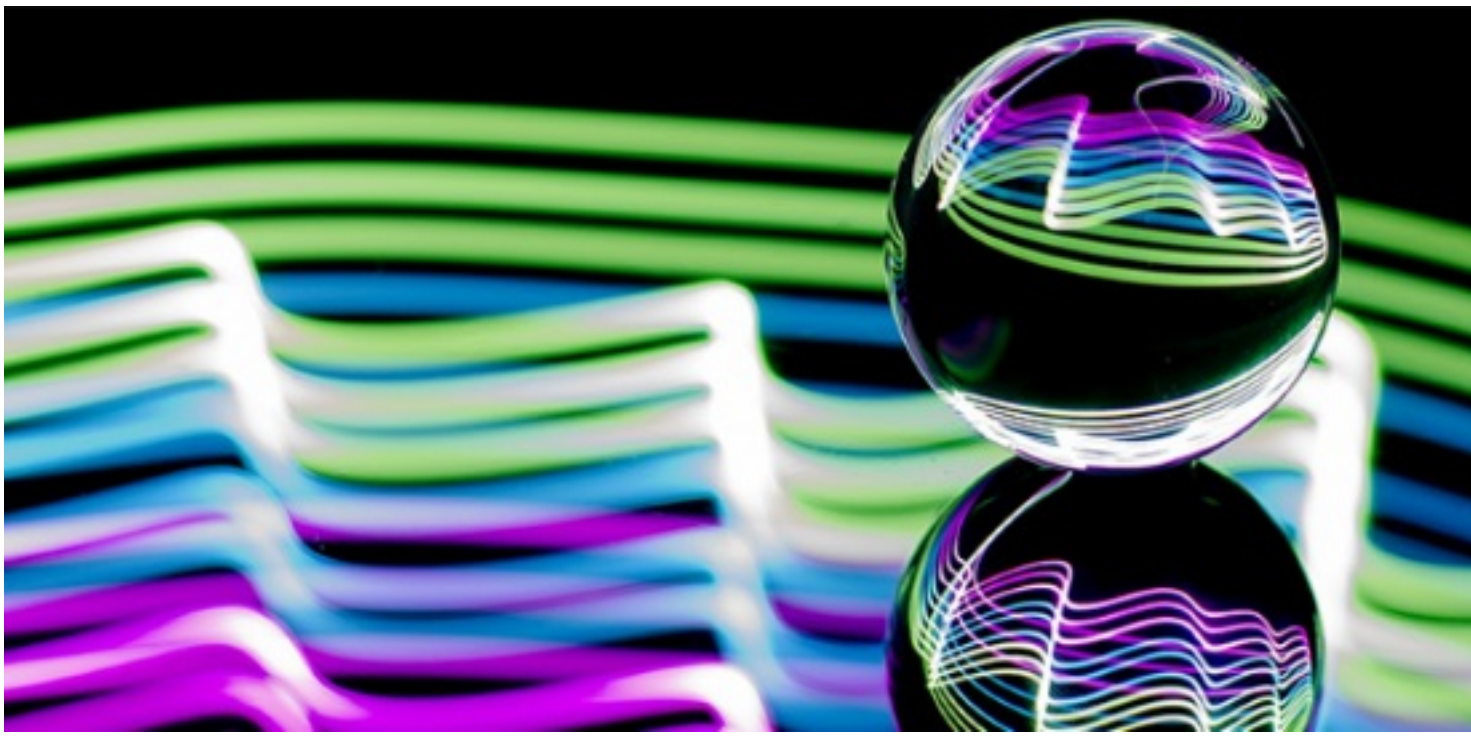
Cyber-criminalitÃ© : les faiblesses humaines exploitÃ©es.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 13/12/2017 13:00:00

En 2018, les cybercriminels vont continuer Ã exploiter les faiblesses inhÃ©rentes Ã la nature humaine pour dÃ©rober des informations personnelles, avec des changements significatifs dans les techniques de cyberattaques. DÃ©couvrez les grandes lignes de ces tendances qui rythmeront lâ□□annÃ©e 2018 selon Proofpoint :

Lâ□□email restera le vecteur de cyberattaque le plus utilisÃ©Â

WannaCry, NotPetya, BadRabbit, l'annÃ©e 2017 a Ã©tÃ© marquÃ©e par des attaques d'envergure Ã l'Ã©chelle mondiale reposant principalement sur une faille de sÃ©curitÃ© nommÃ©e EternalBlue.

Â



Aujourd'hui, mÃªme si cette nouvelle vague de logiciels malveillants rÃ©vÃ¨le de nouveaux schÃ©mas d'attaques (l'exploitation des vulnÃ©rabilitÃ©s d'un rÃ©seau), l'email demeure le principal vecteur avec des campagnes de spam Ã grande Ã©chelle.Â

Pour 2018, les chercheurs de Proofpoint prÃ©voient une propagation de l'exploitation de la faille de sÃ©curitÃ© et des cyberattaques par rÃ©seau, avec cette fois-ci, des techniques plus

sophistiquÃ©es, et une plus grande variÃ©tÃ© de logiciels malveillants et d'acteurs.

Pour autant, l'email reste et restera le vecteur initial de ces contaminations.

Vol de cryptomonnaie : de nouvelles menaces aussi rÃ©pandues que les chevaux de Troie

Pour anticiper les prochaines attaques, il faudra dÃ©sormais suivre les mouvements boursiers ! Avec l'avÃ¨nement des monnaies virtuelles, le vol de cryptomonnaie devient une arme de choix pour les cybercriminels.

En 2018, le phishing et les logiciels malveillants conÃ§us pour dÃ©rober ces monnaies virtuelles deviendront aussi rÃ©pandus que les chevaux de Troie dans les campagnes d'email.Â

Une tendance qui risque de sâ□□intensifier dans la mesure oÃ¹ la plupart des pays ne rÃ¨glementent pas encore ces monnaies virtuelles.

Le facteur humain, toujours au cÅ□ur des cyberattaques

Si les exploitations automatiques de failles de sÃ©curitÃ© logicielles vont et viennent, les attaques exploitant le facteur humain resteront une tendance majeure.Â

MalgrÃ© les mises en garde, de mauvais rÃ©flexes demeurent et les utilisateurs continuent de se faire piÃ©ger en effectuant des virements bancaires directement aux cybercriminels.

Des milliers de cas sont recensÃ©s chaque annÃ©e en raison dâ□□une nÃ©gligence persistante et de techniques toujours plus innovantes. 2018 n'Ã©chappera pas Ã la rÃ¨gle.

La menace grandissante des bots sur les rÃ©seaux sociaux

Depuis quelques annÃ©es, les attaques sur les rÃ©seaux sociaux se sont dÃ©veloppÃ©es et les cybercriminels affinent leur approche : crÃ©ation de faux compte, usurpation dâ□□identitÃ© de marques, etc.Â

Pour lâ□□annÃ©e Ã venir, les bots reprÃ©sentent un nouveau moyen de gÃ©nÃ©rer des logiciels malveillants ou de crÃ©er des liens vers des sites de spams pour soutirer des informations confidentielles et financiÃ¨res aux utilisateurs.

Dans ce systÃ¨me en pleine mutation, il devient de plus en plus difficile de distinguer ces robots des hackers, augmentant ainsi considÃ©rablement le risque de piratage.Â

En 2017, les experts Proopoint ont constatÃ© une augmentation de 20% des contenus piratÃ©s sur les rÃ©seaux sociaux et affirment que cette progression sera constante en 2018.

Toutes ces menaces entraÃ®nent les entreprises et particuliers Ã aller plus loin dans la sÃ©curisation de leurs donnÃ©es. L'adoption de DMARC et d'autres technologies d'authentification des emails a connu une croissance constante au cours des derniÃ¨res annÃ©es mÃªme si certains secteurs sont encore en retard.

Lâ□□annÃ©e 2018 reprÃ©sentera un tournant dÃ©cisif, particuliÃ¨rement avec lâ□□arrivÃ©e du nouveau rÃ¨glement europÃ©en sur la protection des donnÃ©es personnelles (RGPD) le 25 mai prochain. A six mois de son entrÃ©e en vigueur, Proofpoint, a dÃ©voilÃ© les rÃ©sultats de son Ã©tude paneuropÃ©enne (Royaume-Uni, France, Allemagne) analysant le niveau de prÃ©paration des entreprises.

IntitulÃ©e Â« RGPD : entre perception et rÃ©alitÃ© Â», les rÃ©sultats sont sans Ã©quivoque et soulignent un manque de prÃ©paration gÃ©nÃ©rale puisque seules 5% des entreprises auraient effectivement mis en place toutes les stratÃ©gies de gestion de donnÃ©es nÃ©cessaires pour garantir cette mise en conformitÃ©. Les conclusions de cette Ã©tude peuvent Ãªtre tÃ©lÃ©chargÃ©es ici.

Retrouvez tous les dÃ©tails de ces prÃ©visions 2018 sur le blog anglais de ***Proofpoint*** : Threat Insight.