Cybersécurité : Proofpoint livre ses prédictions pour 2018

Avec des ransomwares comme WannaCry, NotPetya ou encore BadRabbit, l'année 2017 a été marquée par des attaques d'envergure mondiale s'appuyant principalement sur l'exploit EternalBlue.

En 2018, les pirates informatiques et les organisations cybercriminelles vont redoubler d'efforts pour exploiter les failles informatiques et les erreurs humaines. Les techniques et les comportements des cybercriminels vont évoluer. Pour mieux tirer profit de données et de cryptomonnaies volées.

C'est en tout cas le point de vue de Proofpoint. Comme d'autres fournisseurs, l'éditeur américain de logiciels de sécurité publie ses prédictions pour l'année à venir.

La vision de l'éditeur de Sunnyvale (Californie) porte sur quatre points clés :

Propagation en cascade

Hier encore, les cybercriminels privilégiaient l'e-mail ou le téléchargement Web pour lancer des attaques par ransomware. Un changement s'opère depuis 2017.

Pour 2018, les chercheurs de Proofpoint prévoient une généralisation de l'adoption de techniques de propagation d'infections et virus informatiques, basées sur les réseaux. Les logiciels malveillants et les acteurs impliqués seront plus nombreux et variés.

Selon Proofpoint, l'e-mail restera le vecteur de distribution le plus utilisé pour une infection informatique initiale. En revanche, ce sont les vulnérabilités connues et les exploits qui auront fuité qui permettront une propagation rapide. Et ce vers d'autres systèmes et réseaux internes d'entreprises et administrations.

Cryptomonnaies volées

« Les *chevaux de Troie bancaires, les voleurs de données et de cryptomonnaies seront les plus utilisés pour les attaques axées sur le profit. Tandis que les ransomwares, les «* wipers » *et d'autres outils destructeurs seront utilisés pour des campagnes axées sur la perturbation des services* », explique Proofpoint dans un billet de blog.

L'engouement du secteur financier pour les cryptomonnaies aiguise les appétits de hackers et pirates, entre autres. En 2018, le phishing et les logiciels malveillants (malwares) conçus pour dérober les monnaies virtuelles (bitcoin, ether, monero, litecoin…) seront aussi répandus que les chevaux de Troie dans les campagnes d'e-mail.

Humain, « maillon faible »

L'exploitation automatisée de failles de sécurité perdure. Et les attaques exploitant le « *facteur humain* »vont rester une tendance majeure. Par le biais de techniques d'ingénierie sociale (des courriels ayant l'apparence de messages légitimes aux faux profils sur les réseaux sociaux) les pirates informatiques trompent la vigilance d'utilisateurs exposant leurs données, y compris leurs informations bancaires.

Par ailleurs, les attaques perpétrées via les réseaux sociaux se développent. Et les cybercriminels affinent leur approche : création de faux compte, usurpation d'identité de marques, etc.

Ainsi, Proofpoint s'attend à une nouvelle augmentation forte du volume de contenus piratés sur les réseaux sociaux en 2018, après une hausse de 20% en 2017.

Bot tout puissant ?

Pour l'année à venir, les bots représentent un autre moyen de générer des logiciels malveillants ou de créer des liens vers des sites usurpant l'identité de marques. Avec un objectif : soutirer des informations confidentielles et financières aux utilisateurs.

Dans ce système en pleine mutation, il devient plus difficile de distinguer les humains des robots. Les entreprises et les particuliers sont amenés à mieux sécuriser leurs données.

C'est d'autant plus important que l'année 2018 sera marquée par l'entrée en vigueur du nouveau Règlement européen sur la protection des données personnelles (RGPD), le 25 mai prochain.

Lire également :

Sécurité : un marché dopé par les cyberattaques et le RGPD

WannaCry : seulement trois antivirus protègent de l'exploit EternalBlue

crédit photo ©shutterstock