Communiqués de presse

Rapport IBM Security : Doublement des attaques contre les industries soutenant les efforts de lutte contre la COVID-19

Un groupe à l'origine de ransomwares a récolté des millions de dollars ; Prévisions floues sur fond d'augmentation de 40% des logiciels malveillants Open Source en 2020 ; Les outils « indispensables » de distanciation sociale dominent parmi les principales marques usurpées

CAMBRIDGE, Massachusetts, le 24 février 2021 - IBM (NYSE: IBM) Security a publié aujourd'hui l'indice 2021 X-Force Threat Intelligence Index qui met en évidence la façon dont les cyberattaques ont évolué en 2020, les acteurs de la menace cherchant à tirer profit des défis socio-économiques, commerciaux et politiques sans précédent engendrés par la pandémie de COVID-19. En 2020, IBM Security X-Force a observé que les attaquants orientaient leurs attaques vers les entreprises dont l'activité était fortement liée aux efforts de lutte contre la COVID-19 au niveau mondial, telles que les hôpitaux, les fabricants de produits médicaux et pharmaceutiques, ainsi que les sociétés d'énergie alimentant la chaîne d'approvisionnement de la COVID-19.

Selon ce nouveau rapport, les cyberattaques dans les domaines des soins de santé, de l'industrie manufacturière et de l'énergie ont doublé par rapport à l'année précédente, les acteurs de la menace visant les organisations qui ne pouvaient pas se permettre de temps d'arrêt en raison des risques de perturbation des efforts médicaux ou des chaînes d'approvisionnement critiques. De fait, l'industrie manufacturière et l'énergie ont été les secteurs les plus attaqués en 2020, juste derrière le secteur de la finance et de l'assurance. Les attaquants ont profité de l'augmentation de près de 50 % des vulnérabilités des systèmes de contrôle industriel (SCI), dont l'industrie manufacturière et l'énergie dépendent toutes deux fortement.

« En substance, la pandémie a remodelé ce qui est aujourd'hui considéré comme une infrastructure critique, et les attaquants en ont pris note. Pour la première fois, de nombreuses organisations ont été en première ligne des efforts de réponse - que ce soit pour soutenir la recherche sur la COVID-19, maintenir les chaînes d'approvisionnement en vaccins et en produits alimentaires, ou produire des équipements de protection individuelle », a déclaré **Nick Rossmann, Global Threat Intelligence Lead, IBM Security X-Force***. « La victimologie des attaquants a changé au fur et à mesure que la chronologie des événements liés à la COVID-19 se déroulait, indiquant une fois de plus la capacité d'adaptation, l'ingéniosité et la persévérance des cyber-attaquants. »*

L'IBM X-Force Threat Intelligence Index est basé sur les informations et les observations provenant de la gestion de plus de 150 milliards d'événements de sécurité par jour dans plus de 130 pays. En outre, des données sont recueillies et analysées à partir de multiples sources au sein d'IBM, notamment IBM Security X-Force Threat Intelligence and Incident Response, X-Force Red, IBM Managed Security Services, et les données fournies par Quad9 et Intezer, qui ont tous deux contribué au rapport 2021.

Voici quelques-uns des principaux points clés du rapport :

- **Les cybercriminels accélèrent l'utilisation des logiciels malveillants liés à Linux** - Avec une augmentation de 40 % des familles de logiciels malveillants liés à Linux au cours de l'année dernière, selon Intezer, et une augmentation de 500 % des logiciels malveillants "Go-written" au cours des six premiers mois de 2020, les attaquants accélèrent la migration vers les logiciels malveillants Linux, qui peuvent s'exécuter plus facilement sur diverses plateformes, y compris les environnements Cloud.

- **La pandémie pèse sur les principales marques usurpées** - Au milieu d'une année de distanciation sociale et de travail à distance, les marques proposant des outils de collaboration telles que Google, Dropbox et Microsoft, ou les marques de commerce en ligne comme Amazon et PayPal, sont dans le top 10 des marques usurpées en 2020. YouTube et Facebook, sur lesquels les consommateurs se sont davantage appuyés pour suivre l'actualité l'année dernière, sont également en tête de liste. Étonnamment, Adidas a fait ses débuts en tant que septième marque la plus souvent usurpée en 2020, probablement en raison de la demande pour les lignes de baskets Yeezy et Superstar.

- **Les groupes à l'origine de ransomwares tirent profit d'un modèle économique rentable** - Les ransomwares ont été à l'origine de près d'une attaque sur quatre à laquelle X-Force a répondu en 2020, les attaques évoluant de manière agressive pour inclure des tactiques de double extorsion. En utilisant ce modèle, X-Force évalue que Sodinokibi - le groupe de ransomware le plus souvent observé en 2020 - a connu une année très rentable. X-Force estime que le groupe a fait une estimation prudente de ses gains de plus de 123 millions de dollars l'année dernière, avec environ deux tiers de ses victimes qui ont payé une rançon, selon le rapport.

L'investissement dans les logiciels malveillants open source menace les environnements Cloud

Dans le contexte de la pandémie de COVID-19, de nombreuses entreprises ont cherché à accélérer leur adoption du Cloud. « Une récente étude du Gartner a révélé que près de 70 % des entreprises utilisant aujourd'hui des services Cloud prévoient d'augmenter leurs dépenses dans ce domaine suite aux perturbations causées par la COVID-19[1] ». Avec Linux utilisé actuellement par 90 % des applications Cloud, et le rapport X-Force qui montre une augmentation de 500 % des familles de logiciels malveillants liés à Linux au cours de la dernière décennie, les environnements Cloud peuvent devenir un vecteur d'attaque privilégié pour les acteurs de la menace.

Avec l'augmentation des logiciels malveillants open source, IBM estime que les attaquants pourraient chercher des moyens d'améliorer leurs marges de profit - en réduisant éventuellement les coûts, en augmentant leur efficacité et en créant des opportunités pour rendre leurs attaques plus rentables. Le rapport met en lumière différents groupes de menaces tels que APT28, APT29 et Carbanak qui se tournent vers les logiciels malveillants open source, indiquant que cette tendance sera un accélérateur pour davantage d'attaques dans le Cloud au cours de l'année à venir.

Le rapport suggère également que les attaquants exploitent la puissance de traitement extensible que fournissent les environnements Cloud, répercutant les lourdes charges d'utilisation du Cloud sur les organisations victimes, comme l'a observé Intezer avec plus de 13 % de nouveaux codes, non observés auparavant, dans les logiciels malveillants de cryptomining Linux en 2020.

Les attaquants visant les Clouds, X-Force recommande aux organisations d'envisager une approche zero-trust dans leur stratégie de sécurité. Les entreprises devraient également faire du confidential computing (informatique confidentielle) un élément essentiel de leur infrastructure de sécurité pour aider à protéger leurs données les plus sensibles - en chiffrant les données en cours d'utilisation, les entreprises peuvent contribuer à réduire le risque d'exploitation par un acteur malveillant, même s'il est en mesure d'accéder à leurs

environnements sensibles.

Des cybercriminels déguisés en marques célèbres

Le rapport 2021 souligne que les cybercriminels ont choisi de se « déguiser » le plus souvent en marques auxquelles les consommateurs font confiance. Considéré comme l'une des marques les plus influentes au monde, Adidas a attiré les cybercriminels qui tentaient d'exploiter la demande des consommateurs pour diriger ceux qui recherchaient des baskets convoitées vers des sites web malveillants conçus pour ressembler à des sites légitimes. Une fois qu'un utilisateur visitait ces domaines d'apparence légitime, les cybercriminels cherchaient soit à réaliser des escroqueries de paiement en ligne, soit à voler les informations financières des utilisateurs, soit à récolter leurs informations d'identification, soit à infecter les terminaux des victimes avec des logiciels malveillants.

Le rapport indique que la majorité des usurpations subies par Adidas sont associées aux lignes de baskets Yeezy et Superstar. La ligne Yeezy à elle seule aurait rapporté 1,3 milliard de dollars en 2019 et était l'une des baskets les plus vendues par le géant de la fabrication de vêtements de sport. Il est probable qu'avec l'engouement pour le lancement des nouvelles baskets début 2020, les attaquants aient exploité la demande pour la marque lucrative pour faire leur propre profit.

Les ransomware sont l'attaque la plus courante en 2020

Selon le rapport, en 2020, le monde a connu plus d'attaques par ransomware qu'en 2019. Près de 60 % des attaques par ransomware auxquelles X-Force a répondu utilisaient une stratégie de double extorsion par laquelle les attaquants chiffraient, volaient et ensuite menaçaient de divulguer des données, si la rançon n'était pas payée. En fait, en 2020, 36 % des violations de données qu'X-Force a suivies provenaient d'attaques par ransomware qui impliquaient également un vol de données présumé, ce qui laisse entendre que les violations de données et les attaques par ransomware commencent à se télescoper.

Le groupe le plus actif en matière de ransomware identifié en 2020 était Sodinokibi (également connu sous le nom de REvil), représentant 22 % de tous les incidents de ransomware observés par X-Force. Ce dernier estime que Sodinokibi a volé environ 21,6 téraoctets de données à ses victimes, que près des deux tiers des victimes de Sodinokibi ont payé une rançon, et qu'environ 43 % ont vu leurs données divulguées - ce qui, selon les estimations de X-Force, a permis au groupe de gagner plus de 123 millions de dollars l'année dernière.

Tout comme Sodinokibi, le rapport a révélé que les groupes les plus prospères en matière de ransomwares en 2020 se concentraient également sur le vol et la fuite de données, ainsi que sur la création de cartels de ransomware-as-a-service et l'externalisation d'aspects clés de leurs opérations à des cybercriminels spécialisés dans différents aspects d'une attaque. En réponse à ces attaques de ransomwares plus agressives, X-Force recommande aux organisations de limiter l'accès aux données sensibles et de protéger les comptes à privilèges avec la gestion des accès privilégiés (PAM) et la gestion des identités et des accès (IAM).

Voici les autres principales conclusions du rapport :

- **Les vulnérabilités dépassent le phishing comme vecteur d'infection le plus courant** - Le rapport 2021 révèle que le moyen le plus efficace d'accéder aux environnements des victimes l'année dernière a été l'analyse et l'exploitation des vulnérabilités (35 %), dépassant le phishing (31 %) pour la première fois depuis des années.

- **L'Europe a subi les conséquences des attaques de 2020** - Avec 31 % des attaques auxquelles X-Force a répondu en 2020, selon le rapport, l'Europe a subi davantage d'attaques que toute autre région, les ransomwares étant les principaux moyens utilisés. En outre, l'Europe a connu plus d'attaques de menaces internes que toute autre région, avec deux fois plus d'attaques de ce type que l'Amérique du Nord et l'Asie réunies.

Le rapport présente les données recueillies par IBM en 2020 afin de fournir des informations pertinentes sur le paysage mondial des menaces et d'informer les professionnels de la sécurité sur les menaces les plus significatives pour leurs organisations. Pour télécharger une copie du X-Force Threat Intelligence Index 2021 : https://www.ibm.biz/threatindex2021

A propos d'IBM Security

IBM Security offre aux entreprises l'une des gammes de produits et services de sécurité les plus performantes et intégrées du marché. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de gérer efficacement les risques et de se défendre face aux menaces émergentes. IBM compte parmi les plus grandes organisations mondiales dédiées à la recherche, au développement et à la conception de solutions de sécurité, gère plus de 150 milliards d'évènements de sécurité par jour dans plus de 130 pays, et possède plus de 10 000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous sur https://www-03.ibm.com/security/fr-fr/, suivez IBMSecurity sur Twitter ou consultez le blog IBM Security Intelligence.

Contacts presse :

IBM
Gaëlle Dussutour
Tél. : + 33 (0) 6 74 98 26 92
dusga@fr.ibm.com

Weber Shandwick pour IBM

Robin Legros / Eric Chauvelot

Tél. : + 33 (0)6 68 04 57 83 / +33 (0)6 21 64 28 48

ibmfrance@webershandwick.com

---

[1] Communiqué de presse Gartner, *Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021*, 17 Novembre 2020