

IBM X-FORCE révèle un nombre historique de fuites de données et de vulnérabilités déclarées en 2016

Les cybercriminels commencent à récolter d

PARIS - 30 mars 2017: L'entité sécurité d'IBM a annoncé les résultats de l'indice IBM X-Force Threat Intelligence de 2017 qui a révélé que le nombre de données compromises a augmenté de 566 % en 2016, de 600 millions à plus de 4 milliards. Ces fuites d'informations incluent des données que les cybercriminels ont traditionnellement ciblées comme des cartes de crédit, des mots de passe et des renseignements médicaux personnels, mais IBM X-Force a également noté un changement dans les stratégies de cybercriminalité. En 2016, un certain nombre de violations significatives étaient liées aux données non structurées telles que les archives d'emails, les documents commerciaux, la propriété intellectuelle et le code source.

L'indice IBM X-Force Threat Intelligence est composé d'observations émanant de plus de 8000 clients suivis dans le domaine de la sécurité dans 100 pays et de données provenant d'éléments non liés à des clients tels que des capteurs de spam et des « pots de miel » (honeynets) en 2016. IBM X-Force exploite des réseaux-pièges à travers le monde et surveille plus de huit millions d'attaques de spams et d'hameçonnage quotidiennement tout en analysant plus de 37 milliards de pages Web et d'images.

« Les cybercriminels ont continué à innover en 2016. Nous avons vu des techniques comme le ransomware passer d'une nuisance à une épidémie, » a déclaré Caleb Barlow, vice-président de Threat Intelligence, IBM Security. *« Alors que le volume des informations compromises l'année dernière a atteint des sommets historiques, nous voyons l'évolution vers les données non structurées comme une tendance majeure. La valeur des données structurées pour les cybercriminels commence à diminuer à mesure que l'offre dépasse la demande. Les données non structurées sont devenues la cible préférée des pirates et nous nous attendons à les voir les monétiser cette année sous de nouvelles formes. »*

La volonté d'exploitation des Ransomwares a fait augmenter le nombre de spams

Dans une [étude distincte](#) l'an dernier, l'entité sécurité d'IBM a constaté que 70 % des entreprises touchées par le ransomware payaient plus de 10 000 \$ pour récupérer l'accès aux données et aux systèmes de l'entreprise. Au cours des trois premiers mois de 2016, le FBI a estimé que les cybercriminels ont été payés 209 millions de dollars suite aux attaques de type ransomware. Cela mettrait les criminels en bonne voie pour obtenir près d'un milliard de dollars de leur utilisation des logiciels malveillants juste sur l'année dernière.

La promesse de profits et de business a augmenté la volonté de payer les cybercriminels professionnels ce qui a conduit à doubler les attaques de type ransomware en 2016. La principale méthode utilisée pour le ransomware s'opère à travers les pièces jointes malveillantes dans les courriers indésirables. Ceci a généré une augmentation de 400 % des spams année après année avec environ 44 % de spams contenant des pièces jointes malveillantes. Le ransomware représentait 85 % de ces attaques malveillantes en 2016.

Transfert de la santé vers les services financiers

En 2015, la santé représentait le secteur le plus attaqué avec les services financiers à la 3ème place. Cependant, les attaquants en 2016 se sont recentrés sur les services financiers. Alors que ces derniers ont été les plus ciblés par les cyber-attaques l'an dernier, les données de l'indice X-Force montrent qu'ils étaient seulement troisièmes en matière d'informations compromises. Le taux de réussite inférieur au volume élevé d'attaques ciblant les services financiers indique que l'investissement continu dans des pratiques de sécurité durables a probablement aidé à protéger les institutions financières.

L'industrie de la santé a continué à être assaillie par un grand nombre d'incidents, bien que les attaquants se soient concentrés sur des cibles plus petites, ce qui a entraîné un nombre plus faible de fuites de données. En 2016, seuls 12 millions d'enregistrements ont été compromis dans le secteur de la santé - le maintenant hors des 5 industries les plus touchées. [Près de 100 millions](#) de dossiers médicaux ont été compromis en 2015, entraînant une baisse de 88 % en 2016.

Les entreprises de services d'information et de communication ainsi que le gouvernement ont connu le plus grand nombre d'incidents et de violations d'informations en 2016.

- Services d'information et de communication (3,4 milliards d'enregistrements divulgués et 85 violations / incidents)
- Gouvernement (398 millions d'enregistrements et 39 violations / incidents)

Bonne nouvelle pour les stratégies défensives

En moyenne les organisations des clients suivis par IBM ont enregistré plus de 54 millions d'événements de

sécurité en 2016, soit seulement 3 % de plus que 2015. Cela a été marqué par une baisse de 12 % des attaques d'une année à l'autre. À mesure que les systèmes de sécurité se sont améliorés et que de nouvelles innovations, comme les systèmes cognitifs, se sont multipliés, le nombre d'incidents a baissé de 48 % en 2016.

Pour télécharger une copie de l'indice IBM X-Force Threat 2017 : https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-13655&S_PKG=ov57325

A propos de la division sécurité d'IBM

La division sécurité d'IBM propose un portefeuille de solutions de sécurité pour les entreprises parmi les plus avancés et les plus intégrés. Ce portefeuille est supporté par IBM X-Force, organisation de recherche connue mondialement, et permet aux organisations de gérer efficacement les risques et de se défendre contre les menaces émergentes. IBM dispose d'une organisation de recherche et développement et de mise en œuvre parmi les plus importantes au monde, gère 35 milliards d'événements de sécurité par jour dans plus de 130 pays et possède plus de 3 000 brevets de sécurité.

Pour plus d'informations : <http://www.ibm.com/security/fr-fr/>

Blog US : www.securityintelligence.com

Suivez notre actualité sur Twitter @IBMSecurityFR

###

IBM X-FORCE FINDS HISTORIC NUMBER OF RECORDS LEAKED AND VULNERABILITIES DISCLOSED IN 2016

Cybercriminals Begin to Harvest Unstructured Data, Spam Skyrockets 400 Percent as Ransomware Runs Rampant

CAMBRIDGE, MA - March 29, 2017 - IBM Security today announced results from the 2017 IBM X-Force Threat Intelligence Index which found the number of records compromised grew a historic 566 percent in 2016 from 600 million to more than 4 billion. These leaked records include data cybercriminals have traditionally targeted like credit cards, passwords and personal health information, but IBM X-Force also noted a shift in cybercriminal strategies. In 2016, a number of significant breaches related to unstructured data such as email archives, business documents, intellectual property and source code were also compromised.

The IBM X-Force Threat Intelligence Index is comprised of observations from more than 8,000 monitored security clients in 100 countries and data derived from non-customer assets such as spam sensors and honeynets in 2016. IBM X-Force runs network traps around the world and monitors more than eight million spam and phishing attacks daily while analyzing more than 37 billion web pages and images.

"Cybercriminals continued to innovate in 2016 as we saw techniques like ransomware move from a nuisance to an epidemic," said Caleb Barlow, Vice President of Threat Intelligence, IBM Security. "While the volume of records compromised last year reached historic highs, we see this shift to unstructured data as a seminal moment. The value of structured data to cybercriminals is beginning to wane as the supply outstrips the demand. Unstructured data is big-game hunting for hackers and we expect to see them monetize it this year in new ways."

Spam Surges on Back of Ransomware

In a separate [study last year](#), IBM Security found 70 percent of businesses impacted by ransomware paid over \$10,000 to regain access to business data and systems. In the first three months of 2016, the FBI estimated cybercriminals were paid a reported [\\$209 million](#) via ransomware. This would put criminals on pace to make nearly \$1 billion from their use of the malware just last year.

The promise of profits and businesses increasing willingness to pay empowered cybercriminals to double down

on ransomware in 2016. The primary delivery method for ransomware is via malicious attachments in spam emails. This fueled a 400 percent increase in spam year over year with roughly 44 percent of spam containing malicious attachments. Ransomware made up 85% of those malicious attachments in 2016.

Shift from Healthcare back to Financial Services

In 2015, Healthcare was the most attacked industry with Financial Services falling to third, however, attackers in 2016 refocused back on Financial Services. While Financial Services was targeted the most by cyber-attacks last year, data from the X-Force report shows it was only third in compromised records. The lower success rate versus the high volume of attacks in Financial Services indicates that continued investment in sustained security practices likely helped protect financial institutions.

The healthcare industry continued to be beleaguered by a high number of incidents, although attackers focused on smaller targets resulting in a lower number of leaked records. In 2016, only 12 million records were compromised in healthcare - keeping it out of the top 5 most-breached industries. For perspective, [nearly 100 million](#) healthcare records were compromised in 2015 resulting in a 88 percent drop in 2016.

Information & communication services companies and government experienced the highest number of incidents and records breached in 2016.

- Information and Communications (3.4 billion records leaked and 85 breaches/incidents)
- Government (398 million records leaked and 39 breaches/incidents)

Good News for Defensive Strategies

The average IBM monitored security client organization experienced more than 54 million security events in 2016—only three percent more events than 2015. This was marked by a 12 percent decrease year-over-year in attacks. As security systems are further tuned and new innovations like cognitive systems grow, the number of incidents overall dropped 48 percent in 2016.

To download a copy of the 2017 IBM X-Force Threat Index please visit: https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-13655&S_PKG=ov573255

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence [blog](#).

Contact(s) relations externes

IBM

Gaëlle Dussutour 01 58 75 17 96 DUSGA@fr.ibm.com

Text100 for IBM

Amélie Chipaux 06 62 49 20 50 amelie.chipaux@text100.fr
