Sécurité : la logistique fortement menacée en 2018, selon Kaspersky

La logistique ne sera pas épargnée par les attaques informatiques en 2018. *« Le nombre d'attaques ciblant la chaîne d'approvisionnement est certainement déjà beaucoup plus élevé que ce que nous croyons »* et la tendance devrait se poursuivre, déclare l'éditeur russe Kaspersky dans ses prédictions de sécurité 2018.

Les tierces parties de la chaîne logistique peuvent être des cibles plus faciles à atteindre pour attaquer l'entreprise ciblée initialement, mais mieux protégée que certains de ses partenaires. En 2017, plusieurs cas ont été dénombrés.

La porte dérobée (backdoor) Shadowpad, le programme ayant infecté CCleaner ou encore les rançongiciels et malwares destructeurs Expetr/NotPetya ont fait des dégâts.

Malwares et logistique

L'augmentation des attaques ciblant les terminaux mobiles est une autre tendance forte, prévient Kaspersky.

En plus des spywares tels que Pegasus et Chrysaor – le premier exploitant des failles iOS, le second des vulnérabilités d'Android –, d'autres programmes malveillants sont développés par différents groupes, y compris ceux sponsorisés par des États.

Dans ses prédictions 2018, Kaspersky met également en exergue les attaques exploitant les failles de sécurité XSS (cross-site scripting) des sites web avec le framework de test BeEF (Browser Exploitation Framework) notamment. Parallèlement à la hausse des tarifs promis par des entreprises et d'autres organisations pour la découverte de failles zero day.

L'éditeur prévoit également une hausse des attaques par contamination des microgiciels UEFI (Unified Extensible Firmware Interface) et BIOS (Basic Input Output System). Ces derniers permettent le chargement du système d'exploitation d'un terminal.

Kaspersky alerte aussi ses clients et prospects sur l'augmentation du nombre d'attaques utilisant d'autres malwares destructeurs (Shamoon, StoneDrill ou encore Wannacry…) que ceux cités plus haut.

Backdoors dans l'IoT

Par ailleurs, l'utilisation de portes dérobées (backdoors) dans les systèmes, pare-feux (firewalls) et objets connectés (IoT) reste d'actualité. Et ce dans le but d'exploiter les failles de sécurité dans le chiffrement.

Enfin, les vols massifs d'identifiants et autres données personnelles devraient perdurer. La régulation (RGPD en Europe…) ne suffira pas à endiguer le phénomène. Il menace les individus, et

constitue un défi à fort impact économique pour les entreprises et les gouvernements.

L'augmentation du piratage de modems et routeurs est également à craindre, selon Kaspersky.

Bots et réseaux sociaux

La prolifération dans les réseaux sociaux de faux profils et de bots cherchant à influencer les masses constitue un autre sujet de préoccupation.

« *Malheureusement, les réseaux sociaux – qui basent leur succès sur des critères comme le nombre d'utilisateurs actifs au quodidien – ne sont pas vraiment incités à purger leurs bases de faux utilisateurs et bots* » aux objectifs malveillants, observe Kaspersky dans son bulletin de sécurité.

Lire également :

Sécurité USA : Kaspersky conteste l'interdiction

Sécurité : un marché dopé par les cyberattaques et le RGPD

crédit photo © adike / shutterstock