Communiqués de presse

Rapport IBM X-FORCE : moins d'enregistrements piratés en 2017, les cybercriminels s'étant concentrés sur les ransomwares et les attaques destructrices

L'erreur humaine responsable des deux tiers des enregistrements compromis, incluant un saut historique de 424% des infrastructures Cloud mal configurées

CAMBRIDGE, MA - 04 avr. 2018: L'entité sécurité d'IBM a annoncé aujourd'hui les résultats de l'indice IBM X-Force Threat Intelligence de 2018 qui a révélé que le nombre d'enregistrements piratés avait chuté de près de 25% en 2017, les cybercriminels s'étant concentrés sur le lancement d'attaques de type ransomwares et d'attaques destructrices qui bloquent ou détruisent les données à moins que la victime ne paye une rançon.

L'année dernière, plus de 2,9 milliards d'enregistrements ont été signalés comme piratés, chiffre en baisse par rapport aux 4 milliards divulgués en 2016. Alors que le nombre d'enregistrements piratés était encore significatif, les ransomwares ont régné en 2017 tandis que des attaques telles que WannaCry, NotPetya et Bad Rabbit ont provoqué le chaos dans toutes les industries sans contribuer au nombre total d'enregistrements compromis signalés.

Les autres principaux constats sont :

- Un saut historique de 424% dans les violations liées à une infrastructure Cloud mal configurée, en grande partie due à une erreur humaine.
- Pour la deuxième année consécutive, l'industrie des services financiers a subi le plus grand nombre de cyber-attaques, représentant 27% des attaques toutes industries confondues.

L'indice IBM X-Force Threat Intelligence comprend des informations et des observations provenant de données analysées via des centaines de millions de terminaux et de serveurs protégés dans près de 100 pays. IBM X-Force exécute des milliers de pièges à spams à travers le monde et surveille quotidiennement des dizaines de millions d'attaques de spam et d'hameçonnage tout en analysant des milliards de pages Web et d'images pour détecter les activités frauduleuses et les abus de marques.

"Alors que les enregistrements piratés sont une bonne indication de l'activité cybercriminelle, ils ne sont pas représentatifs de toute l'année 2017", a déclaré **Wendi Whitmore, Global Lead, IBM X-Force Incident Response and Intelligence Services (IRIS)**. *« L'année dernière, les criminels se sont clairement focalisés sur le verrouillage ou la suppression des données, pas seulement sur leur vol, à travers des attaques de type ransomware. Ces attaques ne sont pas quantifiées dans les enregistrements piratés, mais se sont révélées tout aussi coûteuses, sinon plus, pour les entreprises qu'une violation de données traditionnelle. La capacité à anticiper ces attaques et à se préparer sera critique car les cybercriminels continueront à faire évoluer leurs tactiques vers ce qui s'avère le plus lucratif. »*

Les attaques de type ransomware pèsent sur les réponses aux incidents

Les attaques de type ransomwares et les attaques destructrices, telles queWannaCry, NotPetyaet Bad Rabbit ont non seulement fait les gros titres en 2017, mais ont aussi paralysé les grandes entreprises, les cybercriminels ayant pris le contrôle et verrouillé des infrastructures critiques dans les domaines de la santé, du transport et de la logistique, entre autres. Dans l'ensemble, les incidents de type ransomware ont coûté plus de 8 milliards de dollars1 aux entreprises en 2017, les cybercriminels ayant lancé des attaques extrêmement invalidantes visant à bloquer les données critiques au lieu de compromettre des enregistrements stockés.

Cette tendance augmente la pression sur les entreprises pour qu'elles soient correctement préparées avec des stratégies de réponse aux incidents visant à limiter l'impact d'une attaque.

Selon une étude d'IBM Security réalisée l'année dernière, une réponse lente peut avoir un impact sur le coût d'une attaque, car les incidents qui mettent plus de 30 jours à être contenus coûtent 1 million de dollars de plus que ceux contenus dans les 30 jours.

L'erreur humaine reste un maillon faible

En 2017, les cybercriminels ont continué à profiter des erreurs humaines et des erreurs dans les configurations d'infrastructure pour lancer des attaques. En fait, le rapport montre que des activités involontaires telles qu'une infrastructure Cloud mal configurée étaient responsables de l'exposition de près de 70% des enregistrements compromis identifiés par IBM X-Force en 2017. Le rapport montre que les cybercriminels sont de plus en plus conscients de l'existence de serveurs Cloud mal configurés. Par exemple, l'année 2017 a été marquée par une augmentation incroyable de 424% des enregistrements piratés en raison de mauvaises configurations dans les serveurs Cloud.

Au-delà d'un Cloud mal configuré, les individus touchés par des attaques d'hameçonnage représentaient un tiers des activités par inadvertance ayant conduit à un incident de sécurité en 2017. Ceci comprend les utilisateurs qui cliquent sur un lien ou qui ouvrent une pièce jointe contenant un code malveillant, généralement partagé via une campagne de spams initiée par des cybercriminels. Le rapport a révélé qu'en 2017, les cybercriminels comptaient beaucoup sur le botnet Necurs pour distribuer des millions de spams sur une période de quelques jours dans certains cas. Par exemple, sur une période de deux jours au mois d'août, la recherche IBM X-Force a observé quatre campagnes Necurs distinctes qui spammaient 22 millions d’emails.

Les cybercriminels rencontrent le succès en ciblant les clients des services financiers

Auparavant, les services financiers étaient l'industrie la plus ciblée par les cybercriminels. En 2017, ils sont descendus au troisième rang (17%), derrière les technologies de l'information et des communications (33%) et la production (18%) - pourtant, ils ont subi le plus grand nombre d'incidents de sécurité (27%) - ceux nécessitant une enquête plus poussée - par rapport aux autres industries.

Alors que les organisations de services financiers ont lourdement investi dans les technologies de cybersécurité pour protéger les entreprises, les cybercriminels se sont concentrés sur l'utilisation des chevaux de Troie bancaires ciblant spécifiquement les clients et les utilisateurs finaux de ce secteur.

Par exemple, le rapport IBM X-Force Threat Intelligence Index a révélé qu'en 2017, le cheval de Troie bancaire Gozi et ses variantes était le malware le plus utilisé contre le secteur des services financiers. Le logiciel malveillant Gozi cible spécifiquement les clients car il reprend les écrans de connexion de la banque par défaut aves une invitation aux utilisateurs à entrer d'autres informations personnelles qui sont ensuite partagées directement avec l'attaquant.

L'utilisation de Gozi, considéré comme étant exécuté par une organisation cybercriminelle qualifiée, montre combien le crime organisé dépasse toutes les autres catégories d'acteurs sur la scène de la fraude financière facilitée par les logiciels malveillants.

Le rapport présente les données collectées par IBM entre le 1er janvier 2017 et le 31 décembre 2017 pour fournir des informations pertinentes sur le paysage mondial des menaces et informer les professionnels de la sécurité des menaces les plus susceptibles de toucher leurs entreprises. Pour télécharger une copie de l'Index des menaces IBM X-Force 2018 : https://www.ibm.com/account/reg/us-en/signup?formid=urx-31271

Inscrivez-vous au webinar X-Force Threat Index d'IBM le jeudi 05 avril à 17hhttps://bit.ly/2E2KYSb

A propos d'IBM Security

IBM Security offre l'une des gammes de produits et services de sécurité pour entreprises les plus performantes 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 35 milliards d'évènements de sécurité par jour dans plus de 130 pays, et possède plus de 8000 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.

[1]Cyence/Reinsurance News, Re/insurance to take minimal share of $8 billion WannaCry economic loss:AM Best, May 2017

Contact(s) relations externes

IBM

Gaëlle Dussutour Tél. : + 33 (0)1 58 75 17 96DUSGA@fr.ibm.com

Text100 pour IBM

Nalia Kailali Tél. : + 33 (0)6 59 54 18 32Nalia.Kailali@text100.fr