OT d'après les données de X-Force Incident Response, faisant écho aux tendances globales des attaques observées par X-Force en 2020. Les attaques par ransomware ont représenté 33 % de toutes les attaques contre l'OT en 2020. Cette tendance suggère que les attaquants jugent les entreprises dotées de réseaux d'OT particulièrement intéressantes pour les attaques par ransomware. D'après les observations de X-Force, les principales souches de ransomware utilisées dans les attaques contre des entreprises d'OT en 2020 étaient EKANS, Nefilim, Medusa, PJX et Egregor.

Figure 8

Types d'attaque contre l'OT

Répartition en pourcentage des types d'attaques observés en 2020 contre les entreprises utilisant l'OT (source : IBM Security X-Force)



Chevaux de Troie d'accès à distance (RAT)

Les chevaux de Troie d'accès à distance (RAT) ont été le deuxième type d'attaque le plus courant contre l'OT en 2020, représentant 15 % de toutes les attaques, selon les données X-Force de réponse aux incidents. Les RAT permettent à un attaquant d'accéder à un appareil et d'y activer une surveillance secrète. Trickbot, Adwind et jRAT font partie des RAT observés par X-Force Incident Response sur les réseaux connectés à l'OT en 2020.

Délits d'initiés

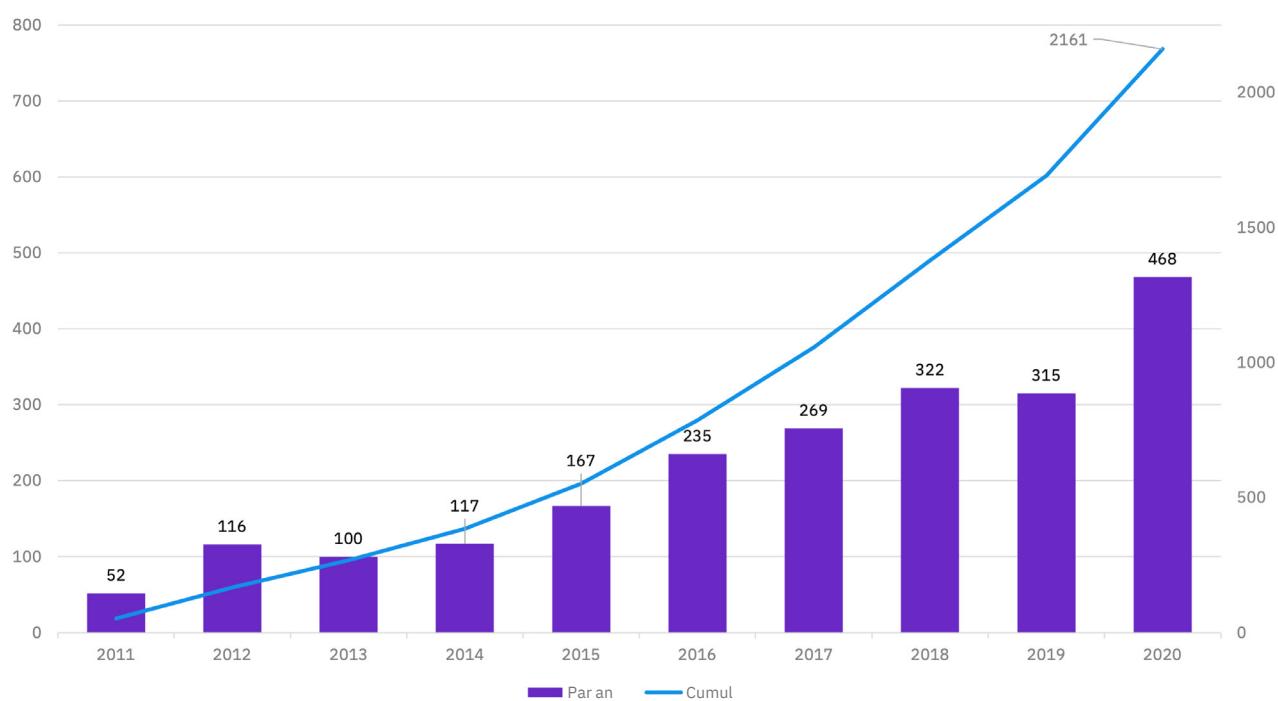
Les incidents causés par des délits d'initiés ont représenté 13 % de tous les incidents liés à l'OT en 2020, 60 % d'entre eux impliquant des délits d'initiés malveillants et 40 % étant dus à une négligence, selon les données de X-Force. Dans le cas de délits d'initiés malveillants, X-Force a déterminé que des employés s'étaient connectés à des sites Web suspects associés à des logiciels malveillants, ou étaient soupçonnés d'avoir vendu des informations propriétaires sur des sites Web tiers.

Vulnérabilités dans les systèmes de contrôle industriels

Figure 9

Vulnérabilités ICS, 2011-2020

Nombre de vulnérabilités divulguées ciblant les ICS, par an et en tant que total cumulé des années 2011 à 2020 (source : IBM Security X-Force)



Le suivi réalisé par X-Force révèle que les vulnérabilités des plates-formes ICS continuent d'augmenter, atteignant un nouveau sommet en 2020, après une légère baisse l'année précédente. En fait, X-Force a observé en 2020 une augmentation de 49 % d'une année sur l'autre des vulnérabilités des ICS. [Les vulnérabilités des ICS](#) sont préoccupantes, car elles agravent le risque pour les systèmes d'OT et peuvent provoquer des effets cinétiques destructeurs.

Principales marques usurpées

Les données de Quad9 effectuent un suivi des domaines malveillants pour avertir et protéger les utilisateurs des activités des cyberattaquants ciblant ces domaines. En moyenne, Quad9 bloque 10 millions de requêtes DNS malveillantes chaque jour, et IBM identifie les domaines malveillants en moyenne huit jours plus tôt que les autres fournisseurs de veille des menaces. X-Force est un partenaire de [Quad9](#) et aide les entreprises à sécuriser les communications Internet via un DNS fiable.

Tout comme en 2019, X-Force et Quad9 ont continué à effectuer le suivi des principales marques usurpées qui ont été utilisées dans des domaines malveillants en 2020. Il s'agit de marques que les attaquants tentent d'imiter, exploitant leur popularité et la confiance qu'elles inspirent aux utilisateurs pour inciter les victimes à ouvrir un e-mail, à cliquer sur un lien ou à divulguer des informations sensibles qui peuvent ensuite être utilisées dans une attaque.

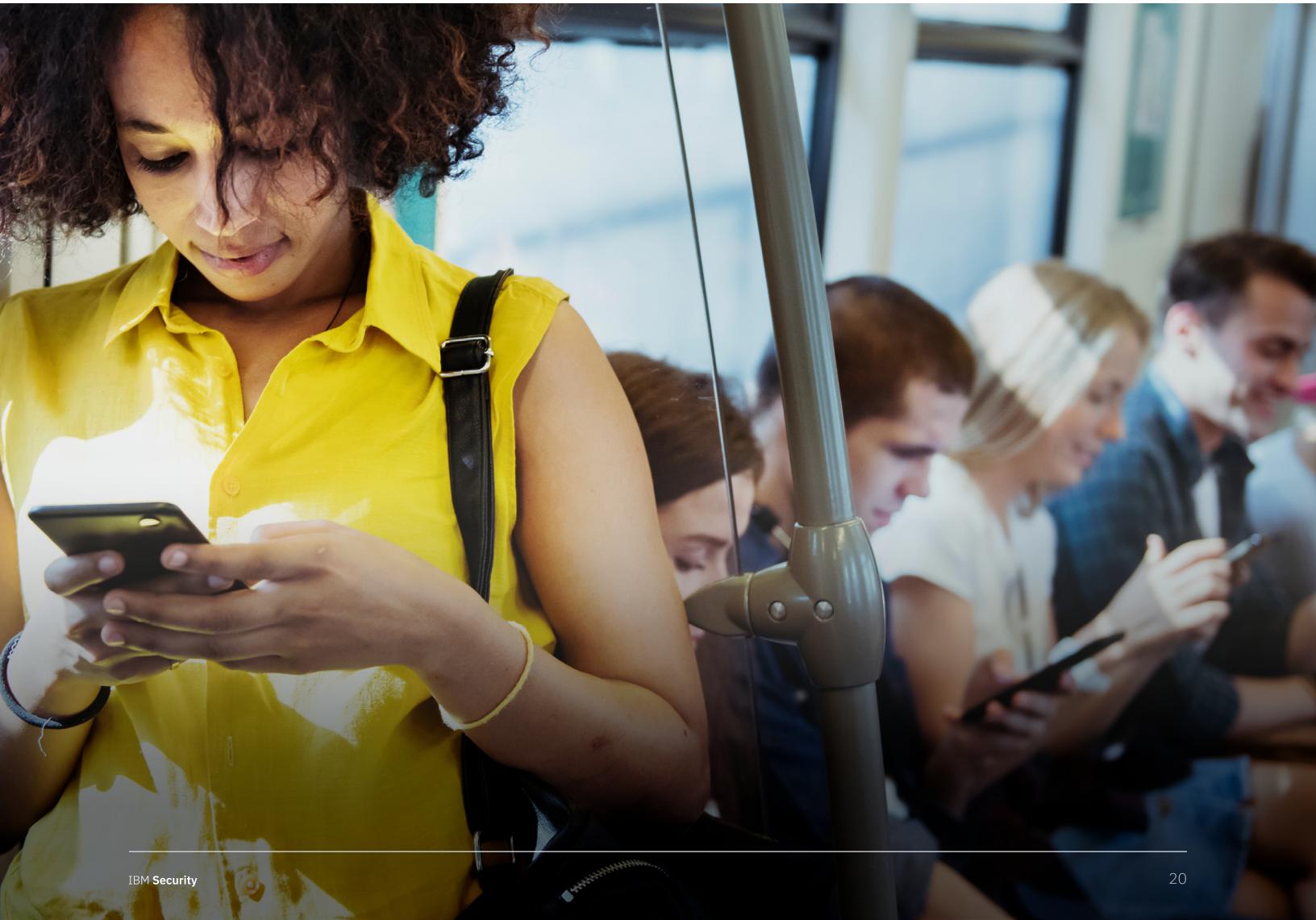
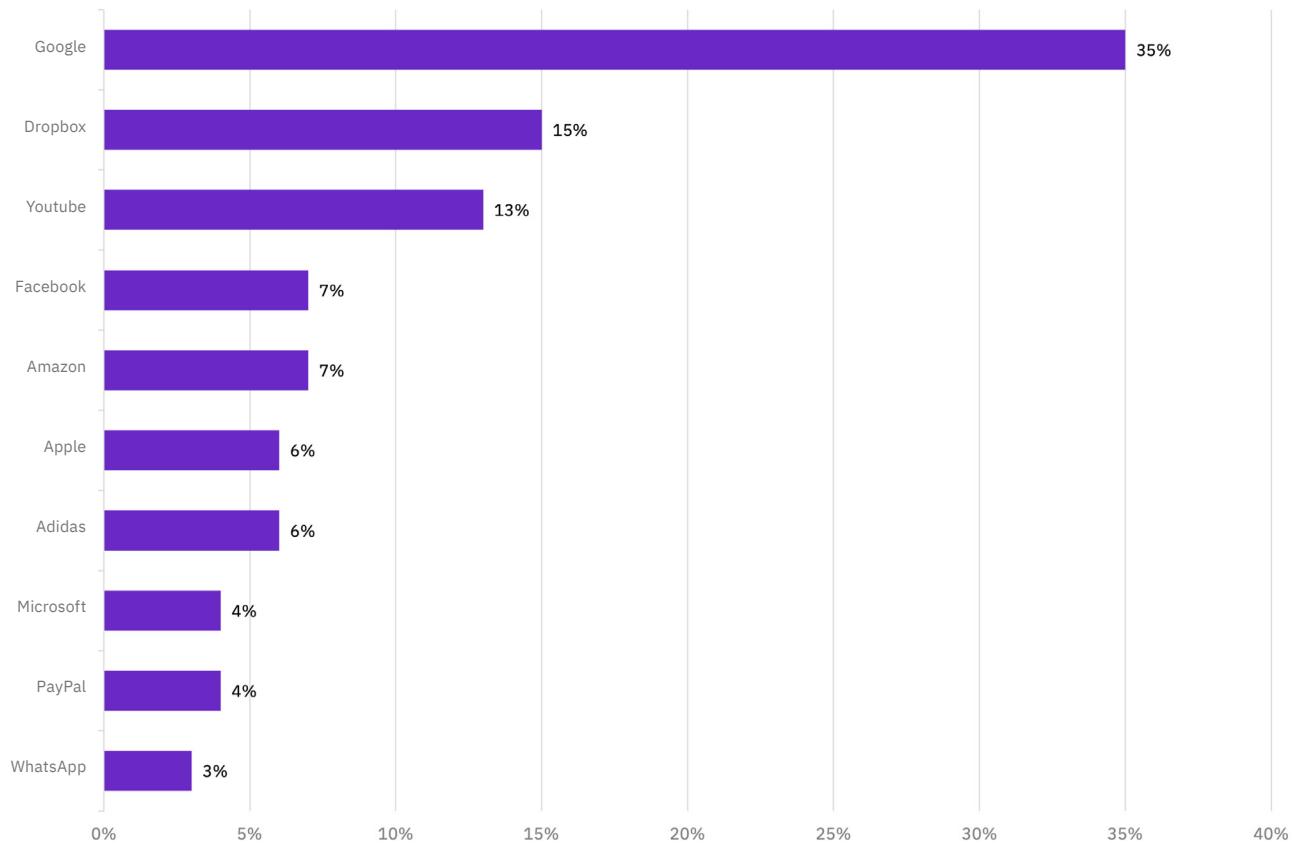


Figure 10**Les 10 marques les plus usurpées**

Répartition des 10 principales marques usurpées par spam en 2020, en pourcentage des 10 marques présentées (source : Quad9)



Les entreprises de technologie et de médias sociaux restent les marques les plus usurpées, Google, Dropbox et YouTube arrivant en tête en termes de pourcentage des marques usurpées en 2020. Google demeure la marque la plus usurpée, tout comme en 2019. Adidas et PayPal ont également fait partie du top 10 en 2020, avec plusieurs autres marques parmi les plus usurpées de l'année précédente : Amazon, Apple, Microsoft et Facebook. La majorité des activités d'usurpation concernant Adidas ont eu lieu en janvier, ce qui laisse à penser qu'elles n'étaient pas liées à la pandémie, mais elles semblent en revanche avoir un lien avec les baskets Superstar et Yeezy. L'arrivée de PayPal dans ce top 10 est très probablement lié à des cybercriminels partageant des intérêts financiers, et désireux de dérober des identifiants ou des fonds.

Les attaquants gravitent probablement vers la technologie d'usurpation et les médias sociaux en raison de leur popularité et du fait qu'ils sont 100 % numériques. En outre, l'usurpation des e-mails et des plates-formes associées aux e-mails telles que Google Gmail ou Microsoft 365 est une technique fréquente chez les attaquants, à en juger par les données X-Force de réponse aux incidents. Ces marques sont également facilement monétisées par les attaquants, car les comptes compromis associés à ces plates-formes populaires peuvent facilement être vendus à bon prix sur le dark web.

Nouvelles menaces liées aux logiciels malveillants

Alors que les cyberattaquants continuent d'adapter, de faire évoluer et de transformer les logiciels malveillants, nos données font ressortir plusieurs tendances concernant leur développement. La prolifération des logiciels malveillants ciblant Linux a été de loin la tendance dominante en 2020, suivie de près par une augmentation des logiciels malveillants écrits dans le langage de programmation Go. Une augmentation spectaculaire des logiciels malveillants Emotet à l'automne 2020 a prouvé que cette souche était réapparue. Chacune de ces tendances souligne un objectif suprême des cyberattaquants : échapper plus efficacement aux techniques de détection.

L'année de tous les dangers pour Linux

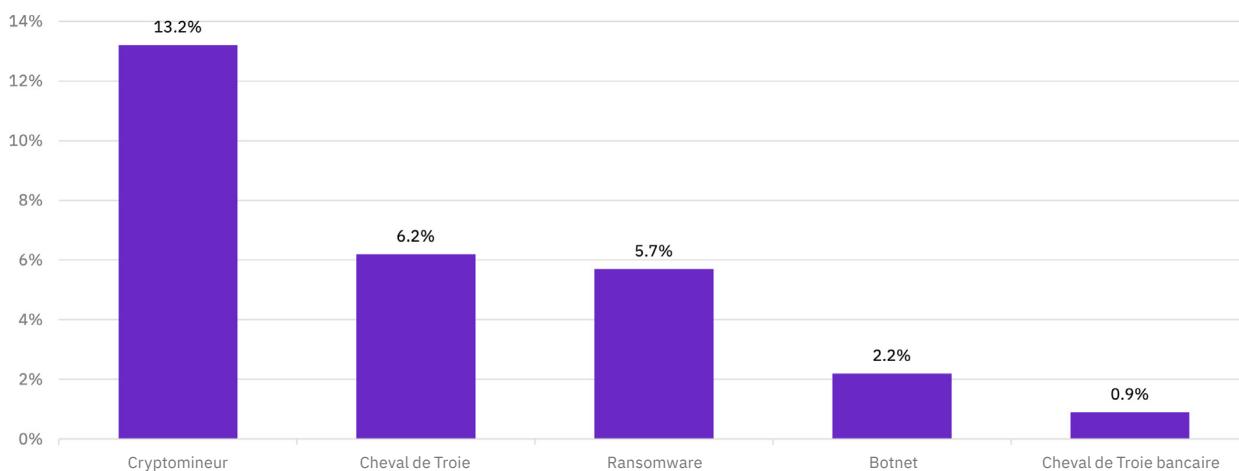
Les chercheurs d'[Intezer](#) — une société spécialisée dans la comparaison des codes des logiciels malveillants qui collabore avec IBM Security — a observé que les attaquants investissaient davantage dans les cryptomineurs et les chevaux de Troie. Il est probable qu'ils cherchent à s'adapter au ciblage d'infrastructures plus modernes telles que le cloud, dans lequel Linux gère déjà 90 % des charges de travail, et dont l'adoption s'est accélérée en raison du COVID-19.

En 2020, les attaquants se sont davantage attachés à développer des cryptomineurs et des ransomware ciblant Linux. Cette tactique s'explique sans doute par le nombre croissant d'entreprises transférant leurs serveurs vers le cloud et par la puissance de traitement extensible fournie par les environnements cloud. Le graphique de la *Figure 11* indique le pourcentage moyen de nouveau code utilisé pour développer différents types de logiciels malveillants ciblant Linux en 2020.

Figure 11

Proportion de nouveau code dans les logiciels malveillants ciblant Linux

Pourcentage moyen de nouveau code utilisé pour développer des logiciels malveillants ciblant Linux, par type de logiciel, 2020 (source : Intezer)

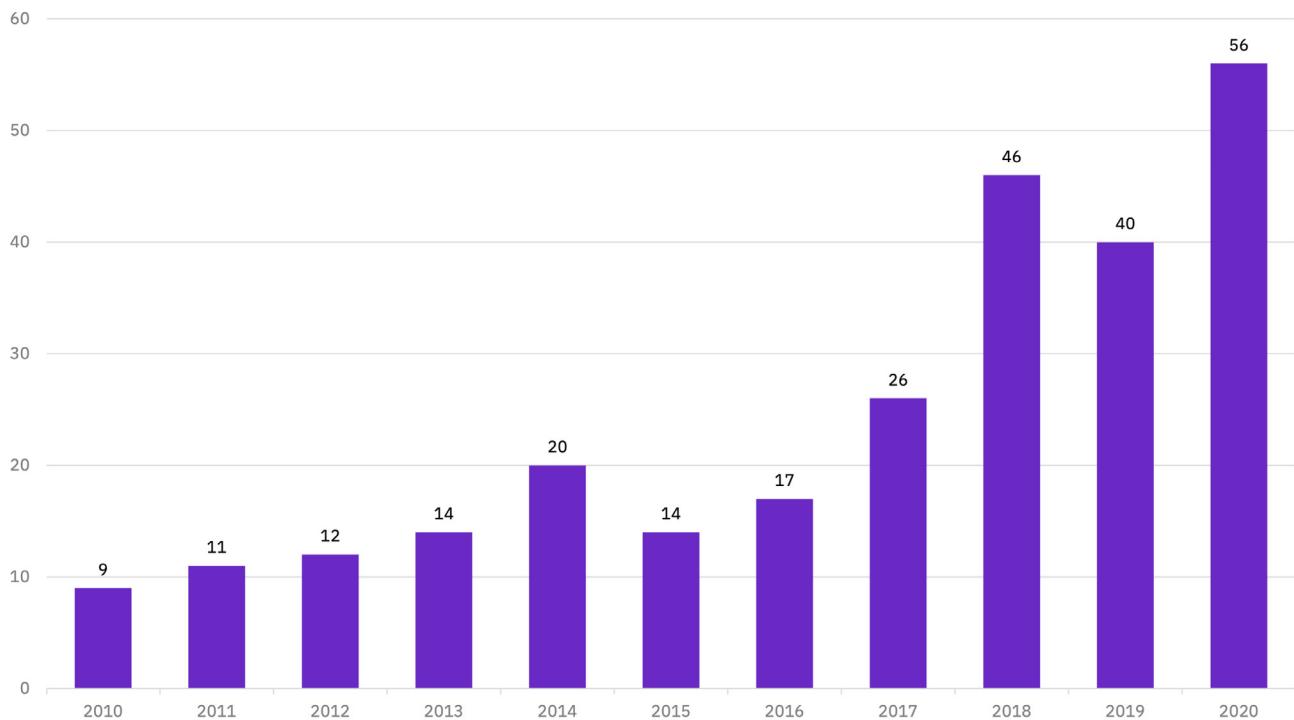


Depuis 2010, Intezer a observé une augmentation du nombre de nouvelles familles de logiciels malveillants ciblant Linux, 2020 ayant enregistré un chiffre record : 56, soit une augmentation de 40 % par rapport à 2019. Il s'agit d'une tendance claire qui met en évidence l'augmentation des familles de logiciels malveillants faisant leur entrée dans l'univers des menaces contre Linux.

Figure 12

Nouvelles familles de logiciels malveillants ciblant Linux, 2010-2020

Nombre de nouvelles familles de logiciels malveillants ciblant Linux par an (source : Intezer)



Les spécialistes X-Force en ingénierie inverse ont également observé une augmentation des logiciels malveillants ciblant Linux en 2020 dans les incidents traités par IBM Security X-Force. Vers le début de 2020, plusieurs cyberattaquants exploitant la faille de traversée de répertoire (CVE-2019-19781) développaient également des logiciels malveillants ciblant les périphériques NetScaler vulnérables, par exemple avec NotRobin. Vers la seconde moitié de 2020, les ingénieurs spécialisés en logiciels malveillants ont relevé plusieurs indices démontrant que les cyberattaquants, qui se concentraient auparavant sur Windows, incluaient désormais dans leur arsenal des logiciels malveillants ciblant Linux.

Lors de missions de X-Force Incident Response, IBM Security X-Force a par exemple observé des variantes Linux d'un ransomware qui ne ciblait auparavant que les systèmes Windows. Il s'agit notamment d'une variante Linux du ransomware Defray911/RansomEXX et d'une variante Linux du ransomware SFile.

Nouveau langage « Go-to »

Tout au long de 2020, les spécialistes X-Force en ingénierie inverse ont observé une utilisation de plus en plus fréquente du langage de programmation Go (abréviation de Golang) dans la création de nouveaux logiciels malveillants. Le langage de programmation Go est un langage open-source similaire au langage C, conçu pour améliorer la productivité de la programmation. Il a été publié en 2012.

Tout au long de 2020, les logiciels malveillants écrits en Go ont augmenté de 500 % de janvier pour atteindre une apogée en juin. Ils ont continué d'être fréquemment utilisés jusqu'à la fin de l'année, ce qui souligne la popularité croissante de ce langage de programmation auprès des cyberattaquants. Par contraste, nous n'avions vu que très peu d'échantillons de logiciels malveillants écrits en Go en 2019. Nous avons observé que Go était fréquemment utilisé en 2020 pour les ransomware. Il semble être populaire auprès des cyberattaquants ciblant les réseaux d'OT, tout en étant utilisé par de nombreux autres agresseurs sur une grande variété de cibles.

Les attaquants écrivent en Go car il est extrêmement facile à déployer dans plusieurs systèmes. Au lieu d'écrire des logiciels malveillants distincts pour Linux, Windows ou OS X, Go permet à l'attaquant d'écrire le logiciel malveillant une seule fois, puis de compiler le même code source pour une grande diversité de plates-formes. Il en résulte des logiciels malveillants pouvant être exécutés sur de nombreux systèmes d'exploitation différents.

Les fichiers binaires Go contribuent également à éviter la détection en créant un seul « package ». Contrairement aux logiciels malveillants écrits dans d'autres langages, ceux qui sont écrits en Go peuvent créer une liaison statique entre toutes leurs bibliothèques à l'intérieur du code. Le logiciel malveillant peut par conséquent fonctionner indépendamment, sans nécessiter d'injecteurs ou de chargement latéral, ce qui lui permet d'échapper plus facilement à la détection par les antivirus. Cependant, la même fonctionnalité génère un fichier binaire très volumineux, ce qui écarte la possibilité pour les logiciels malveillants écrits en Go d'être utilisés comme pièces jointes pour le hameçonnage.

Intezer a également observé que Go était devenu le langage de programmation de prédilection de plusieurs opérateurs de menaces persistantes avancées (APT) pour développer des logiciels malveillants multiplateformes ciblant à la fois les systèmes Windows et Linux :

- **APT28 (ITG05)** : Un groupe de l'État-nation russe. En décembre 2020, ce groupe [a utilisé](#) le COVID-19 commeurre de hameçonnage pour fournir la version Go du malware Zebrocy.
- **APT29 (ITG11)** : Un autre groupe de l'État-nation russe. Intezer Analyze a pu identifier une [variante Linux](#) de WellMail, avec lequel il a du code en commun, comme l'indiquent les indicateurs de compromission selon un [rapport britannique](#).
- **Carbanak (ITG14 ou FIN7)** : Un grand groupe de cybercriminels. Un échantillon Linux a du code commun avec un échantillon de Carbanak Windows de 2019, ce qui a permis à Intezer de l'identifier.

Emotet fait son retour

Les pièges de spam et de hameçonnage d'IBM ont suivi de près Emotet en 2020 et ont détecté une accalmie prononcée de son activité au printemps et au début de l'été. Le malware est cependant réapparu en juillet 2020 et a été très actif en septembre et octobre, en particulier au Japon. Les opérateurs d'Emotet ont probablement fait une pause pour améliorer ses capacités à échapper à la détection, comme le laissent conclure de nouvelles capacités anti-analyse observées par X-Force.

Figure 13

Tendance du spam Emotet, période de juin à décembre 2020

Volume de spam Emotet quotidien en pourcentage du spam quotidien total, période de juin à décembre 2020 (source : IBM Security X-Force)



Emotet est largement diffusé via des campagnes de spam. Les pièges à spam d'IBM [ont observé](#) que tous les logiciels malveillants Emotet s'étaient propagés en 2020 via des pièces jointes contenant des macros malveillantes d'Office Word. Emotet a également semblé surfer sur la vague d'autres campagnes de spam, notamment les campagnes habituelles de spam ayant pour thème le casino ou la sextorsion, en faisant suivre ces e-mails, puis en y joignant une charge malveillante. Emotet peut également lire des conversations par e-mail légitimes et y répondre en envoyant des pièces jointes infectées, sous un prétexte de légitimité. L'analyse d'IBM a également révélé que la majorité des spams d'Emotet sont envoyés les jours ouvrables.

Les analystes du renseignement X-Force ont découvert de nouvelles fonctionnalités dans les échantillons d'Emotet, telles que des capacités anti-analyse. Ces mises à jour indiquent que les cyberattaquants continuent d'investir dans Emotet et que cette famille de logiciels malveillants reste sans doute une menace pour les entreprises du monde entier.

Cybercriminalité financière

Dans l'arène de la cybercriminalité, les logiciels malveillants financiers continuent de constituer une menace pour les organismes financiers et d'autres entreprises, alors que les cyberattaquants continuent d'innover et que de nouvelles menaces émergent. En 2020, IBM Trusteer a observé que les gangs de cybercriminels utilisaient un processus hautement automatisé pour vider les comptes bancaires via la fraude bancaire mobile, et que les attaques par superposition à distance étaient devenues encore plus courantes cette même année, en particulier en Europe.

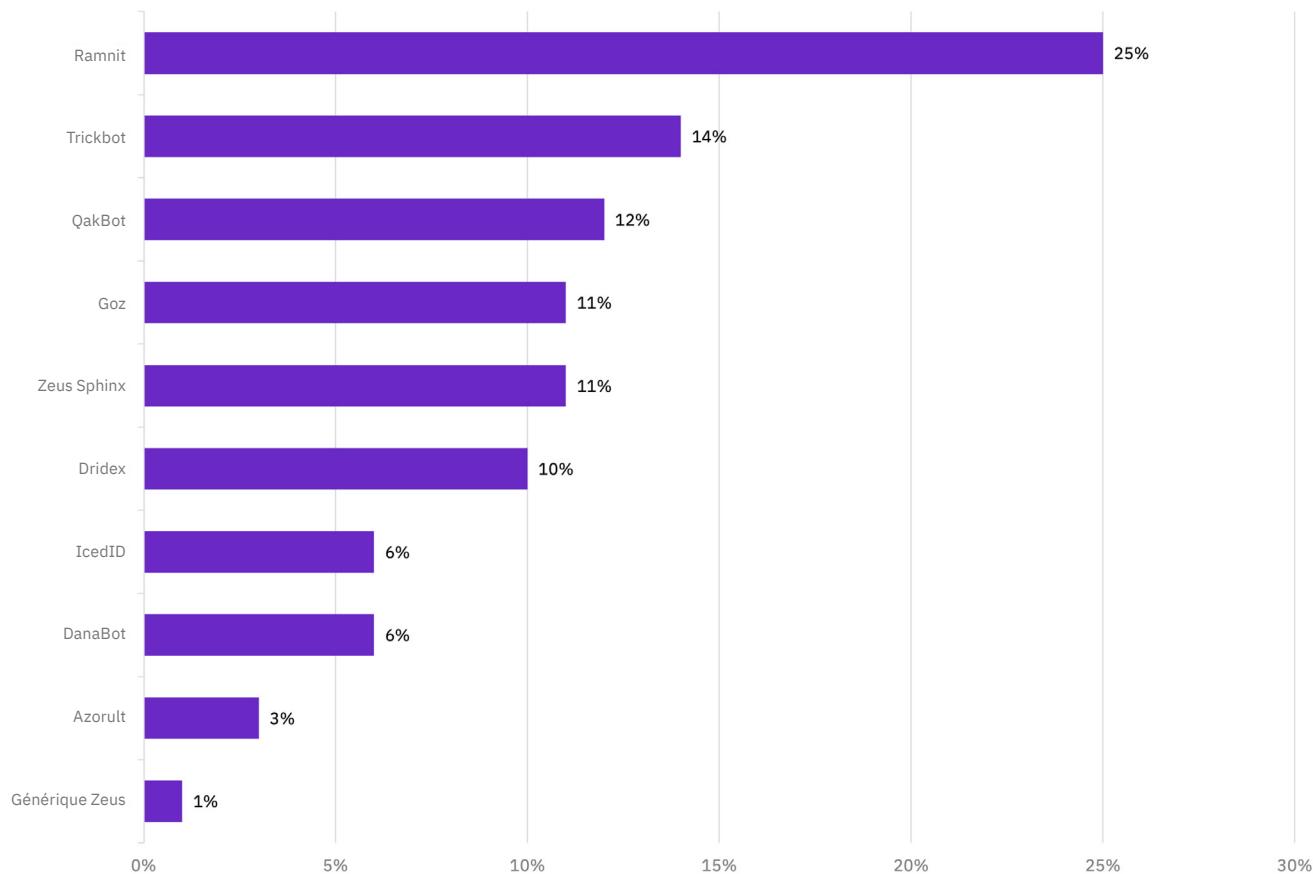
Les meilleurs chevaux de Troie bancaires

Les principales familles de logiciels malveillants financiers de 2020 comptaient parmi leurs rangs tous les suspects habituels, sans surprises ni nouveaux venus. Cela ne signifie pas que les gangs de cybercriminalité financière existants n'ont pas évolué ni créé de nouveaux moyens d'attaque et de monétisation des logiciels criminels au cours de l'année.

Figure 14

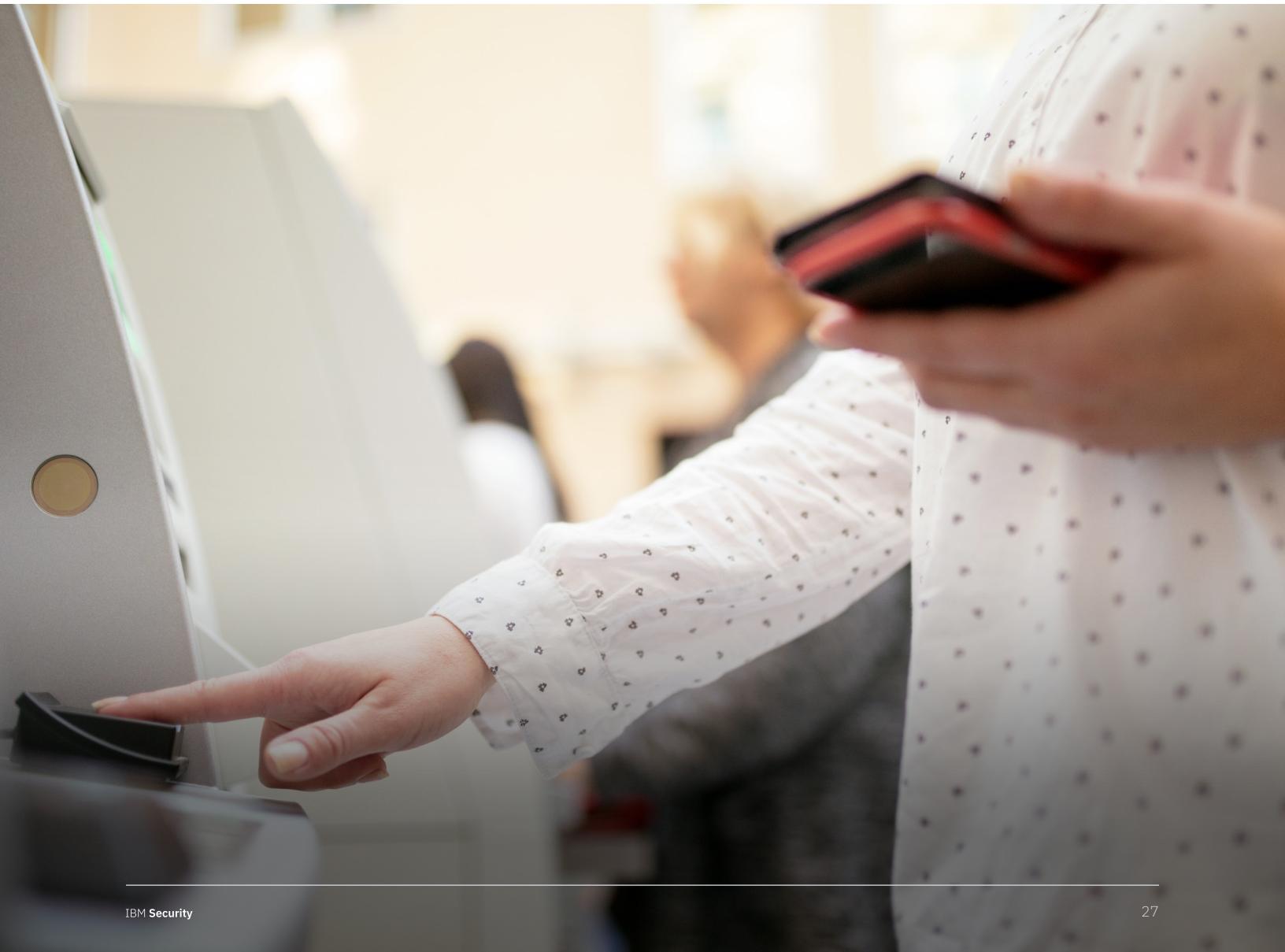
Les 10 principales familles de chevaux de Troie bancaires

Répartition des principaux chevaux de Troie bancaires en 2020, exprimée en pourcentage des 10 premiers (source : IBM Trusteer)



Points clés des chevaux de Troie bancaires

1. **Ramnit** : Second l'année dernière, il s'est hissé à la première place. Ce logiciel malveillant continue d'être exploité par un gang cybercriminel fermé, diversifiant ses modèles de monétisation et s'adaptant aux différentes zones géographiques ciblées. Les attaques continuent de privilégier les comptes de particuliers et de professionnels.
2. **Trickbot** : Souvent surpris à déployer le ransomware Ryuk, ce logiciel malveillant a rétrogradé à la deuxième place, probablement à la suite de son démantèlement éphémère en octobre 2020. Il est originaire d'Europe de l'Est et cible les entreprises, les banques d'affaires et les grandes entreprises.
3. **Qakbot** : Occupant la troisième place, ce logiciel malveillant est propagé dans les réseaux d'entreprise par le botnet Emotet. En 2020, il a organisé des attaques avec le ransomware ProLock dans le cadre d'une stratégie visant à monétiser davantage ses implantations. Également originaire d'Europe de l'Est, il cible les entreprises, les banques d'affaires et les grandes entreprises.



Tendances géographiques et sectorielles

Chaque zone géographique et chaque secteur d'activité sont confrontés à un contexte d'attaques unique, car l'activité des attaques dépend de cyberattaquants, de motivations, d'actifs et d'événements géopolitiques différents. Cette section présente une répartition des tendances générales des attaques décrites dans ce rapport, et explique plus en détail comment ces tendances et d'autres facteurs ont affecté chaque géographie et chaque secteur.

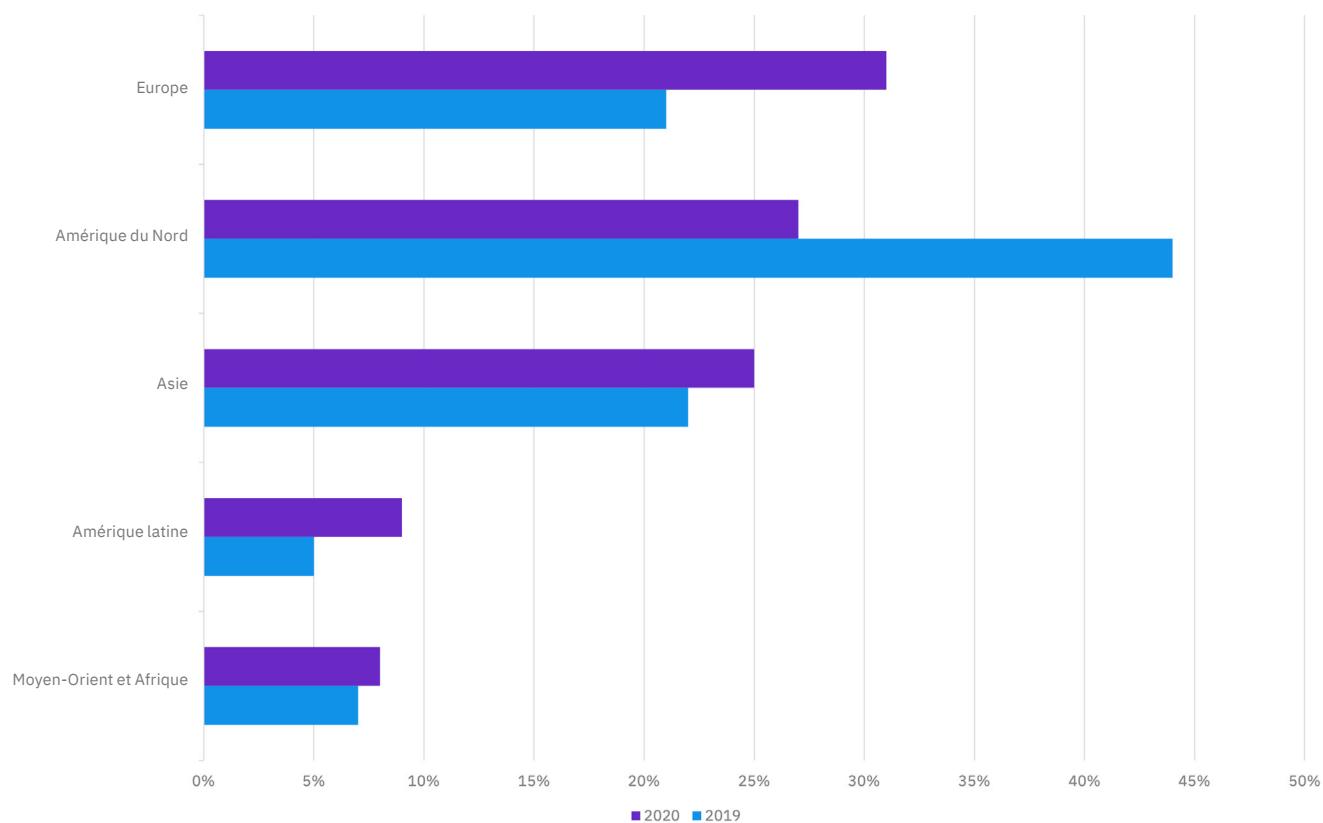
Impact géographique

L'Europe, l'Amérique du Nord et l'Asie ont subi la majeure partie des attaques en 2020, attirant l'activité des cybercriminels sans doute en raison du pourcentage élevé de la richesse mondiale qui circule sur ces continents, soit plus de 89 % du produit intérieur brut (PIB) mondial. Dans ces trois régions du monde, ce sont les attaques contre les entreprises européennes qui ont le plus augmenté, avec en tête les attaques par ransomware, les attaques internes et les attaques par accès aux serveurs.

Figure 15

Répartition géographique des attaques, comparatif entre 2020 et 2019

Répartition géographique du total des attaques dans les données de X-Force de réponse aux incidents, comparatif entre 2020 et 2019 (source : IBM Security X-Force)



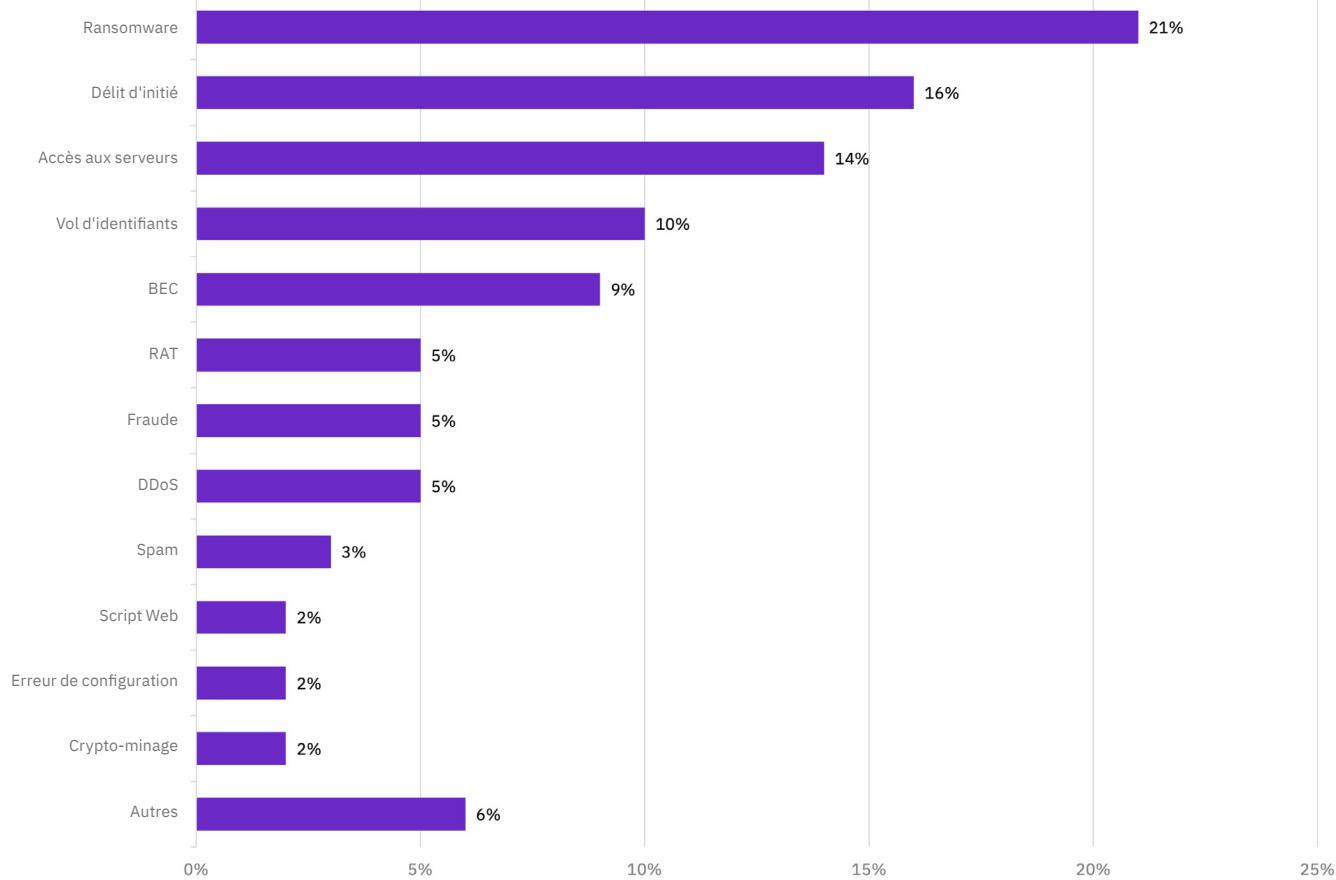
Europe

- Volume des attaques :** IBM Security X-Force a observé que 31 % des attaques en 2020 se sont produites en Europe, soit une hausse significative par rapport aux 21 % en 2019, propulsant l'Europe au rang de région la plus attaquée au monde en 2020.
- Types d'attaques :** Les attaques par ransomware ont été le principal type d'attaque en Europe en 2020, représentant 21 % des attaques, soit un volume important, mais qui reste cependant inférieur au taux des attaques par ransomware lancées contre l'Amérique du Nord. L'Europe a de loin subi le plus d'attaques internes en 2020, avec deux fois plus d'attaques de ce type que l'Amérique du Nord et l'Asie réunies. L'Europe a également connu un volume élevé d'attaques d'accès aux serveurs, soit 14 % de toutes les attaques sur le continent en 2020. Le vol d'identifiants, la compromission des e-mails professionnels (BEC), les chevaux de Troie d'accès à distance (RAT), la fraude et les attaques DDoS ont également affecté les entreprises européennes en 2020, dans une moindre mesure. L'Europe a subi 33 % de toutes les attaques exploitant la vulnérabilité CVE-2019-19781 dans le monde en 2020, soit plus que toute autre zone géographique.
- Pays attaqués :** Le Royaume-Uni, la Suisse, la France et l'Italie ont été les pays les plus attaqués d'Europe en 2020.

Le schéma 16

Types d'attaques en Europe

Répartition du total des attaques contre l'Europe par type d'attaque, à partir des données X-Force de réponse aux incidents en 2020 (source : IBM Security X-Force)



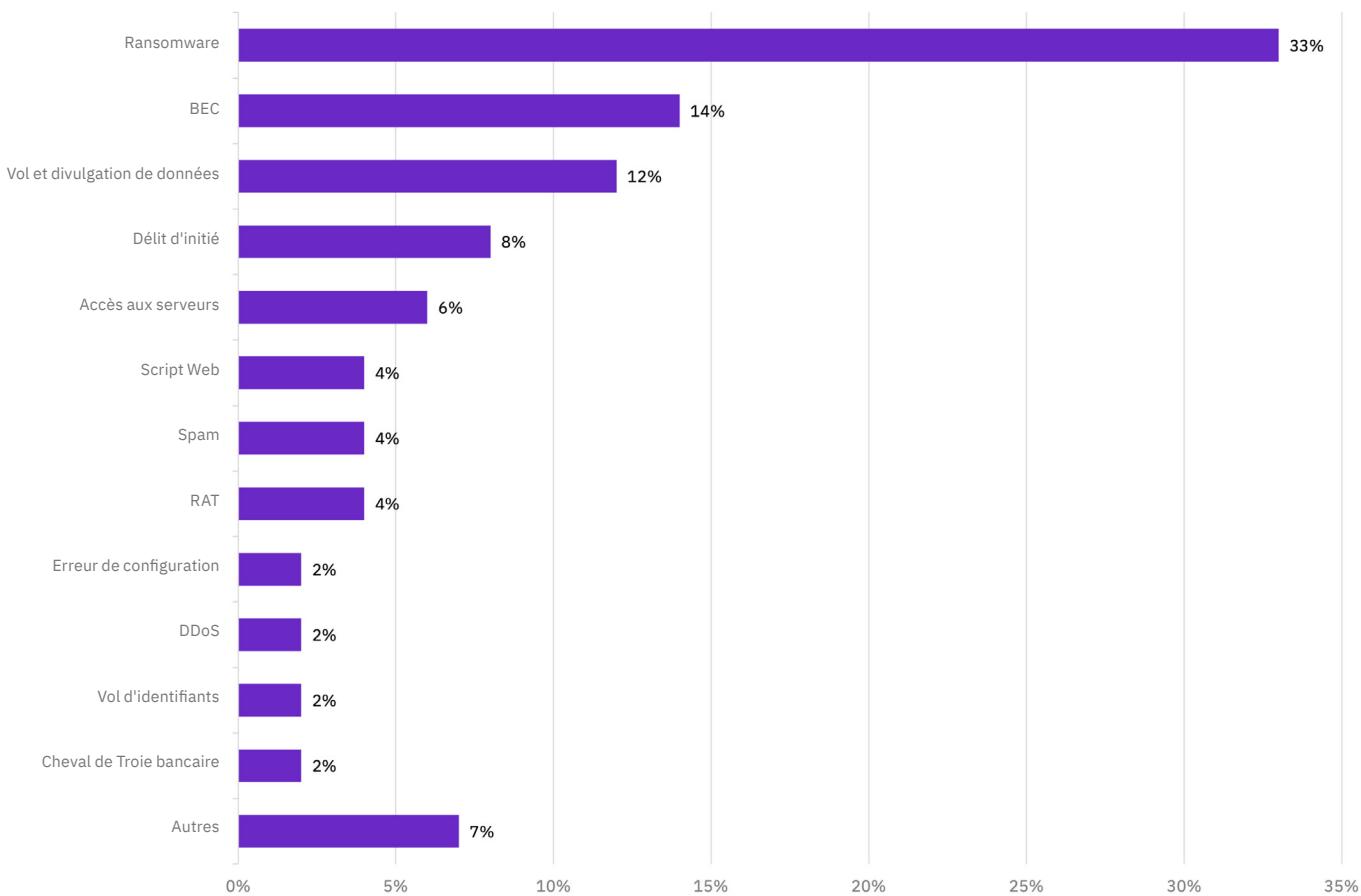
Amérique du Nord

- Volume des attaques :** L'Amérique du Nord a subi 27 % de toutes les attaques résolues par X-Force en 2020, ce qui la fait chuter au deuxième rang des régions géographiques les plus attaquées dans le monde. Cette baisse brutale contraste fortement avec 2019, année où l'Amérique du nord avait été l'objet de 44 % de toutes les attaques. Une augmentation du taux des attaques en Europe et en Asie est la principale raison de ce changement.
- Types d'attaques :** L'Amérique du Nord a connu plus d'attaques par ransomware que toute autre région du monde en chiffres bruts, soit 33 % de toutes les attaques menées contre elle en 2020. Les attaques de type BEC, le vol et les divulgations de données, ainsi que les RAT ont aussi largement frappé les entreprises nord-américaines tout au long de 2020. L'Amérique du Nord a également connu 29 % des attaques qui ont exploité la vulnérabilité CVE-2019-19781 en 2020, soit le deuxième taux le plus élevé après l'Europe.
- Pays attaqués :** Les États-Unis ont été le pays d'Amérique du nord le plus attaqué en 2020, suivis du Canada.

Figure 17

Types d'attaques en Amérique du Nord

Répartition du total des attaques contre l'Amérique du Nord par type d'attaque, à partir des données X-Force de réponse aux incidents en 2020 (source : IBM Security X-Force)



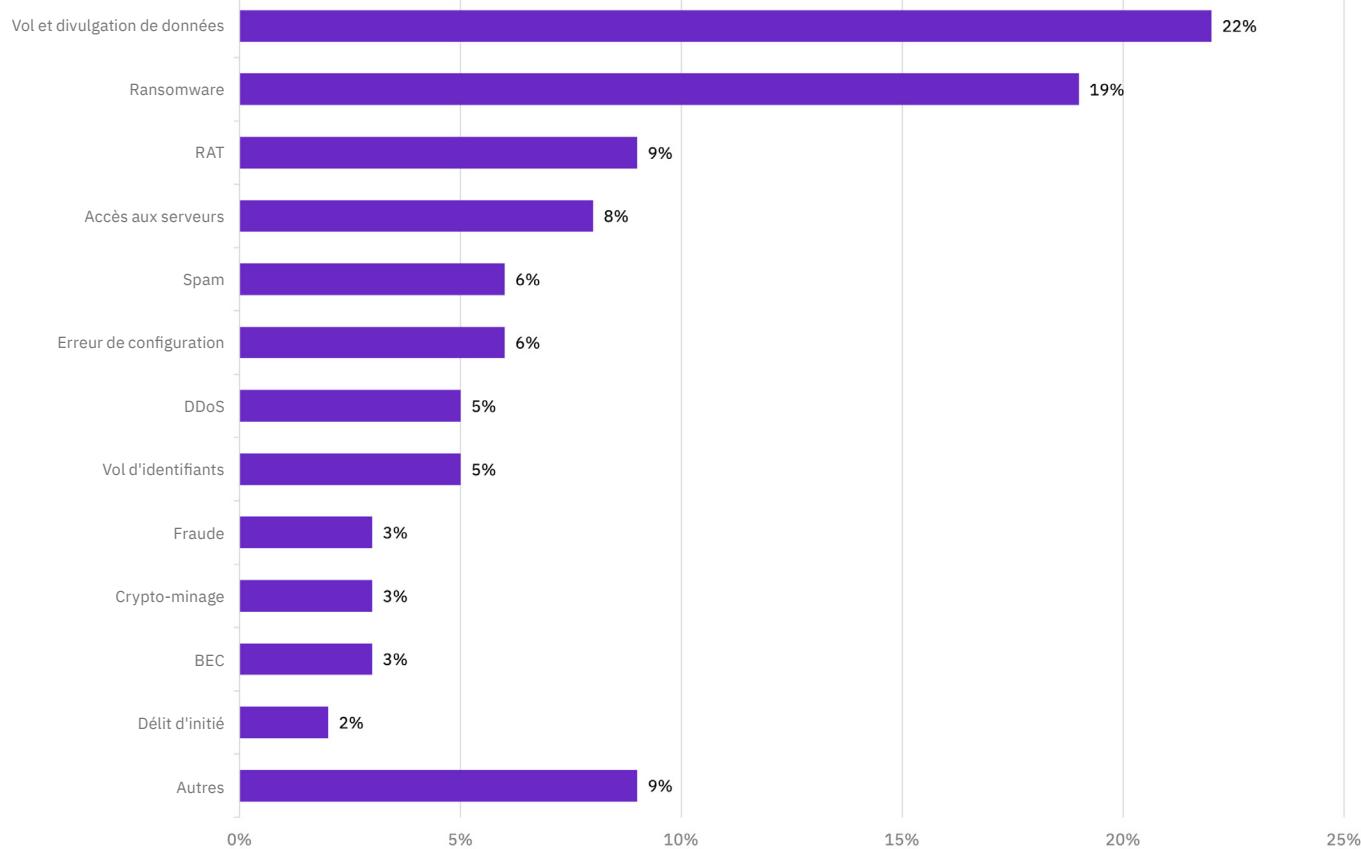
Asie Pacifique

- Volume des attaques :** La région Asie-Pacifique a représenté 25 % de toutes les attaques observées par IBM Security X-Force en 2020, contre 22 % en 2019.
- Types d'attaques :** Le vol de données a été le type d'attaque le plus courant en Asie en 2020, principalement en raison d'une rafale d'attaques de vol de données dues à Emotet à l'automne 2020. Les vols de données ont représenté 22 % de toutes les attaques dans la région, soit plus encore que les ransomware. Les attaques par ransomware ont représenté 19 % de toutes les attaques en Asie en 2020, y compris par des souches telles que PJX et Locky. L'Asie-Pacifique a connu plus d'attaques impliquant des RAT que toute autre région du monde, les chevaux de Troie d'accès à distance représentant 9 % de toutes les attaques dans la région en 2020. L'Asie a également subi 21 % de toutes les attaques exploitant la vulnérabilité CVE-2019-19781 en 2020. Les attaques de type BEC (compromission des e-mails professionnels) ont été moins courantes en Asie que d'autres en 2020, sans doute en raison de la mise en œuvre de l'authentification multifactorielle. Le secteur manufacturier ainsi que celui de la finance et des assurances ont été les deux principaux secteurs visés dans la zone Asie-Pacifique.
- Pays attaqués :** Le Japon a été le pays le plus attaqué d'Asie en 2020, suivi de loin par l'Inde puis de l'Australie.

Figure 18

Types d'attaques en Asie

Répartition du total des attaques contre l'Asie par type d'attaque, à partir des données X-Force de réponse aux incidents en 2020 (source : IBM Security X-Force)



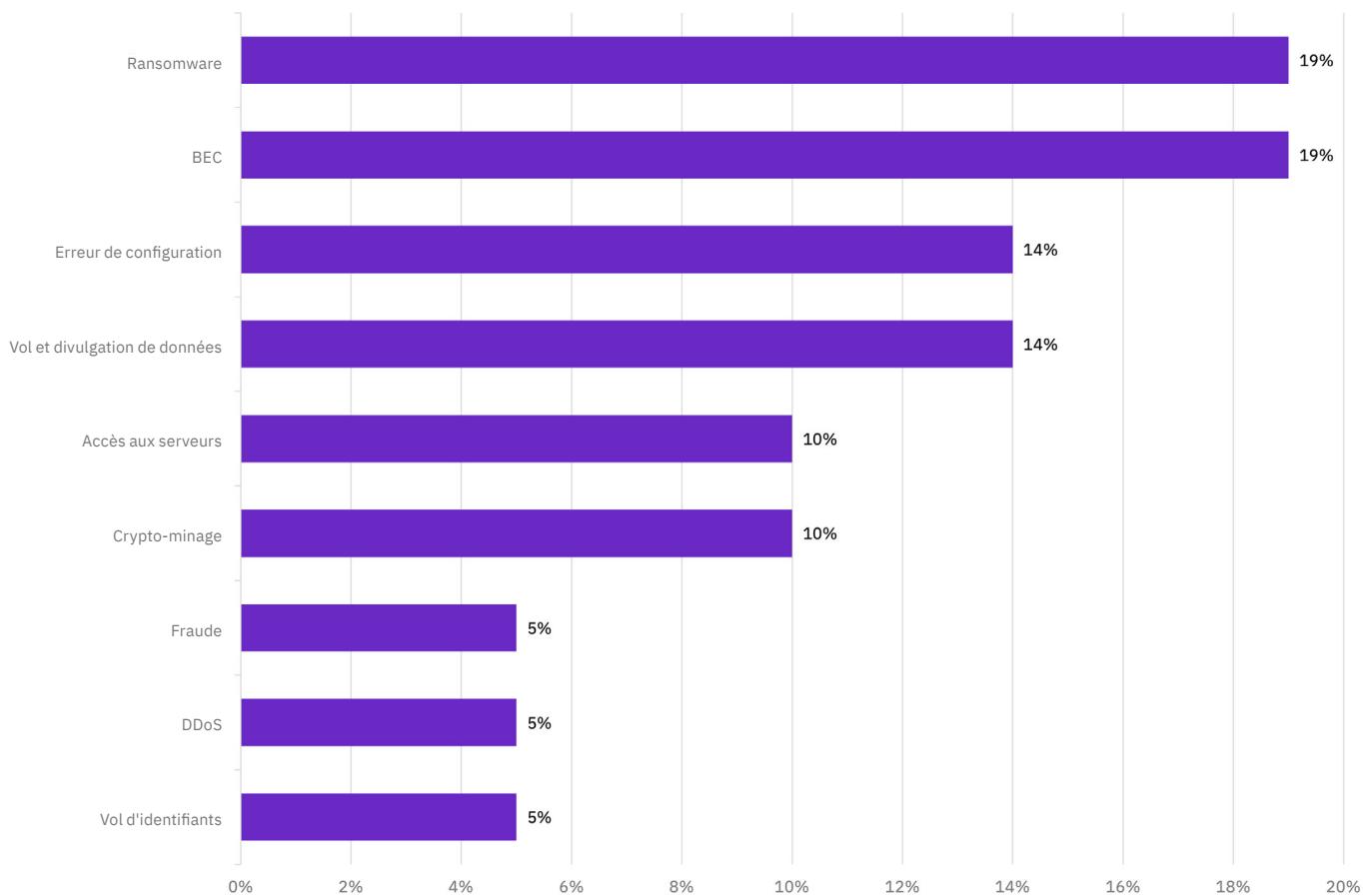
Amérique centrale et du sud

- Volume des attaques :** Les entreprises d'Amérique centrale et d'Amérique du Sud ont subi 9 % du total des attaques observées par IBM Security X-Force en 2020, contre 5 % en 2019.
- Types d'attaques :** Les attaques de type BEC (compromission des e-mails professionnels) sont à égalité avec les attaques par ransomware en Amérique centrale et en Amérique du Sud, toutes deux représentant 19 % des attaques dans la région, talonnées de près par des erreurs de configuration et par le vol et la divulgation de données. On remarquera que l'Amérique centrale et l'Amérique du Sud ont connu plus d'incidents dus à des erreurs de configuration que l'Amérique du Nord ou l'Europe. Les attaques par accès aux serveurs, en revanche, n'ont pas affecté l'Amérique centrale et du Sud dans la même mesure que d'autres zones géographiques en 2020.
- Pays attaqués :** Le Brésil a été le pays le plus attaqué d'Amérique centrale et du Sud en 2020.

Figure 19

Types d'attaques en Amérique centrale et en Amérique du Sud

Répartition du total des attaques contre l'Amérique centrale et du sud par type d'attaque, à partir des données X-Force de réponse aux incidents en 2020 (source : IBM Security X-Force)



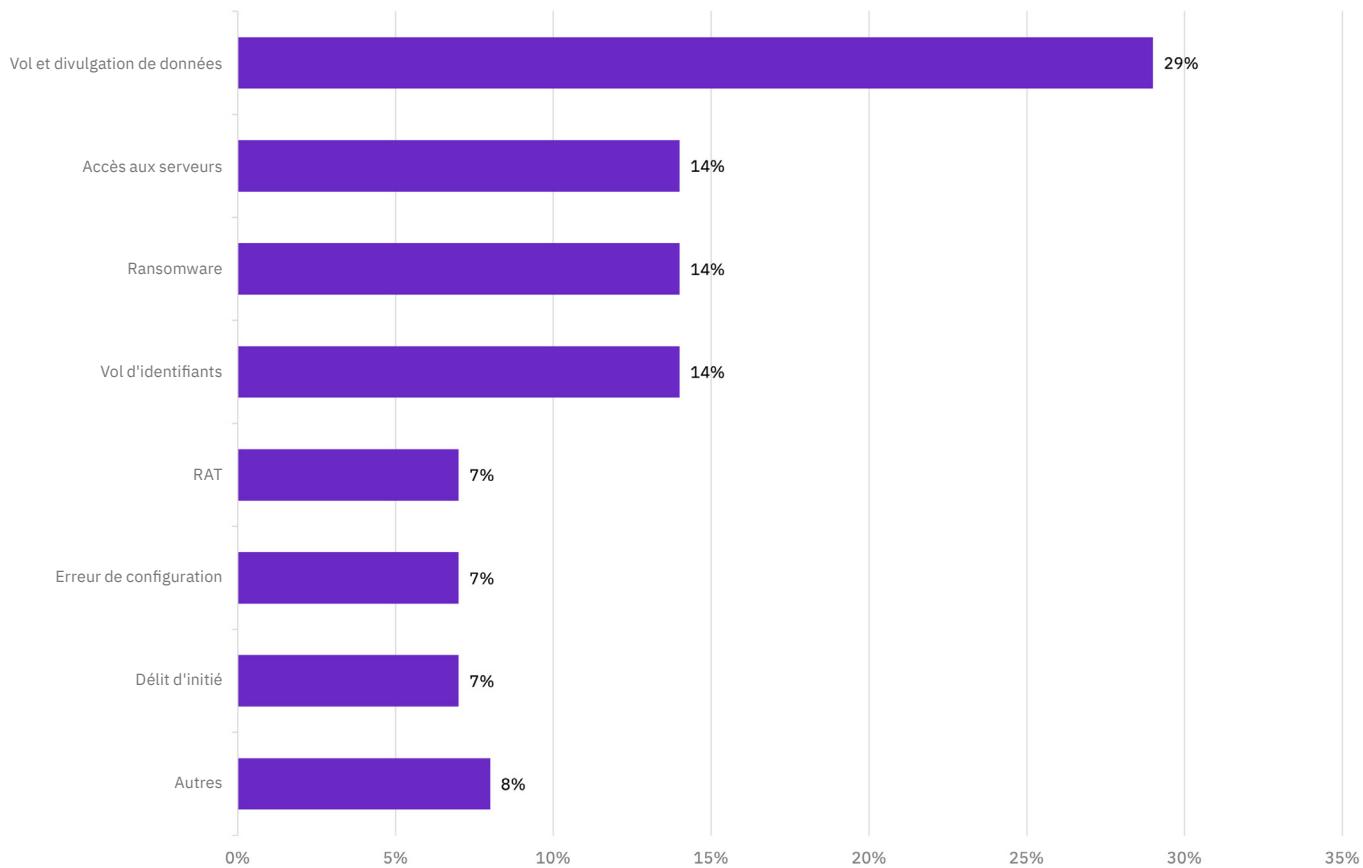
Moyen-Orient et Afrique

- Volume des attaques :** Les entreprises du Moyen-Orient et d'Afrique ont subi 8 % des attaques selon les données X-Force en 2020, en légère hausse par rapport aux 7 % de l'année précédente.
- Types d'attaques :** Le vol et la divulgation de données ont de loin été le type d'attaque le plus courant au Moyen-Orient et en Afrique en 2020, soit 29 %, un chiffre assez imposant. Les attaques par accès aux serveurs, par ransomware et par vol d'identifiants se sont classées à égalité à la deuxième place, avec 14 % chacune. Les RAT, les erreurs de configuration et les menaces internes ont également affecté les entreprises au Moyen-Orient et en Afrique en 2020.
- Pays attaqués :** L'Arabie saoudite, les Émirats arabes unis, l'Afrique du Sud et la Turquie ont été les principaux pays attaqués au Moyen-Orient et en Afrique en 2020.

Figure 20

Types d'attaques au Moyen-Orient et en Afrique

Répartition du total des attaques contre le Moyen-Orient et l'Afrique par type d'attaque, à partir des données X-Force de réponse aux incidents en 2020 (source : IBM Security X-Force)



Secteurs d'activité les plus attaqués

Chaque année, X-Force identifie les 10 secteurs d'activité les plus attaqués et les classe en fonction du pourcentage des attaques. Pour la cinquième année consécutive, le secteur de la finance et des assurances a été le plus attaqué, soulignant l'intérêt considérable qu'il suscite chez les cyberattaquants.

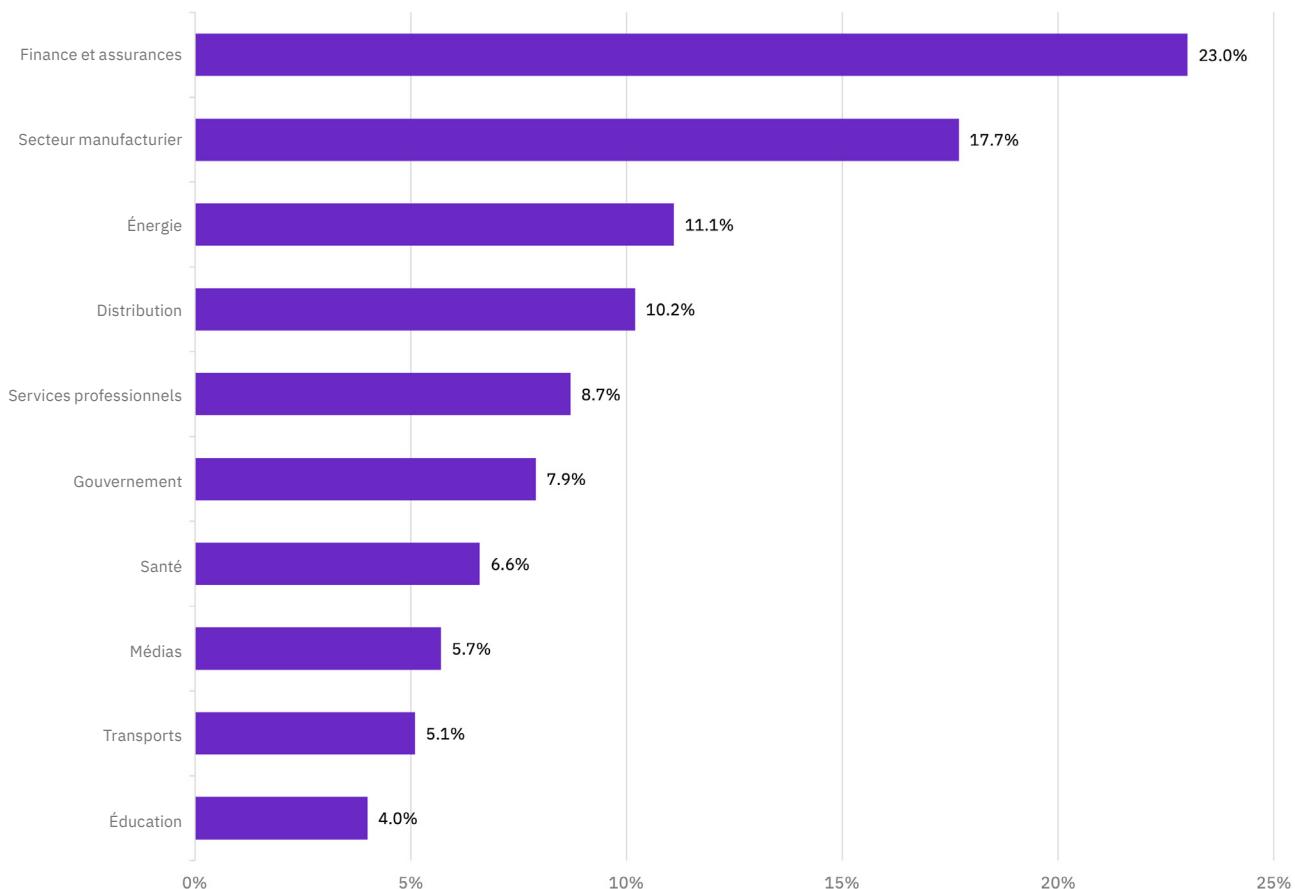
Plusieurs autres secteurs d'activité ont connu des changements importants depuis les classements de l'année dernière (voir *la Figure 21* des classements comparatifs des 10 principaux secteurs d'activités en 2020 par rapport à 2019). Le secteur manufacturier, classé au huitième rang des secteurs les plus attaqués dans le rapport de 2019, a bondi à la deuxième place en 2020. La raison est peut-être l'intérêt pour les cyberattaquants de cibler des infrastructures liées à l'OT (technologie d'exploitation). De même, le secteur de l'énergie a bondi de la neuvième place en 2019 à la troisième place en 2020, confirmant l'intérêt des attaquants pour les entreprises en lien avec l'OT en 2020. Les soins de santé sont passés de la dernière place en 2019 à la septième place en 2020, probablement en raison d'attaques en lien avec le COVID et à un feu nourri d'attaques par ransomware contre les hôpitaux. Les attaques contre le secteur des transports ont continué de diminuer en 2020, le faisant tomber à la neuvième place, alors qu'il occupait le troisième rang en 2019. La raison en est peut-être une baisse de l'utilisation des transports pendant la pandémie.

Secteur	Classement 2020	Classement 2019	Changement
(Source: IBM Security X-Force)			
Finance et assurances	1	1	-
Secteur manufacturier	2	8	6
Énergie	3	9	6
Distribution	4	2	-2
Services professionnels	5	5	-
Gouvernement	6	6	-
Santé	7	10	3
Médias	8	4	-4
Transports	9	3	-6
Éducation	10	7	-3
-3		1	

Figure 22

Répartition des attaques dans les 10 principaux secteurs d'activité visés

Principaux secteurs d'activité attaqués en 2020, exprimé en pourcentage des attaques contre les 10 secteurs les plus visés (source : IBM Security X-Force)



Le graphique de la *Figure 22* montre le pourcentage d'attaques contre chacun des 10 principaux secteurs d'activité visés, 23 % de ces attaques ciblant les secteur de la finance et des assurances. Le secteur manufacturier a été la cible de 17,7 % des attaques contre les 10 principaux secteurs, suivi du secteur de l'énergie (11,1 %) et de la distribution (10,2 %), tandis que les secteurs restants du top 10 ont été visés par moins de 10 % des attaques chacun.

Figure 23**Types d'attaques par secteurs d'activité**

Répartition en pourcentage des attaques contre les secteurs d'activité par type d'attaque, sur la base des données X-Force de réponse aux incidents en 2020 (source : IBM Security X-Force)



Le graphique de la *Figure 23* décrit les principales attaques contre chaque secteur sur la base des données X-Force de réponse aux incidents. Ces données et les pourcentages calculés sont décrits plus en détail dans chacune des sections suivantes.

Finance et assurances



28 %

des attaques contre le secteur de la finance et des assurances en 2020 étaient des attaques par accès aux serveurs.

10 %

des attaques contre le secteur financier ont été des attaques par ransomware.

Depuis 2016, le secteur de la finance et des assurances est classé comme le secteur le plus attaqué, une position qu'il a conservée en 2020. Les institutions financières ont subi 23 % de toutes les attaques que nous avons analysées en 2020, contre 17 % en 2019.

Parmi tous les secteurs, la finance et les assurances ont subi le plus grand nombre d'attaques par accès aux serveurs, principalement liées à la vulnérabilité Citrix CVE-2019-19781, par rapport aux autres secteurs. Les attaques par accès aux serveurs ont représenté 28 % de toutes les attaques contre la finance et des assurances. Ce secteur s'est classé ex-æquo avec le secteur manufacturier en termes de pourcentage le plus élevé d'attaques exploitant la vulnérabilité CVE-2019-19781, soit 22 %.

La nature fortement réglementée du secteur de la finance et des assurances et l'approche proactive des organismes financiers en matière d'identification et de traitement des attaques par accès aux serveurs ont probablement contribué au pourcentage élevé d'attaques contre ce secteur.

En outre, la finance et les assurances ont subi moins d'attaques par ransomware par rapport à d'autres secteurs, tels que le secteur manufacturier, les services professionnels et le secteur gouvernemental. Seulement 10 % des attaques contre ce secteur en 2020 ont été le fait de ransomware. Les attaquants par ransomware ont probablement jugé que les entreprises hors secteur financier étaient plus rentables pour ce type d'attaque, sans doute en raison des contrôles de sécurité rigoureux mis en place dans le secteur de la finance et des assurances, ou parce qu'ils estiment que les industries telles que le secteur manufacturier et les services professionnels ont une tolérance plus faible aux temps d'indisponibilité causés par les ransomware.

Secteur manufacturier



Le secteur manufacturier s'est classé au deuxième rang des secteurs les plus attaqués en 2020, alors qu'il était huitième en 2019. Il a subi 17,7 % de toutes les attaques menées contre les dix principaux secteurs, soit plus du double des 8,1 % d'attaques qu'il avait essuyées l'année dernière. L'attention renouvelée des cyberattaquants envers le secteur manufacturier, qui s'était également classé deuxième en 2015 et troisième en 2017, souligne son intérêt en tant que cible, en particulier pour les attaques par ransomware, et de type BEC et RAT (chevaux de Troie d'accès à distance).

21 % des attaques contre le secteur manufacturier en 2020 sont imputables à des ransomware, un pourcentage important qui indique que les cyberattaquants le considèrent comme un secteur rentable pour les attaques par ransomware. En chiffres bruts, le secteur manufacturier a subi plus d'attaques par ransomware que tout autre secteur. La faible tolérance de ce secteur aux temps d'indisponibilité - chaque heure d'arrêt se chiffrant souvent des millions de dollars de pertes chacune - est probablement un facteur qui justifie sa rentabilité élevée aux yeux des cyberattaquants.

En plus des ransomware, les attaques de type BEC (compromission des emails professionnels) ont représenté 17 % des attaques contre le secteur manufacturier en 2020. En chiffres bruts, c'est un nombre quatre fois supérieur aux attaques BEC dans tout autre secteur. Les entreprises du secteur manufacturier ont souvent besoin de se procurer de nombreux composants auprès de fournisseurs différents. Pour les cyberattaquants, ce sont autant d'occasions de s'infiltrer dans les conversations par email et de détourner les fonds destinés au paiement des pièces et matériaux de fabrication. De nombreuses attaques contre le secteur manufacturier semblent utiliser l'ingénierie sociale pour capter les versements, plutôt que de cibler la technologie d'exploitation (OT).

Le secteur manufacturier a également subi 22 % de toutes les attaques exploitant la vulnérabilité CVE-2019-19781 en 2020, se classant premier ex-æquo avec le secteur de la finance et des assurances.

21 %

des attaques contre le secteur manufacturier étaient des attaques par ransomware.

4x

plus d'attaques BEC dans le secteur manufacturier que dans tout autre secteur.

Énergie



35 %

des attaques contre le secteur de l'énergie étaient des tentatives de vol et de divulgation de données.

Encaissant 11,1 % des attaques contre les 10 principaux secteurs d'activité en 2020, le secteur de l'énergie s'est classé au troisième rang des secteurs les plus attaqués, alors qu'il était neuvième l'année précédente. Les attaques par accès aux serveurs, en particulier celles qui exploitent la vulnérabilité CVE-2019-19781, ont frappé durement le secteur en 2020. Il arrive à la quatrième place après le secteur des soins de santé en termes du nombre d'attaques de ce type.

Le vol et la divulgation de données ont été le principal type d'attaque dans ce secteur, représentant 35 % de toutes les attaques subies. Ce chiffre confirme la menace liée au vol d'informations et au hameçonnage. Un grand nombre de ces attaques visaient en particulier des sociétés pétrolières et gazières.

Les attaques de type BEC, le crypto-minage, les ransomware, les chevaux de Troie d'accès à distance (RAT) et les attaques par accès aux serveurs ont également affecté le secteur de l'énergie en 2020, mais sans excès par rapport à d'autres secteurs. En fait, les attaques par ransomware contre le secteur n'ont représenté que 6 % de toutes les attaques qu'il a subies, ce qui est de très loin inférieur aux taux constatés dans la plupart des autres secteurs verticaux les plus attaqués.

Distribution



36 %

des attaques contre la distribution étaient des vols d'identifiants.

18 %

des attaques contre le secteur de la distribution ont été des attaques par ransomware.

Le secteur de la distribution s'est classé au quatrième rang des secteurs les plus attaqués en 2020, perdant sa deuxième place de l'année dernière. Il a subi 10,2 % de toutes les attaques contre les 10 principaux secteurs visés, contre 16 % l'année dernière. En tant que plaque tournante de paiements par carte de crédit et d'autres transactions financières, la distribution est depuis longtemps une cible de choix pour les cyberattaquants.

La distribution a connu majoritairement des vol d'identifiants, soit 36 % des attaques qu'elle a subies en 2020. En chiffres bruts, ce type d'attaque est supérieur à celui constaté dans tous les autres secteurs. Ce secteur a également souffert d'attaques par ransomware en 2020, qui représentent 18 % du total des attaques à son encontre. Presque toutes ces attaques par ransomware étaient imputables à Sodinokibi, selon les données X-Force de réponse aux incidents.

Dans une moindre mesure, les attaques DDoS, la fraude, les erreurs de configuration, les attaques de type RAT et les attaques par accès aux serveurs ont également affecté la distribution. Ceci indique que les cyberattaquants utilisent toute une gamme de types d'attaques pour infiltrer ce secteur à des fins de gains financiers.

Services professionnels



35 %

des attaques contre les services professionnels en 2020 ont été des attaques par ransomware, soit un pourcentage plus élevé que dans tout autre secteur.

13%

des attaques contre les services professionnels ont été le vol de données et 13 % ont été des attaques par accès aux serveurs.

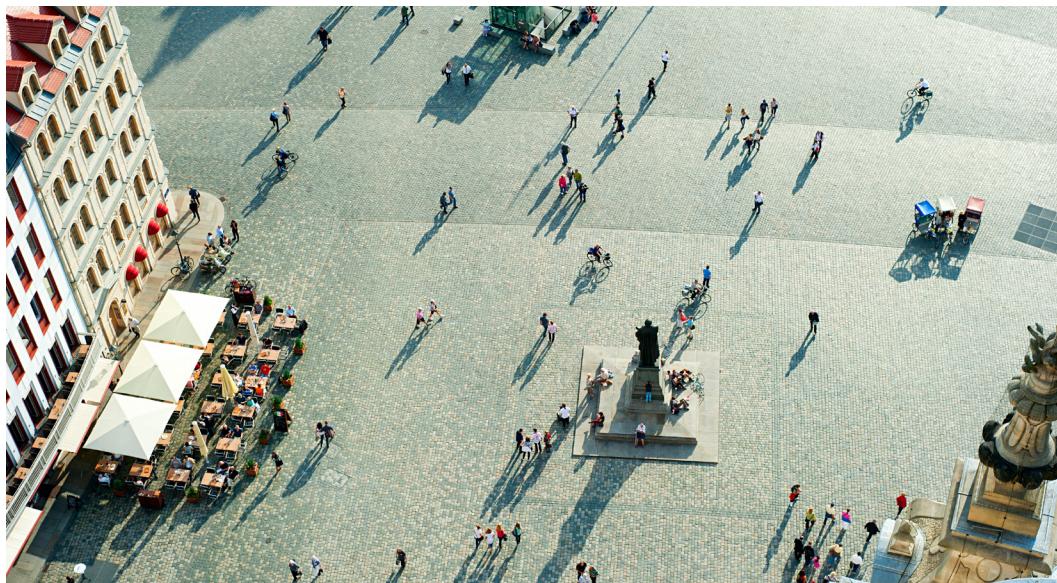
Les services professionnels se sont classés au cinquième rang des secteurs le plus attaqués en 2020 et ont subi 8,7 % de toutes les attaques contre les dix principaux secteurs, conservant le même rang qu'en 2019, où ils avaient encaissé 10 % de toutes les attaques. Les services professionnels sont particulièrement attrayants pour les attaquants parce qu'ils donnent accès à tout un vivier de nouvelles victimes.

Les ransomware ont représenté 35 % des incidents dans les entreprises de services professionnels en 2020, soit le pourcentage le plus élevé de tous les secteurs. En termes de nombre brut d'attaques par ransomware, les services professionnels sont arrivés en deuxième position, précédés seulement par le secteur manufacturier. Certains attaquants par ransomware de 2020, notamment ceux exploitant Sodinokibi, ont attaqué sans relâche des sociétés de services professionnels en 2020, y compris des cabinets d'avocats. Les données sensibles que ces entreprises détiennent sur leurs clients, et dans certains cas sur des célébrités, ont peut-être amené les cyberattaquants à estimer qu'elles seraient plus enclines à payer une rançon pour éviter une divulgation de l'information. Les données d'un cabinet d'avocats ont ainsi été mises aux enchères pour 40 millions de dollars, signe que les cyberattaquants pensent pouvoir obtenir des rançons élevées.

En plus des attaques par ransomware, les vols de données et les attaques par accès aux serveurs ont frappé durement les services professionnels en 2020, représentant chacun 13 % des attaques contre ce secteur. Ces tendances suggèrent que les attaques par injection et l'exploitation des vulnérabilités dans le secteur des services professionnels sont courantes, car les cyberattaquants cherchent à accéder à des données sensibles.

Les chevaux de Troie d'accès à distance (RAT) étaient le troisième type d'attaque le plus courant à toucher les services professionnels, représentant 9 % des attaques contre ce secteur.

Gouvernement



33 %

des attaques contre le secteur gouvernemental ont été des attaques par des ransomware, soit le deuxième pourcentage le plus élevé parmi tous les secteurs.

25 %

des attaques contre le gouvernement ont été des tentatives de vol et de divulgation de données.

Le secteur public - y compris la défense, les administrations publiques et les services gouvernementaux - s'est classé au sixième rang du classement des secteurs les plus attaqués en 2020, avec 7,9 % de toutes les attaques contre les dix principaux secteurs. Le secteur gouvernemental conserve le même classement qu'en 2019, année où il avait été ciblé par 8 % des attaques contre les dix principaux secteurs. D'après les données IBM Security X-Force de réponse aux incidents, il semble que ce soient surtout les attaques par ransomware qui ont touché les organismes gouvernementaux en 2020, suivies de près par le vol de données.

33 % des attaques contre les organismes gouvernementaux en 2020 ont été des attaques par ransomware, ce qui le place ce secteur au deuxième rang, juste après les services professionnels. Ces chiffres perpétuent une tendance continue d'attaques par ransomware contre les entités gouvernementales, mais en 2020, X-Force Incident Response a également observé que les systèmes judiciaires et les entités de transport gouvernementaux s'étaient retrouvés dans la ligne de mire des ransomware. Près de 50 % des attaques par ransomware observées par X-Force contre des entités gouvernementales en 2020 émanaient d'opérateurs de Sodinokibi, dans le droit fil d'une tendance amorcée par le groupe en septembre 2019, avec un feu nourri d'attaques par ransomware visant [23 municipalités au Texas](#).

Le deuxième type d'attaque le plus courant contre les organismes gouvernementaux était le vol et la divulgation de données, ce qui confirme la menace posée par le vol de données et l'espionnage pour les entités gouvernementales. Les attaques par vol et divulgation de données ont représenté 25 % des attaques contre le secteur gouvernemental en 2020. Les gouvernements étrangers, les cybercriminels et même les hacktivistes ont tous révélé leur intérêt pour le vol de données d'organismes gouvernementaux.

Dans une moindre mesure, les attaques de type BEC (compromission des emails professionnels) ont également affecté ce secteur en 2020, représentant 9 % de toutes les attaques à son encontre, soit le quatrième pourcentage le plus élevé d'attaques BEC dans les secteurs que nous avons étudiés. Une mise en œuvre plus robuste de technologies d'authentification multifactorielle permettrait de faire baisser ce pourcentage à l'avenir.

Santé



28 %

des attaques contre le secteur de la santé ont été des attaques par ransomware.

17 %

des incidents exploitant la vulnérabilité CVE-2019-19781 ont ciblé le secteur des soins de santé.

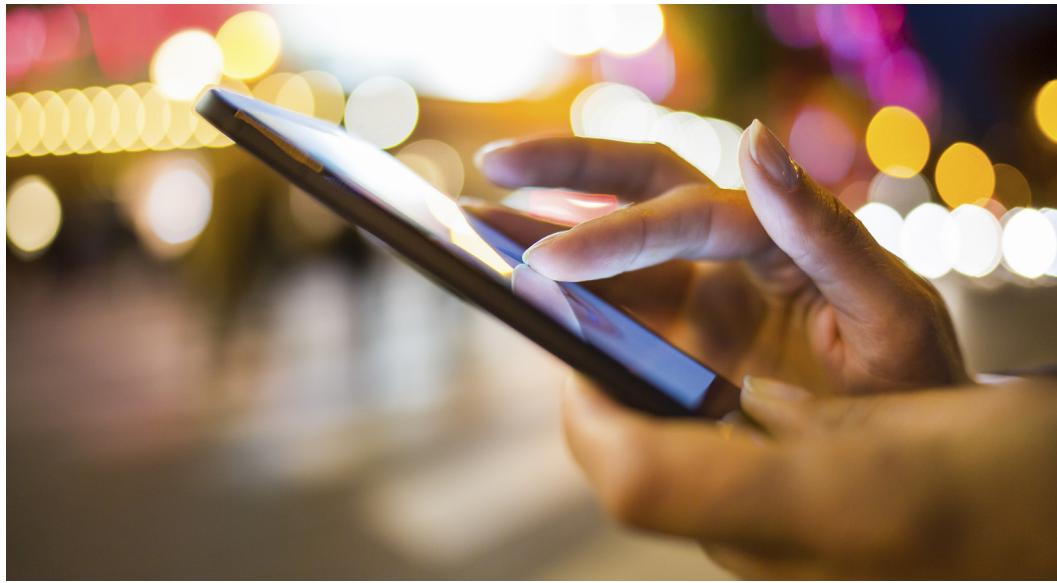
En 2020, le secteur des soins de santé se classait au septième rang des secteurs les plus attaqués, faisant l'objet de 6,6 % de toutes les attaques contre les dix principaux secteurs, alors qu'il n'occupait que le dixième rang et ne subissait que 3 % des attaques en 2019. Il s'agit d'un bond non négligeable qui correspond aux harcèlement subi par le secteur des soins de santé pendant la pandémie de COVID-19 en 2020, qu'il s'agisse d'attaques par ransomware ou d'autres tentatives par des cyberattaquants intéressés par [les travaux de recherche sur le COVID](#) et les traitements anti-COVID.

Près de 28 % des attaques contre le secteur en 2020 sont imputables à des ransomware. Les attaques par ransomware contre ce secteur peuvent être particulièrement dévastatrices, comme le montre l'issue tragique d'une attaque par ransomware contre un hôpital allemand en septembre 2020. L'attaque avait contraint une ambulance à emmener un patient dans un autre hôpital distant de 32 km, où il avait succombé. Même si les autorités allemandes avaient conclu que cette attaque [n'avait pas joué un rôle décisif](#) dans le décès du patient, à l'avenir d'autres attaques de ce type pourraient bel et bien provoquer directement des décès.

Fin octobre, des chercheurs en sécurité avaient découvert que des cybercriminels utilisant Ryuk projetaient d'attaquer plus de 400 hôpitaux américains. [Les forces de l'ordre américaines](#) et plusieurs entreprises spécialisées dans la sécurité, [dont IBM Security X-Force](#), avaient de toute urgence informé les victimes potentielles et identifié des mesures d'atténuation. Par chance, seuls sept hôpitaux sur plus de 400 avaient été touchés par Ryuk la semaine suivante.

Outre les attaques par ransomware, l'exploitation de la vulnérabilité CVE-2019-19781 pour accéder aux réseaux de santé a été courante en 2020. Le secteur des soins de santé a en fait été le troisième le plus exploité par le biais de cette CVE, cumulant 17 % de ce type d'attaques. Dans au moins un cas impliquant cette CVE dans un réseau de soins de santé, les cyberattaquants ont combiné leur activité avec PowerShell et Cobalt Strike pour les déplacements latéraux et l'exécution des objectifs.

Médias et communications



90 %

de tous les squattages DNS malveillants ont ciblé les médias, qui sont de loin le secteur le plus usurpé.

Le secteur des médias et des communications est arrivé au huitième rang des secteurs les plus attaqués en 2020, subissant 5,7 % de toutes les attaques contre les dix principaux secteurs. Il a perdu sa quatrième place de l'an dernier, lorsqu'il avait totalisé 10 % des attaques. Ce secteur englobe les fournisseurs de télécommunications et de communications mobiles, ainsi que les médias et les médias sociaux qui peuvent jouer un rôle essentiel dans les résultats politiques, en particulier en période électorale.

Les données X-Force ont déterminé que les erreurs de configuration sont le type d'attaque le plus courant contre les médias en 2020, d'où l'importance de configurer correctement les instances cloud pour éviter les divulgations de données involontaires.

Les données de Quad9 indiquent que les médias ont été le principal secteur victime de tentatives d'usurpation, les agresseurs créant des URL similaires pouvant être confondues avec les médias légitimes. Près de 90 % de tous les squattages DNS malveillants, consistant à créer un nom de domaine volontairement semblable à une page Web légitime, concernaient des médias. Cette tendance est semblable aux principales tendances d'usurpation de marques décrites précédemment dans ce rapport. Elle démontre que les cyberattaquants cherchent à jouer sur la popularité des médias et la confiance qu'ils inspirent aux consommateurs.

Transports



25 %

des attaques contre le secteur des transports en 2020 ont impliqué un délit d'initié ou une erreur de configuration.

Contrairement au secteur manufacturier, le transport a fait un bond significatif dans le classement d'IBM Security X-Force cette année, mais dans le sens inverse : à la baisse, descendant à la neuvième place, après avoir occupé la troisième place en 2019 et la deuxième en 2018. Les transports ont subi 5,1 % de toutes les attaques en 2020, contre 10 % en 2019.

Il peut y avoir plusieurs raisons à cette baisse du ciblage en 2020. Une diminution de l'utilisation des transports en 2020 en raison de la pandémie de COVID-19, ainsi que les mesures de confinement peuvent avoir diminué la rentabilité de ce secteur pour les cyberattaquants, qu'il s'agisse de cybercriminels en quête d'informations financières ou d'États-nations traquant des individus les intéressent. En outre, des contrôles de sécurité renforcés et efficaces dans ce secteur et une veille sur les menaces peuvent contribuer à la baisse des attaques observées.

Les incidents dus à des délits d'initiés et des erreurs de configuration ont eu un impact disproportionné sur les transports en 2020, surtout par rapport à d'autres secteurs. Ces deux types d'attaques cumulés ont représenté environ 25 % des attaques contre le secteur des transports l'année dernière.

La menace que les attaques internes font peser sur le secteur des transports est importante, d'autant plus que certaines des cyberattaques les plus destructrices, y compris celles dont les conséquences pourraient être mortelles, ont plus de chances de se réaliser lorsqu'un initié est impliqué.

Les ransomware et les attaques par accès aux serveurs ont représenté 26 % des attaques contre le secteur des transports en 2020.

Éducation



50 %

des attaques contre le secteur de l'éducation en 2020 ont été du spam ou des logiciels publicitaires.

10 %

des attaques ont été des attaques par ransomware.

Le secteur de l'éducation s'est classé dixième parmi les secteurs les plus attaqués en 2020, subissant 4 % de toutes les attaques contre les dix principaux secteurs. Il perd son septième rang de 2019, lorsqu'il avait fait l'objet de 8 % de toutes les attaques.

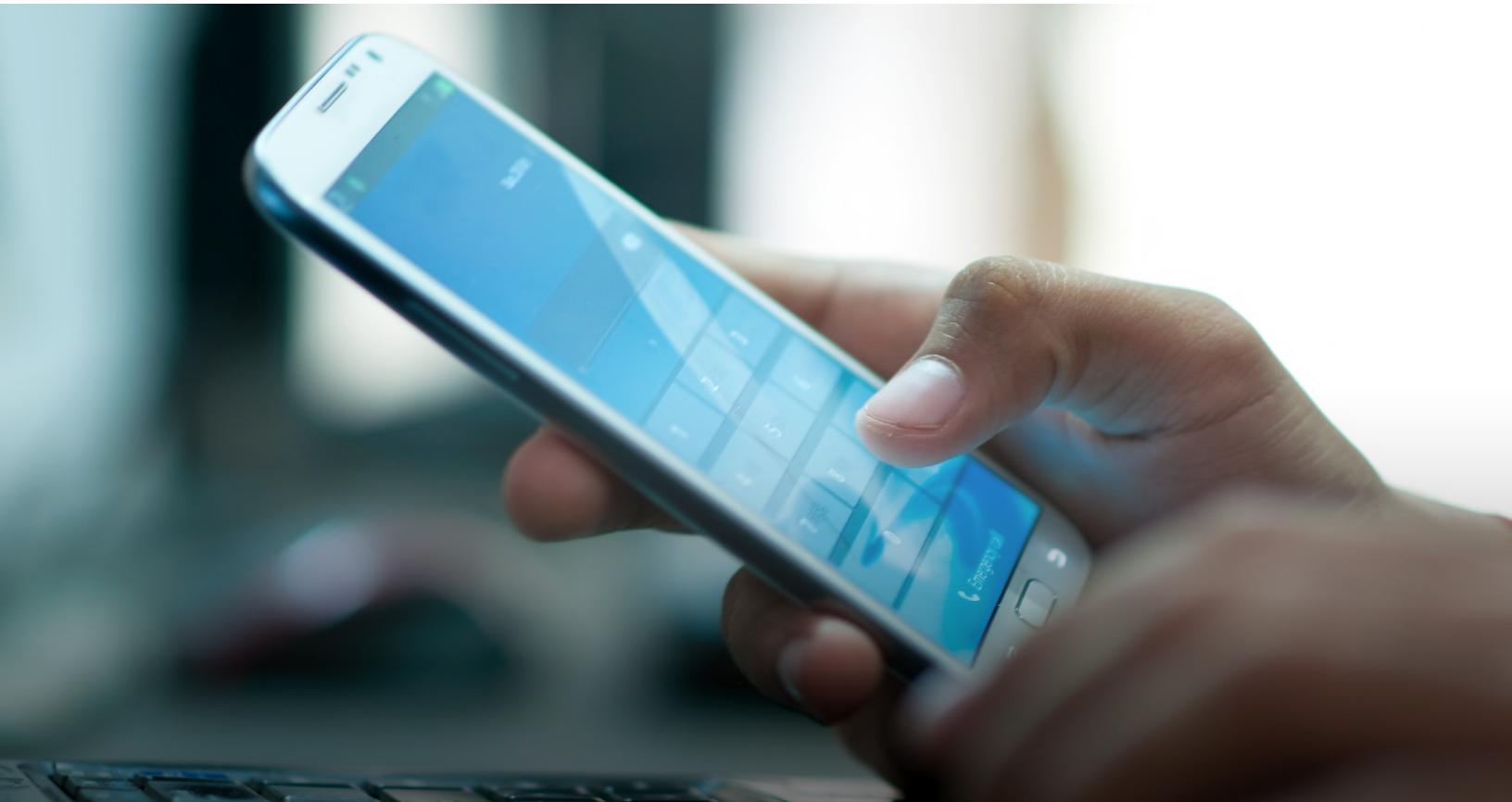
Il a été fréquemment été l'onjet d'attaques par spam et logiciels publicitaires en 2020, soit 50 % de toutes les attaques le visant. Environ la moitié des attaques était imputable au spam, soit un pourcentage plus élevé que dans tous les autres secteurs. Le hameçonnage reste donc une menace importante pour les établissements d'enseignement.

Le secteur de l'éducation a également été victime d'attaques par ransomware, selon les données de X-Force, mais avec une ampleur moindre que dans d'autres secteurs. Les ransomware ont représenté 10 % des attaques contre le secteur en 2020. Les violations de sécurité rendues publiques montrent que plusieurs établissements scolaires et universitaires ont été touchés par un ransomware en 2020, plusieurs d'entre eux choisissant de payer la rançon.

Les botnets, la fraude et les RAT ont également contribué aux attaques contre ce secteur. Les techniques d'attaque cybercriminelle courantes, le hameçonnage et les logiciels malveillants standard semblent avoir été des menaces fréquentes pour les établissements d'enseignement en 2020.

En 2021, un mélange de menaces anciennes et nouvelles va contraindre les équipes de sécurité à prendre en compte simultanément un grand nombre de risques. Sur la base de l'analyse de X-Force, voici quelques-uns des principaux points à retenir pour les priorités de l'année prochaine.

- **La surface de risque continuera de s'accroître en 2021.** Des milliers de nouvelles vulnérabilités liées aux applications et aux appareils, tant anciens que nouveaux, sont susceptibles d'être signalées.
- **La double extorsion lors des attaques par ransomware persistera probablement pendant tout 2021.** La divulgation publique de données sur les sites de dénonciation donnent plus de pouvoir aux cyberattaquants, qui peuvent en conséquence exiger des prix élevés suite aux infections par ransomware qu'ils provoquent.
- **Les cyberattaquants continuent d'étudier différents vecteurs d'attaque.** Le ciblage des systèmes Linux, de la technologie d'exploitation (OT), des appareils IoT et des environnements cloud est appelé à se poursuivre. Au fur et à mesure que le ciblage de ces systèmes et ces appareils va se perfectionner, les cyberattaquants risquent de réorienter rapidement leurs actions, en particulier à la suite de tout incident de grande envergure.
- **Chaque secteur d'activité comporte sa part de risques.** Le changement d'une année à l'autre des secteurs ciblés spécifiquement met en évidence le risque pour tous les secteurs d'activité. Il montre aussi la nécessité d'améliorations importantes et de l'arrivée à maturité des programmes de cybersécurité à tous les niveaux.



Recommandations pour la résilience

Sur la base des conclusions d'IBM Security X-Force dans ce rapport, un suivi adéquat de la veille des menaces et la mise en place de solides solutions de réponse sont des moyens efficaces pour contribuer à atténuer les menaces dans un contexte en constante évolution, quel que soit le secteur ou le pays dans lequel opère l'entreprise.

X-Force recommande aux entreprises de prendre les mesures suivantes pour mieux se préparer aux cybermenaces en 2021 :

<p>Anticipez la menace plutôt que d'y réagir. Mettez à profit la veille sur les menaces pour mieux comprendre les motivations et les tactiques des cyberattaquants et hiérarchiser les ressources de sécurité.</p> 	<p>La préparation est primordiale pour gérer les attaques par ransomware. La prévision d'une attaque par ransomware, avec l'élaboration d'un plan de réponse aux techniques mixtes d'extorsion combinant ransomware et vol de données, ainsi que l'examen régulier de ce plan peuvent faire toute la différence dans la manière dont votre entreprise réagit au moment critique.</p> 
<p>Vérifiez minutieusement la structure de gestion des correctifs de votre entreprise. Les attaques par analyse et exploitation étant les vecteurs d'infection les plus courants l'année dernière, renforcez votre infrastructure et redynamisez les détections internes pour repérer et stopper rapidement et efficacement les tentatives d'exploitation automatisées.</p> 	<p>Protégez-vous contre les menaces internes. Utilisez les solutions de prévention des pertes de données (DLP), la formation et la surveillance pour empêcher des utilisateurs internes de commettre des violations de sécurité par inadvertance ou par malveillance.</p> 
<p>Créez et formez une équipe interne de réponse aux incidents. Si vous n'en avez pas la possibilité, engagez des ressources efficaces de réponse aux incidents pour pouvoir traiter rapidement les incidents à fort impact.</p> 	<p>Organisez un test de résistance de votre plan de réponse en cas d'incident pour développer un bon entraînement pratique. Les exercices d'entraînement théoriques et les cyber-simulations peuvent doter votre équipe d'une expérience stratégique qui lui permettra de réagir plus rapidement, de réduire les temps d'indisponibilité et, en fin de compte, de limiter les pertes financières en cas de violation de sécurité.</p> 
<p>Mettez en place l'authentification multifactorielle (MFA). L'ajout de couches de protection supplémentaires aux comptes reste l'une des priorités de sécurité les plus efficaces pour les entreprises.</p> 	<p>Effectuez des sauvegardes, testez-les et stockez-les hors ligne. Le fait de pouvoir compter sur des sauvegardes, mais aussi de garantir leur efficacité grâce à des tests en conditions réelles introduit une différence cruciale pour la sécurité de l'entreprise, d'autant plus que les données de 2020 attestent d'une résurgence de l'activité des ransomware.</p> 

À propos d'IBM Security X-Force

[IBM Security X-Force](#) fournit des solutions d'information, de détection et de réponse pour aider les clients à améliorer leur stratégie de sécurité.

IBM Security [X-Force Threat Intelligence](#) combine la télémétrie des opérations de sécurité IBM, la recherche, les enquêtes de réponse aux incidents, les données commerciales et des solution open source pour aider les clients à comprendre les menaces émergentes et à prendre rapidement des décisions de sécurité éclairées.

De plus, l'équipe hautement qualifiée de [X-Force Incidents Response](#) assure une remédiation stratégique qui aide les entreprises à mieux contrôler les incidents et les violations de sécurité.

X-Force, s'appuyant sur les cyber-simulations de l'[IBM Security Command Center](#), enseigne aux clients à se préparer aux réalités des menaces d'aujourd'hui.

Tout au long de l'année, les chercheurs d'IBM X-Force proposent également des travaux de recherche et des analyses sous la forme de blogs, de livres blancs, de webinaires et de podcasts, exposant leurs connaissances sur les cyberattaquants avancés, les nouveaux logiciels malveillants et les nouvelles méthodes d'attaque. De plus, nous mettons à disposition un large corpus d'analyses sophistiquées et parfaitement à jour à l'attention des clients abonnés à notre [plateforme Premier Threat Intelligence](#).

Votre prochaine étape

[En savoir plus sur l'orchestration de votre réponse aux incidents avec IBM Security >](#)

À propos d'IBM Security

Pour vous aider à protéger votre entreprise, IBM Security s'appuie sur son portefeuille sophistiqué et intégré de produits et de services de sécurité d'entreprise basés sur l'IA. Nous vous proposons une approche moderne de votre stratégie de sécurité régie par les principes du Zero Trust, pour vous aider à prospérer face à l'incertitude. Nous alignons votre stratégie de sécurité sur votre activité métier. Nous intégrons des solutions conçues pour protéger vos ressources numériques : utilisateurs, actifs et données. Nous déployons une technologie dont le but est de gérer vos défenses contre les menaces croissantes. De cette façon, nous vous aidons à gérer et gouverner les risques inhérents aux environnements de cloud hybride d'aujourd'hui.

Notre nouvelle approche moderne et ouverte, la plate-forme IBM Cloud Pak for Security, est basée sur RedHat Open Shift et prend en charge les environnements multicloud hybrides d'aujourd'hui, grâce à un vaste écosystème de partenaires. Cloud Pak for Security est une solution logicielle conteneurisée prête pour l'entreprise qui vous permet de gérer la sécurité de vos données et de vos applications. Pour ce faire, elle intègre rapidement vos outils de sécurité existants et génère des informations approfondies sur les menaces dans les environnements de cloud hybride. Vos données ne sont pas déplacées, ce qui facilite l'orchestration et l'automatisation de votre stratégie de réponse de sécurité.

Pour plus d'informations, visitez www.ibm.com/security, suivez [@IBMSecurity](#) sur Twitter ou visitez le [blog IBM Security Intelligence](#).

Contributeurs

Auteur principal :Camille Singleton

Contributeurs :

Allison Wikoff
Ari Eitan (Intezer)
Charles DeBeck
Charlotte Hammond
Chenta Lee
Chris Sperry
Christopher Kiefer
Claire Zaboeva

David McMillen
David Moulton
Dirk Hartz
Georgia Prassinos
Ian Gallagher (Intezer)
John Zorabedian
Joshua Chung
Kelly Kane

Lauren Jensen
Limor Kessem
Mark Usher
Martin Steigemann
Matthew DeFir
Megan Radogna
Melissa Frydrych
Michelle Alvarez

Mitch Mayne
Nick Rossman
Patty Cahill-Ingraham
Randall Rossi
Richard Emerson
Salina Wuttke
Scott Craig
Scott Moore

© Copyright IBM Corporation 2021

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

Produit aux Etats-Unis
Février 2021

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp., enregistrées dans de nombreux pays. Les autres noms de produits et de services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée des marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse ibm.com/legal/copytrade.shtml

L'information contenue dans ce document était à jour à la date de sa publication initiale, et peut être modifiée sans préavis par IBM. Les offres mentionnées dans le présent document ne sont pas toutes disponibles dans tous les pays où IBM est présent. Les exemples cités concernant des clients et les performances ne sont présentés qu'à titre d'illustration. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitation.

LES RENSEIGNEMENTS CONTENUS DANS LE PRÉSENT DOCUMENT SONT FOURNIS « TELS QUELS », SANS GARANTIE, EXPRESSE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, LES GARANTIES OU CONDITIONS RELATIVES À LA QUALITÉ MARCHANDE, À L'ADAPTATION À UN USAGE PARTICULIER ET À L'ABSENCE DE CONTREFAÇON.

Les produits IBM sont garantis conformément aux dispositions des contrats. Chaque client est tenu de s'assurer qu'il respecte la réglementation applicable. IBM ne donne aucun avis juridique et ne garantit pas que ses services ou produits sont conformes aux lois applicables. Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.