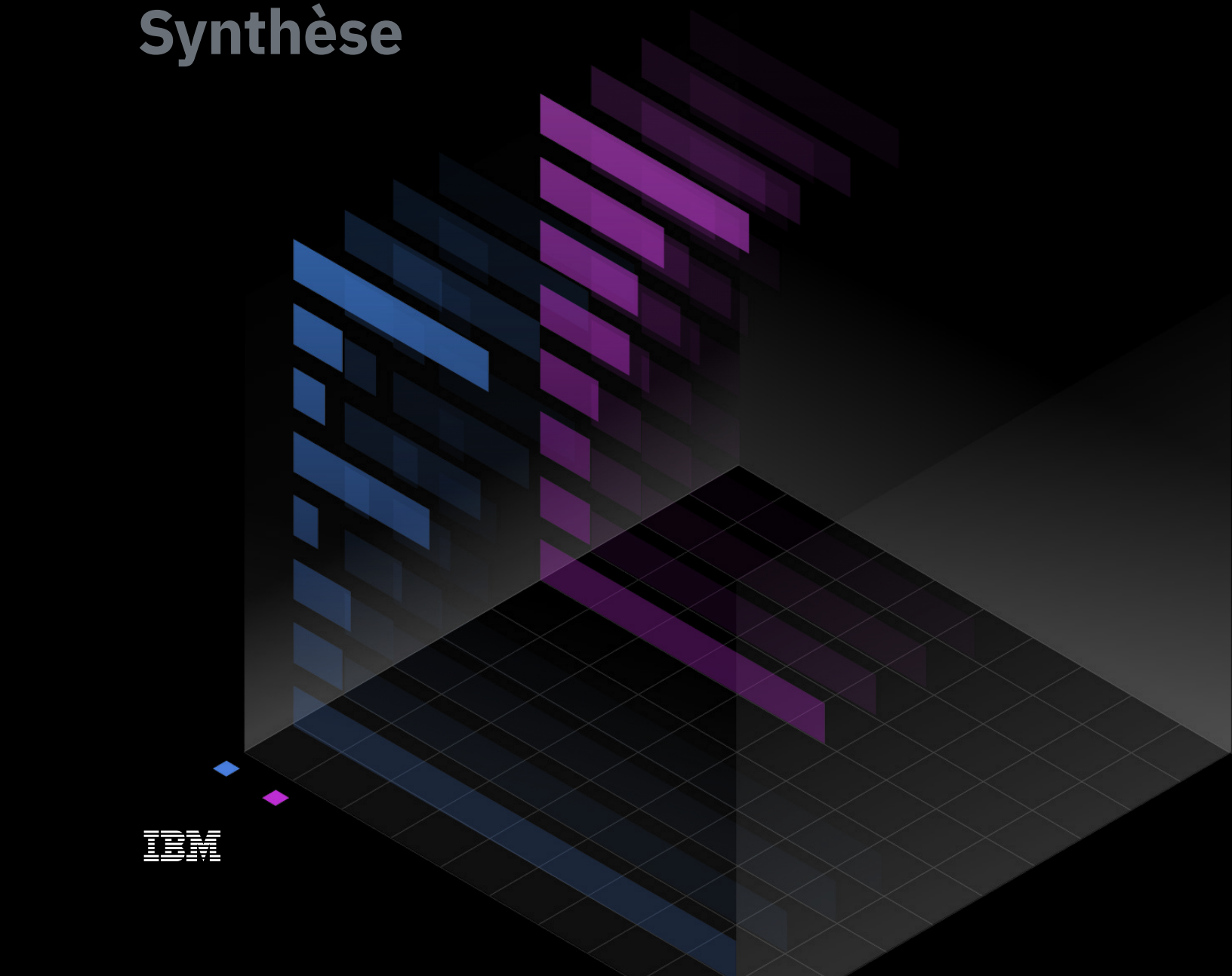
IBM Security

X-Force Threat Intelligence Index 2021

Synthèse



IBM

Introduction

L'année 2020 a sans aucun doute été l'une des plus marquantes et des plus transformatrices de notre histoire récente : une pandémie mondiale, des bouleversements économiques affectant la vie de millions de personnes et des troubles sociaux et politiques. Les répercussions de ces événements ont profondément affecté les entreprises, dont beaucoup ont opté pour une répartition de la main-d'œuvre.

Dans le domaine cybernétique, les circonstances extraordinaires de 2020 ont donné aux cyber-attaquants la possibilité d'exploiter les besoins des réseaux de communication et ont fourni de riches cibles en termes de chaînes d'approvisionnement et d'infrastructures vitales. L'année s'est terminée comme elle a commencé, avec la découverte d'une menace de portée mondiale qui nécessite une réaction et des mesures correctives rapides. Une attaque largement attribuée à un acteur de l'État-nation, qui a utilisé une porte dérobée dans un logiciel de surveillance de réseau pour attaquer des organisations du gouvernement et du secteur privé, a démontré que les risques liés aux tiers doivent être anticipés, mais ne peuvent être prévus.

Pour aider à relever les défis de notre époque, IBM Security X-Force évalue le paysage des cyber-menaces et aide les organisations à comprendre l'évolution des menaces, les risques qui y sont associés et la manière de hiérarchiser les efforts de cybersécurité. En plus de fournir à nos clients des renseignements de première qualité sur les menaces, nous analysons la richesse des données que nous recueillons pour produire le X-Force Threat Intelligence Index, un bilan annuel sur le paysage des menaces et son évolution.

Parmi les tendances que nous avons suivies, les logiciels de rançon ont continué leur ascension pour devenir le type de menace numéro un, et représenter 23 % des événements de sécurité auxquels X-Force a répondu en 2020. Les attaquants de rançon ont augmenté la pression pour extorquer des paiements en combinant le cryptage des données avec des menaces de fuite de données sur les sites publics. Le succès de ces manœuvres a permis à un seul gang de rançon de récolter des profits de plus de 123 millions de dollars en 2020[1], selon les estimations de la X-Force.

En 2020, les entreprises manufacturières ont fait face à une avalanche de rançons et d'autres attaques. L'industrie manufacturière dans son ensemble a été la deuxième plus ciblée, après les secteurs des finances et des assurances, alors qu'elle était la huitième plus ciblée en 2019. X-Force a découvert des attaquants sophistiqués utilisant des campagnes de harponnage ciblées lors d'attaques contre des entreprises manufacturières et des ONG impliquées dans la chaîne d'approvisionnement du vaccin contre le COVID-19.

1. Dans ce rapport, toutes les devises sont exprimées en dollars américains.

Les acteurs de la menace ont également innové dans le domaine des logiciels malveillants, en particulier ceux qui visent Linux, le code open source qui soutient l'infrastructure cloud et le stockage de données critiques des entreprises. L'analyse d'Intezer a permis de découvrir 56 nouvelles familles de logiciels malveillants pour Linux en 2020, ce qui est bien plus que le niveau d'innovation constaté pour d'autres types de menaces.

Il y a des raisons d'espérer que 2021 sera une année meilleure. Les tendances sont évidemment difficiles à prévoir, mais nous pouvons toujours compter sur le changement. La résilience face aux défis croissants et décroissants de la cybersécurité exige des renseignements exploitables et une vision stratégique pour l'avenir d'une sécurité plus ouverte et plus connectée.

Dans un esprit de force communautaire, IBM Security a le plaisir de proposer le 2021 X-Force Threat Intelligence Index. Les conclusions de ce rapport peuvent aider les équipes de sécurité, les professionnels du risque, les décideurs, les chercheurs, les médias et autres, à comprendre où se trouvaient les menaces au cours de l'année écoulée et à se préparer aux menaces à venir.

Synthèse

IBM Security X-Force s'est appuyé sur des milliards de points de données collectés auprès de nos clients et de sources publiques entre janvier et décembre 2020 pour analyser les types d'attaques, les vecteurs d'infection et les comparaisons mondiales et sectorielles. Voici quelques-unes des principales conclusions présentées dans le X-Force Threat Intelligence Index.

23 %

Part des attaques avec rançon
Les rançons étaient la méthode d'attaque la plus populaire en 2020, et représentait 23 % de tous les incidents auxquels IBM Security X-Force a répondu et aidé à remédier.

Plus de 123 millions de dollars

Bénéfices estimés des principaux logiciels de rançon
X-Force estime que, selon des estimations prudentes, les acteurs de Sodinokibi (également connu sous le nom de REvil) ont réalisé à eux seuls au moins 123 millions de dollars de bénéfices en 2020 et ont volé environ 21,6 téraoctets de données.

25 %

Pourcentage de vulnérabilité aux attaques au premier trimestre 2020
Les acteurs de la menace ont profité d'une faille de Citrix pour exploiter cette vulnérabilité dans 25 % des attaques des trois premiers mois de l'année et dans 8 % des attaques totales en 2020.

35 %

Part des techniques de balayage-exploitation comme principaux vecteurs d'infection
Le balayage et l'exploitation des vulnérabilités sont devenues le premier vecteur d'infection en 2020, dépassant le hameçonnage qui était le premier vecteur en 2019.

N°2

Classement de l'industrie manufacturière parmi les secteurs les plus attaqués
L'industrie manufacturière était la deuxième industrie la plus attaquée en 2020, alors qu'elle occupait la huitième place en 2019, et n'était devancée que par le secteur des 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 iraniens ont permis aux chercheurs de la X-Force de découvrir environ 5 heures de vidéo sur un serveur mal configuré, apportant des informations sur leurs techniques.

Plus de 100

Cadres ciblés par une campagne d'hameçonnage de précision
Au milieu de l'année 2020, X-Force a démasqué une campagne mondiale d'hameçonnage qui a touché plus de 100 cadres de haut niveau occupant des fonctions de gestion et d'approvisionnement pour un groupe de travail chargé d'acquérir des équipements de protection individuelle (EPI) dans le cadre de la lutte contre le COVID-19.

49 %

Taux de croissance de la vulnérabilité liée aux SCI, 2019-2020
Les vulnérabilités liées aux systèmes de contrôle industriel (SCI) découvertes en 2020 étaient 49 % plus élevées d'une année à l'autre par rapport à 2019.

56

Nombre de nouvelles familles de logiciels malveillants pour Linux
Le nombre de nouvelles familles de logiciels malveillants liés à Linux découverts en 2020 était de 56, le plus haut niveau jamais atteint. Cela représente une augmentation de 40 % par rapport à l'année 2019.

31 %

Pourcentage d'attaques perpétrées en Europe
L'Europe était la zone géographique la plus attaquée en 2020, avec 31 % des attaques observées par X-Force, suivie par l'Amérique du Nord (27 %) et l'Asie (25 %).

Perspectives d’avenir

En 2021, un mélange d'anciennes et de nouvelles menaces obligera les équipes de sécurité à considérer simultanément un grand nombre de risques. Selon l'analyse de la X-Force, voici quelques unes des principales priorités pour l'année 2021.

- **La surface de risque continuera à augmenter en 2021.** Avec des milliers de nouvelles vulnérabilités susceptibles d'être signalées dans les applications et les appareils à la fois nouveaux et existants.
- **La double extorsion de rançon persistera probablement pendant toute l'année 2021.** Le fait que les attaquants divulguent publiquement des données sur des sites à scandale augmente le pouvoir des acteurs de la menace de commander des prix élevés pour les infections par des logiciels de rançon.
- **Les acteurs de la menace continuent à se tourner vers des vecteurs d'attaque différents.** Le ciblage des systèmes Linux, de la technologie opérationnelle (OT), des dispositifs IoT et des environnements cloud se poursuivra. À mesure que le ciblage de ces systèmes et dispositifs devient plus avancé, les acteurs de la menace peuvent rapidement réorienter leurs efforts, en particulier à la suite d'un incident très médiatisé.
- **Chaque industrie a sa part de risques.** Les changements observés d'une année sur l'autre dans le ciblage spécifique à l'industrie mettent en évidence le risque pour tous les secteurs industriels et la nécessité de faire progresser et de faire mûrir de manière significative les programmes de cybersécurité dans tous les domaines.

Recommandations pour la résilience

Selon les conclusions du rapport d'IBM Security X-Force, le suivi des renseignements sur les menaces et la mise en place de solides capacités de réaction sont des moyens efficaces de contribuer à atténuer les menaces dans un paysage en évolution, quel que soit le secteur d'activité ou le pays dans lequel on opère.

X-Force recommande aux organisations de prendre les mesures suivantes pour mieux se préparer aux cyber-menaces de 2021 :

Cessez de réagir aux menaces, prenez les devants. Exploitez les renseignements sur la menace pour mieux comprendre les motivations et les tactiques des acteurs de la menace afin de hiérarchiser les ressources de sécurité.

La préparation est essentielle pour répondre aux demandes de rançon. La planification d'une attaque par demande de rançon - y compris un plan qui traite des techniques mixtes de demande de rançon et de vol de données - et l'exécution régulière de ce plan peuvent faire toute la différence dans la manière dont votre organisation réagit au moment critique.

Vérifiez la structure de gestion des correctifs de votre organisation. Le balayage et l'exploitation étant le vecteur d'infection le plus courant l'année dernière, durcissez votre infrastructure et redynamisez les détections internes pour trouver et arrêter rapidement et efficacement les tentatives d'exploitation automatisée.

Protégez-vous contre les menaces d'initiés. Utilisez les solutions de prévention des pertes de données (DLP), la formation et la surveillance pour éviter que des intrus ne pénètrent accidentellement ou malicieusement dans votre organisation.

Créez et formez une équipe de réponse aux incidents au sein de votre organisation. Si ce n'est pas possible, mettez en place un dispositif efficace de réaction aux incidents afin de réagir rapidement aux incidents à fort impact.

Testez le plan de réponse aux incidents de votre organisation pour développer une mémoire musculaire. Les exercices sur table ou les expériences de cyber-surveillance peuvent fournir à votre équipe une expérience essentielle pour améliorer le temps de réaction, réduire les temps d'arrêt et, en fin de compte, économiser de l'argent en cas de faille.

Mettez en œuvre une authentification multifactorielle (AMF). L'ajout de couches de protection aux comptes reste l'une des priorités de sécurité les plus efficaces pour les organisations.

Effectuez des sauvegardes, testez-les et stockez-les hors ligne. Le fait de garantir non seulement la présence de sauvegardes mais aussi leur efficacité par des tests en situation réelle fait une différence essentielle dans la sécurité de l'organisation, surtout si l'on considère la hausse des demandes de rançon en 2020.

À propos d'IBM Security X-Force

IBM Security X-Force offre des capacités de repérage, de détection et de réponse pour aider les clients à améliorer leur posture de sécurité.

IBM SecurityX-Force Threat Intelligence combine la télémétrie des opérations de sécurité IBM, la recherche, les enquêtes de réponse aux incidents, les données commerciales et les sources ouvertes pour aider les clients à comprendre les menaces émergentes et à prendre rapidement des décisions de sécurité éclairées.

En outre, l'équipe hautement qualifiée de réponse aux incidents de X-Force fournit des mesures correctives stratégiques qui aident les organisations à mieux contrôler les incidents et les brèches de sécurité.

La X-Force combinée aux expériences du centre de commande de sécurité IBM dans le domaine de la cybersécurité permet aux clients d'être prêts à faire face aux réalités des menaces actuelles.

Tout au long de l'année, les chercheurs de l'IBM X-Force fournissent également des recherches et des analyses continues sous la forme de blogs, de livres blancs, de webinaires et de podcasts, mettant en avant notre connaissance des acteurs-clés de la menace, des nouveaux logiciels malveillants et des nouvelles méthodes d'attaque. En outre, nous fournissons un grand nombre d'analyses actuelles et avant-gardistes aux clients abonnés à notre plateforme Premier Threat Intelligence.

Votre prochaine étape

Découvrez comment orchestrer votre réponse aux incidents avec IBM Security

À propos d'IBM Security

IBM Security travaille avec vous pour vous aider à protéger votre entreprise grâce à un portefeuille avancé et intégré de produits et services de sécurité d'entreprise, enrichis par l'IA, et à une approche moderne de votre stratégie de sécurité utilisant les principes de confiance zéro, afin de vous aider à prospérer face à l'incertitude. En alignant votre stratégie de sécurité sur votre entreprise, en intégrant des solutions conçues pour protéger vos utilisateurs, vos ressources et vos données numériques, et en déployant des technologies pour vous permettre de vous défendre contre les menaces croissantes, nous vous aidons à gérer et à gouverner les risques qui vont de pair avec les environnements cloud hybrides actuels.

Notre nouvelle approche moderne et ouverte, la plate-forme IBM Cloud Pak for Security, s'appuie sur RedHat Open Shift et prend en charge les environnements hybrides multi-clouds actuels avec un vaste écosystème de partenaires. Cloud Pak for Security est une solution logicielle conteneurisée prête à l'emploi qui vous permet de gérer la sécurité de vos données et de vos applications en intégrant rapidement vos outils de sécurité existants pour obtenir une meilleure compréhension des menaces dans les environnements cloud hybrides, et en laissant vos données là où elles se trouvent, afin de faciliter l'orchestration et l'automatisation de vos mesures de sécurité.

Pour plus d'informations, veuillez consulter www.ibm.com/security, suivre @IBMSecurity sur Twitter ou visiter le blog IBM Security Intelligence.

Contributeurs

Auteur principal :
Camille Singleton

Collaborateurs :
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

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

Produit aux Etats-Unis
Février 2021

IBM **Security**