Communiqués de presse

Rapport IBM X-Force : le ransomware ne s'est pas révélé payant en 2018 pour les cybercriminels - Il faut se tourner vers le cryptojacking pour faire du profit

Le rapport révèle également que plus de la moitié des attaques cybercriminelles se détournent des attaques basées sur les logiciels malveillants ; par contre les campagnes ciblées de compromission d'e-mails commerciaux sont en hausse

CAMBRIDGE, MA - 26 févr. 2019: IBM Security a annoncé aujourd'hui les résultats del'IBM X-Force Threat Intelligence Index annuel 2019, qui a révélé que les mesures de sécurité et la prise de conscience accrues poussent les cybercriminels à modifier leurs techniques en quête d'un meilleur retour sur investissement. En conséquence, le rapport détaille deux changements majeurs, à savoir un détournement surprenant des attaques de type ransomware et une diminution du recours aux logiciels malveillants.

IBM X-Force a noté une baisse significative des ransomwares utilisés dans les attaques. En fait, les chercheurs d'IBM en matière de spams n'ont suivi qu'une seule campagne de ransomware en 2018, celle de Necurs, l'un des plus grands botnets mondial de distribution de spams malveillants. IBM X-Force a également observé que le nombre d'attaques par cryptojacking - l'utilisation illégale de la puissance informatique d'une entreprise ou d'un individu à son insu pour exploiter des crypto-monnaies - était presque le double du montant des attaques par ransomaware en 2018. Avec le prix des crypto-monnaies telles que le Bitcoin qui a atteint un pic à près de 20 000 $ en 2018, les attaques à faible risque et à moindre effort utilisant secrètement la puissance informatique d'une victime étaient considérées comme plus rentables.

L'indice IBM X-Force Threat Intelligence a également révélé que les cybercriminels modifiaient leurs techniques de dissimulation pour réaliser des profits illicites. IBM X-Force a constaté une augmentation de l'utilisation abusive des outils du système d'exploitation, au lieu de l'utilisation de logiciels malveillants. Plus de la moitié des cyberattaques (57%) ont utilisé des applications d'administration courantes comme PowerShell et PsExec pour échapper à la détection, tandis que les attaques de phishing ciblées représentaient près du tiers (29%) des attaques.

L'indice IBM X-Force Threat Intelligence comprend des informations et des observations issues de la gestion de 70 milliards d'événements de sécurité par jour dans plus de 130 pays. En outre, les données sont collectées et analysées à partir de sources multiples, notamment IRIS X-Force, X-Force Red, IBM Managed Security Services et des informations sur les violations de données divulguées publiquement. IBM X-Force exécute également des milliers de pièges à spam dans le monde entier et surveille des dizaines de millions d'attaques de spam et de phishing chaque jour tout en analysant des milliards de pages Web et d'images pour détecter toute activité frauduleuse et tout abus de marque.

Voici d'autres constatations :

- **Rapport de vulnérabilité à la hausse :** Près d'un tiers (42 000) des 140 000 vulnérabilités suivies par IBM X-Force durant les 30 dernières années ont été signalées au cours des trois dernières années. En fait, IBM X-Force Red trouve en moyenne 1 440 vulnérabilités uniques par entreprise.

- **Les erreurs de configuration sont toujours un fléau pour les entreprises :**Le nombre d'incidents de configuration publiquement divulgués a augmenté de 20% d'une année à l'autre. Fait intéressant, le nombre d'enregistrements compromis en raison de ce vecteur de menace a diminué de 52%.
- **Les campagnes de compromission d'emails commerciaux (BEC) continuent de payer les factures :**En matière d'hameçonnage, il a été observé un usage intensif des campagnes de compromission d'emails commerciaux (BEC : Business Email Compromise), qui ont représenté 45% des attaques de hameçonnage suivies par X-Force.
- **Le transport devient une industrie à surveiller (en matière de cyberattaques) :**L'industrie du transport est passée du 10ème secteur le plus attaqué en 2017, au 2ème en 2018.

« Si l'on considère la baisse de l'utilisation des logiciels malveillants, le déclin des ransomwares et l'augmentation des campagnes ciblées, toutes ces tendances nous montrent que le retour sur investissement est un véritable facteur de motivation pour les cybercriminels. Nous constatons que les efforts déployés pour déstabiliser les adversaires et rendre les systèmes plus difficiles à infiltrer fonctionnent. Avec 11,7 milliards d'enregistrements qui ont fait l'objet de fuites ou de vols au cours des trois dernières années, l'exploitation des informations personnelles identifiables (PII) volées à des fins lucratives nécessite davantage de connaissances et de ressources, ce qui incite les pirates à explorer de nouveaux modèles de profits illicites afin d'accroître leur retour sur investissement. », a déclaré **Wendi Whitmore, Global Lead, IBM X-Force Incident Response and Intelligence Services (IRIS)**. *« La puissance informatique associée à l'émergence des crypto-monnaies est l'un des produits les plus en vogue. Cela a conduit à ce que les réseaux d'entreprise et les appareils grand public soient secrètement détournés à des fins d'exploitation pour ces monnaies numériques. »*

Montée en puissance des utilisateurs criminels de PowerShell

La sensibilisation accrue aux questions de cybersécurité et le renforcement des contrôles de sécurité compliquent la tâche des cybercriminels pour s'implanter sur des systèmes cibles. Par conséquent, l'utilisation de logiciels malveillants dans les attaques semble être à la baisse. Plus de la moitié (57%) des attaques analysées par X-Force en 2018 ont révélé que les acteurs de la menace ne s'appuyaient pas sur des logiciels malveillants résidant sur le système. Les principaux utilisateurs de logiciels malveillants sont les grands gangs cybercriminels et les groupes de menace persistante avancée (APT).

Dans les cas où les réseaux ont été compromis par des attaquants, IBM X-Force a vu un changement majeur : les cybercriminels ciblent les outils de système d'exploitation existants au lieu d'utiliser des logiciels malveillants pour atteindre leurs objectifs. Le cœur de ces techniques est l'utilisation avancée de PowerShell, un outil de système d'exploitation intégré capable d'exécuter du code depuis la mémoire et de fournir un accès administratif directement au cœur d'un périphérique. L'équipe IRIS (IBM X-Force Incident Response and Intelligence Services) a également observé des attaquants exécutant des requêtes Windows Management Interface Command (WMIC), qui sont ensuite utilisées pour automatiser l'exécution à distance de commandes et de scripts PowerShell, parmi d'autres fonctions conçues pour exécuter des requêtes, faire des recherches dans bases de données, accéder à des répertoires d'utilisateurs et se connecter à des systèmes présentant un

intérêt.

Les cybercriminels piratent les systèmes pour gagner de l'argent sur le dos des entreprises

Les cybercriminels ne sont pas du genre à dépenser de l'argent en matériel coûteux ou à exploiter légitimement une crypto-monnaie. Au lieu de cela, ils ont développé divers outils et tactiques pour infecter à la fois les serveurs de l'entreprise et les utilisateurs individuels avec des logiciels malveillants d'extraction de pièces afin de leur faciliter la tâche. En retour, ces infections détournent la puissance informatique, ce qui entraîne une utilisation accrue de la CPU et ralentit les périphériques. Cette tendance au cryptojacking est en train d'exploser et les cybercriminels ont l'avantage car deux des vecteurs d'infection les plus courants sont l'hameçonnage et l'injection de code dans des sites Web aux contrôles de sécurité faibles.

IBM X-Force a découvert que les attaques illicites de cryptojacking sont à la hausse tandis que les ransomware semblent être en baisse. Au cours de l'année 2018, les tentatives d'installation de ransomware sur des appareils surveillés par X-Force au quatrième trimestre (octobre-décembre) ont chuté à moins de la moitié (45%) des tentatives au premier trimestre. Au lieu de cela, les attaques de cryptojacking ont plus que quadruplé (450%) au cours de la même période.

L'industrie des transports de plus en plus ciblée par la cybercriminalité

Les cybercriminels ne changent pas seulement la façon dont ils piratent, mais aussi les personnes qu'ils ciblent. L'industrie financière est restée le secteur le plus attaqué en 2018, représentant 19 % de toutes les attaques observées par IBM X-Force IRIS. Cependant, l'industrie du transport - qui ne figurait même pas parmi les cinq premiers l'an dernier - est passée au rang de deuxième secteur le plus attaqué en 2018, les tentatives d'attaques ayant triplé depuis l'année précédente.

Il ne s'agit pas seulement du nombre d'attaques, mais aussi du calibre des victimes. X-Force a observé davantage de divulgations publiques en 2018 qu'au cours des années précédentes dans l'industrie du transport. Ces divulgations ont probablement encouragé les pirates informatiques, car elles peuvent révéler que ces entreprises sont vulnérables aux cyberattaques et qu'elles détiennent des données précieuses telles que les données clients, les informations relatives aux cartes de paiement, les informations personnelles identifiables (PII) et les comptes de fidélité.

Le rapport présente les données recueillies par IBM entre le 1er janvier 2018 et le 31 décembre 2018, 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 entreprises. Pour télécharger une copie de l'index des menaces IBM X-Force 2019 : https://www.ibm.com/security/data-breach/threat-intelligence.

Pour vous inscrire au webinar IBM X-Force Threat Intelligence Index 2019 le vendredi 29 mars 2019 à 16h00 : https://ibm.biz/Bd2VcT

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 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 IBMSecurity sur Twitter ou consultez le blog IBM Security Intelligence.

Contact(s) relations externes

IBM

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

Weber Shandwick pour IBM

Eric Chauvelot / Julie Fontaine Tél. : + 33 (0) 1 47 59 56 57 / + 33 (0) 1 47 59 56 24ibmfrance@webershandwick.com