Sécurité : quand la fraude via les réseaux sociaux menace les entreprises

Les plateformes Web abritent moins de liens d'hameçonnage (phishing). En revanche, la fraude ciblant les utilisateurs des réseaux sociaux (angler phishing) bondit.

C'est ce qu'indique Proofpoint dans un rapport (Quaterly Threat Report Q3 2018). Celui-ci s'appuie sur la base mondiale de clients du fournisseur.

Premier constat : la proportion de liens de phishing repérés sur les réseaux sociaux a chuté de 90% en un an. En revanche, les manipulations psychologiques et les techniques d'ingénierie sociale qui trompent la vigilance d'internautes ont augmenté.

Résultat, la fraude visant les utilisateurs des réseaux sociaux atteint des sommets. Elle a augmenté de 485% au troisième trimestre 2018 par rapport à la même période l'an dernier ! Au risque d'exposer des données sensibles d'entreprises.

Par ailleurs, l'utilisation de code malveillant pour miner des cryptomonnaies (cryptojacking) est également en hausse. Le nombre d'événements détectés au cours des deux trimestres est ainsi environ six fois supérieur à celui du premier trimestre 2018.

À l'inverse, l'utilisation de kits d'exploitation (en anglais Exploit Kit, EK) pour lancer des campagnes malveillantes (malware bancaire, fraude au clic…) se stabilise sur le Web.

Cheval de Troie et RAT

Qu'en est-il de l'email ? Il reste le principal vecteur d'attaques utilisant des programmes malveillants (malwares) ou par hameçonnage.

Au troisième trimestre, le vol et le téléchargement d'informations confidentielles ont ainsi représenté 94% du volume d'emails malveillants. Alors que le ransomware (ou rançongiciel) pèse désormais moins de 1% de ce volume identifié par Proofpoint.

En revanche, l'utilisation de chevaux de Troie pour contrôler à distance les terminaux infectés (RAT ou Remote Administration Tools) a progressé de deux points en un trimestre. Atteignant les 4% durant l'été 2018, selon l'éditeur américain de logiciels de sécurité.

Dans ce contexte, Proofpoint réaffirme l'importance pour les entreprises de sensibiliser leurs équipes au risque que représentent les techniques d'ingénierie sociale. Et d'adopter une protection robuste pour renforcer la sécurité de leurs données et marques.