

IBM X-Force : Vols de données d'identification et vulnérabilité des entreprises en 2019

Les marques de technologie grand public ciblées par les attaques de phishing ; les erreurs de configuration représentent plus de 85% des enregistrements exposés ; les chevaux de Troie et les ransomwares dans le domaine bancaire sont fortement liés

CAMBRIDGE, MA - 11 févr. 2020: L'entité sécurité d'IBM (NYSE : IBM) a publié aujourd'hui son rapport [X-Force Threat Intelligence Index 2020](#), qui souligne la façon dont les techniques des cybercriminels ont évolué après des décennies d'accès à des dizaines de milliards de données d'entreprises et de particuliers et à des centaines de milliers de failles logicielles. Selon le rapport, 60% des entrées initiales observées dans les réseaux des victimes ont exploité soit des données d'identification volées précédemment, soit des vulnérabilités logicielles connues, ce qui a permis aux attaquants de moins recourir à la ruse pour y accéder.

L'IBM X-Force Threat Intelligence Index met en évidence les facteurs qui contribuent à cette évolution, notamment les trois principaux vecteurs d'attaque initiale :

- Le phishing a été un vecteur d'infection initial efficace dans moins d'un tiers des incidents observés (31%), contre la moitié en 2018.
- L'analyse et l'exploitation des vulnérabilités ont entraîné 30% des incidents observés, contre seulement 8% en 2018. En fait, les anciennes vulnérabilités connues de Microsoft Office et de Windows Server Message Block présentaient encore des taux d'exploitation élevés en 2019.
- L'utilisation de données d'identification précédemment volées gagne également du terrain en tant que point d'entrée privilégié dans les incidents observés (29% des cas). Rien qu'en 2019, le rapport indique que plus de 8,5 milliards d'enregistrements ont été compromis, ce qui a entraîné une augmentation de 200% des données exposées signalées d'une année sur l'autre, ce qui s'ajoute au nombre croissant d'informations d'identification volées que les cybercriminels peuvent utiliser comme source.

*« La quantité d'enregistrements exposés que nous observons aujourd'hui signifie que les cybercriminels mettent la main sur davantage de clés de nos maisons et de nos entreprises. Les attaquants n'auront pas besoin d'investir du temps pour concevoir des moyens sophistiqués d'entrer dans une entreprise ; ils peuvent déployer leurs attaques simplement en utilisant des entités connues, comme la connexion avec des identifiants volés », a déclaré **Wendi Whitmore, Vice President, IBM X-Force Threat Intelligence**. « Les mesures de protection, telles que l'authentification multifactorielle et l'authentification unique, sont*

importantes pour la cyber-résilience des organisations ainsi que pour la protection et la confidentialité des données des utilisateurs ».

Voici quelques-unes des principales informations clés du rapport :

- **L'importance d'une bonne configuration** - L'analyse d'IBM a révélé que sur les plus de 8,5 milliards d'enregistrements violés signalés en 2019, 7 milliards, soit plus de 85%, étaient dus à la mauvaise configuration de serveurs Cloud ou d'autres systèmes - ce qui est très différent de 2018, où ces enregistrements représentaient moins de la moitié du total des enregistrements.
- **Les attaquants mises sur les ransomwares** - Certains des chevaux de Troie bancaires les plus actifs mentionnés dans le rapport de cette année, tels que TrickBot, sont de plus en plus souvent utilisés pour préparer le terrain à des attaques de type ransomware. En fait, les nouveaux codes utilisés par les chevaux de Troie bancaires et les ransomwares sont en tête du classement par rapport aux autres variantes de logiciels malveillants évoquées dans le rapport.
- **Le rachat de Tech Trust pour le phishing** - Le rapport IBM X-Force d'IBM a révélé que les marques de technologie, de médias sociaux et de contenu en streaming des ménages font partie du "Top 10" des marques usurpées que les cyber-attaquants imitent dans leurs tentatives de phishing. Ce changement pourrait démontrer la confiance croissante accordée aux fournisseurs de technologie plutôt qu'aux marques historiques de confiance dans les domaines du commerce de détail et de la finance. Parmi les marques les plus utilisées dans les systèmes de squatting, on trouve Google, YouTube et Apple.

Les attaques de type ransomware évoluent

Le rapport a révélé les tendances des attaques de type ransomware dans le monde entier, visant à la fois le secteur public et le secteur privé. Le rapport montre une hausse de l'activité en matière de ransomware en 2019. IBM X-Force, qui a déployé son équipe de réponse aux incidents de type ransomware dans 13 secteurs différents dans le monde, réaffirme que ces attaques sont agnostiques à un secteur d'activité.

Alors que plus de [100 entités du gouvernement américain](#) ont été touchées par des attaques de type ransomware l'année dernière, IBM X-Force a également observé des attaques importantes contre les secteurs industriel, du commerce de détail et des transports - qui sont connus pour détenir un surplus de données

monétisables ou pour s'appuyer sur une technologie obsolète et, par conséquent, font face à l'extension de la vulnérabilité. En fait, dans 80% des tentatives de ransomware observées, les attaquants exploitaient les vulnérabilités de Windows Server Message Block, la même tactique utilisée pour propager [WannaCry](#), une attaque qui a paralysé des entreprises dans 150 pays en 2017.

Les attaques de type ransomware [ayant coûté](#) aux organisations plus de 7,5 milliards de dollars en 2019, les adversaires en récoltent les fruits et n'ont aucune incitation à ralentir en 2020. En collaboration avec [Intezer](#), le rapport d'IBM indique qu'un nouveau code malveillant a été observé dans 45% des chevaux de Troie bancaires et 36% des ransomwares. Cela suggère qu'en créant de nouveaux codes, les attaquants maintiennent leurs efforts pour éviter d'être détectés.

En parallèle, IBM X-Force a observé une forte relation entre les ransomwares et les chevaux de Troie dans le domaine bancaire, ces derniers étant utilisés pour ouvrir la porte à des attaques ciblées et à fort enjeu, diversifiant ainsi la manière dont les ransomwares sont déployés. Par exemple, le logiciel malveillant financier le plus actif selon le rapport, TrickBot, est soupçonné de déployer Ryuk sur les réseaux d'entreprise, tandis que divers autres chevaux de Troie bancaires, tels que QakBot, GootKit et Dridex se diversifient également en proposant des variantes de ransomwares.

Les attaquants usurpent les sociétés de technologie et de médias sociaux avec des systèmes de phishing

Les consommateurs étant de plus en plus sensibilisés aux emails de phishing, les tactiques de phishing elles-mêmes sont de plus en plus ciblées. En collaboration avec [Quad9](#), IBM a observé une tendance au squatting dans les campagnes de phishing, où les attaquants se font passer pour des marques de produits technologiques de consommation avec des liens attrayants, en utilisant des sociétés de technologie, de médias sociaux et de streaming de contenu, pour inciter les utilisateurs à cliquer sur des liens malveillants dans leurs tentatives de phishing.

Près de 60% des 10 marques les plus usurpées identifiées étaient des domaines Google et YouTube, tandis que les domaines Apple (15%) et Amazon (12%) ont également été usurpés par des attaquants cherchant à voler les données monétisées des utilisateurs. IBM X-Force estime que ces marques ont été ciblées principalement en raison des données monétisables qu'elles détiennent.

Facebook, Instagram et Netflix figurent également dans la liste des 10 marques les plus usurpées observées, mais à un taux nettement inférieur. Ceci peut être dû au fait que ces services ne détiennent généralement pas directement de données monétisables. Comme les attaquants parient souvent sur la réutilisation des données d'identification pour accéder à des comptes avec des revenus plus lucratifs, IBM X-Force indique que la réutilisation fréquente des mots de passe pourrait être ce qui a potentiellement fait de ces marques des cibles. En fait, [l'étude Future of Identity](#) d'IBM a révélé que 41% des millennials interrogées réutilisent le même mot de passe plusieurs fois et que la génération Z n'utilise en moyenne que cinq mots de passe, ce qui indique un taux de réutilisation plus élevé.

Discerner les domaines usurpés peut s'avérer extrêmement difficile, et c'est exactement ce sur quoi les attaquants misent. Avec près de 10 milliards de comptes combinés^[1], les dix principales marques usurpées répertoriées dans le rapport offrent aux attaquants un large éventail de cibles, ce qui augmente la probabilité qu'un utilisateur peu méfiant clique sur un lien semblant inoffensif d'une marque usurpée.

Voici d'autres conclusions clés du rapport :

- **Le commerce de détail remonte dans les classements des secteurs ciblés :** Le commerce de détail est passé au deuxième rang des secteurs les plus attaqués dans le rapport de cette année, dans une course très serrée avec les services financiers qui sont restés en tête pour la quatrième année consécutive. Les attaques Magecart sont parmi les plus importantes observées contre le commerce de détail, impactant [80 sites de e-commerce](#) à l'été 2019. Les cybercriminels semblent avoir jeté leur dévolu sur les données personnelles des consommateurs, les données des cartes de paiement ainsi que les précieuses informations des programmes de fidélité. Les détaillants ont également été victimes d'un grand nombre d'attaques de type ransomware, d'après les informations fournies par IBM dans le cadre de ses missions de réponse aux incidents.
- **Les attaques des systèmes de contrôle industriel (ICS) et de la technologie d'exploitation (OT) s'envolent :** En 2019, les attaques ciblant les technologies d'exploitation ont augmenté de 2000 % par rapport à l'année précédente, avec davantage d'attaques contre les systèmes de contrôle industriel et les technologies d'exploitation qu'au cours des trois années précédentes. La plupart des attaques observées impliquaient une combinaison de vulnérabilités connues dans le matériel SCADA et ICS ainsi que le password-spraying.
- **Amérique du Nord et Asie - Régions les plus ciblées :** Ces régions ont connu le plus grand nombre d'attaques observées ainsi que les plus grandes pertes de données signalées au cours de l'année passée,

soit plus de 5 milliards et 2 milliards d'enregistrements exposés respectivement.

Le rapport présente des données recueillies par IBM en 2019 pour fournir des informations pertinentes sur le paysage mondial des menaces et informer les professionnels de la sécurité sur les menaces les plus pertinentes pour leurs entreprises. Pour télécharger une copie de l'IBM X-Force Threat Index 2020 : <https://ibm.biz/downloadxforcethreatindex>

Pour vous inscrire au webinaire IBM X-Force Threat Intelligence Index 2020 qui aura lieu le **mardi 18 février 2020 à 17h00** : <https://ibm.biz/BdqExS>

Données France :

La France se situe au 2ème rang du top 20 des pays qui hébergent des réseaux de commande & contrôle de spam.

La France se situe au 7ème rang du top 20 des pays en ce qui concerne les attaques par spam botnet :

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 70 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 IBM Security sur Twitter ou consultez [le blog IBM Security Intelligence](#).

[1] Basé sur une analyse d'IBM des informations disponibles publiquement

Contact(s) relations externes

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

Weber Shandwick pour IBM France

Robin Legros / Morad Salehi Tél. : + 33 (0) 6 68 04 57 83 ibmfrance@webershandwick.com
