Cybersécurité : le machine learning au top des tendances 2018, selon McAfee

En 2018, l'apprentissage automatique (**machine learning**) devrait être au centre d'une bataille entre cybercriminels et responsables de la sécurité informatique. C'est l'une des cinq grandes tendances qui marqueront le marché de la cybersécurité dans les mois à venir.

McAfee Labs, l'activité de recherche sur les cybermenaces de l'éditeur de logiciels de sécurité, vient de publier son rapport sur le sujet (*McAfee Labs 2018 Threats Predictions Report*).

Le machine learning est une branche de l'intelligence artificielle – IA. Les programmes d'apprentissage automatique peuvent être utilisés par les organisations pour détecter des comportements suspects, corriger des vulnérabilités ou encore faire face aux attaques zero-day, entre autres.

Elles peuvent aussi être utilisées par les pirates pour leurs attaques. En apprenant des réponses défensives, en perturbant les modèles de détection ou en exploitant les vulnérabilités nouvellement découvertes avant que la brèche ne soit colmatée.

Applications « sans serveur »

Les **ransomwares** restent une tendance forte du marché de la cybersécurité. La profitabilité d'attaques *« traditionnelles »* par ransomwares déclinant, selon McAfee Labs, les pirates pourraient se tourner vers de nouvelles cibles, plus rentables. Parmi lesquelles : des individus aux revenus élevés, des objets connectés et leurs utilisateurs, particuliers et entreprises.

Autre tendance : la montée en puissance d'**applications « sans serveur »**. Elles permettent aux entreprises de se libérer de la gestion de serveurs (le service étant entièrement managé par un tiers, un fournisseur Cloud, par exemple). Pour mieux se concentrer sur le développement et l'exécution d'applications, et ne payer que les ressources consacrées à l'exécution du code…

Mais ces applications sans serveur sont vulnérables aux attaques exploitant l'escalade de privilèges et les dépendances applicatives, les données en transit sur le réseau. Avec un risque de déni de service distribué (DDoS).

Objets connectés

McAfee Labs observe, enfin, que les entreprises ne sont pas les seules cibles de choix de cybercriminels. Les particuliers peuvent l'être également.

L'éditeur pointe deux risques : la surveillance à grande échelle de données par des entreprises à des fins marketing, d'une part. Notamment, les données qui transitent par les **objets connectés** équipant de nombreux foyers.

Le traitement et la collecte de **contenus générés par les mineurs**, d'autre part. Un *« bagage*

numérique » qui pourrait bien peser lourd une fois les mineurs devenus adultes.

L'entrée en vigueur, le 25 mai 2018, du Réglement général sur la protection des données (RGPD) pourrait changer la donne en Europe. Toutefois certaines entreprises seraient prêtes à prendre des risques en matière de conformité, voire à payer une amende.

Pour Steve Grobman, chief technology officer (CTO) de McAfee : *« Le machine learning, le deep learning et l'intelligence artificielle sont les piliers de la cyberdéfense de demain. Et nos adversaires travaillent tout aussi ardemment à leur implémentation et usage. Comme c'est souvent le cas en matière de cybersécurité, l'intelligence humaine amplifiée par la technologie sera la clé du succès dans la bataille technologique que se livrent les attaquants et les garants de la sécurité. »*

Lire également :

Sécurité : un marché dopé par les cyberattaques et le RGPD

Sécurité Cloud : McAfee met un pied dans le CASB

crédit photo © Shutterstock.com