Sécurité : le phishing se déchaîne sur les réseaux sociaux

Proofpoint a publié son rapport trimestriel sur les menaces cyber qui pèsent sur les entreprises (*Quaterly Threat Report Q1 2018*). Le rapport s'appuie sur l'analyse quotidienne de 5 milliards de courriels. Des centaines de millions de messages sur les réseaux sociaux sont couverts. Et plus de 250 millions d'échantillons de malwares.

L'étude s'appuie sur la base mondiale de clients du fournisseur américain de solutions de sécurité. Proofpoint, après avoir livré ses prédictions pour 2018, confirme la progression de menaces sophistiquées perpétrées via les emails, les médias sociaux et le Web.

Ingénierie sociale

L'utilisation de kits d'exploitation (en anglais Exploit Kit, EK) est en forte progression au T1 2018 (+71% par rapport au T4 2017). Ces boîtes à outils logiciels « clés en main » permettent de lancer des campagnes malveillantes (malware bancaire, ransomware, fraude au clic…). Sans forcément disposer de grandes compétences techniques.

Désormais, 95% des attaques basées sur le Web s'appuient sur des techniques d'ingénierie sociale. Celles-ci permettent de tromper la vigilance de cibles à travers la manipulation psychologique, l'utilisation des réseaux sociaux et d'autres plateformes communautaires.

Justement, la fraude ciblant les utilisateurs des réseaux sociaux (ou « angler phishing ») a bondi au T1 2018. Elle est en augmentation de 200% par rapport au trimestre précédent !

Chevaux de Troie

Plus classiques, les chevaux de Troie ont représenté près de 59% des programmes malveillants dans les courriels. Ils devancent ainsi les ransomwares (rançongiciels) hier encore au sommet du classement des principaux malwares.

C'est donc une première depuis le deuxième trimestre 2016.

Par ailleurs, Proofpoint note que le cheval de Troie bancaire le plus largement distribué a été Emotet. Il a représenté 57% de l'ensemble des « trojans » bancaires identifiés.

Après les trojans et les ransomwares, le vol d'identifiants (19%) et le téléchargement d'informations confidentielles (18%) suivent.

Enfin, 40% des organisations ciblées par des messages frauduleux ont été attaquées entre 10 et 50 fois au premier trimestre 2018. Et le nombre d'entreprises qui ont été la cible de plus de 50 attaques a augmenté de 20% par rapport au dernier trimestre de 2017.