

Forte hausse des applications Android malveillantes



Les applications Android malveillantes et les ransomwares dominent le paysage des menaces au 1er trimestre 2016.

La société Proofpoint a publié son Rapport trimestriel sur les menaces, qui analyse les menaces, les tendances et les transformations observées au sein de notre clientèle et sur le marché de la sécurité dans son ensemble au cours des trois derniers mois. Chaque jour, plus d'un milliard de courriels sont analysés, des centaines de millions de publications sur les réseaux sociaux et plus de 150 millions d'échantillons de malwares afin de protéger les utilisateurs, les données et les marques contre les menaces avancées. On apprend, entre autres, que 98 % des applications mobiles malveillantes examinées au 1er trimestre 2016 ont ciblé des appareils Android. Cela demeure vrai en dépit de la découverte médiatisée d'un cheval de Troie pour iOS et de la présence persistante d'applications iOS ou officieuses dangereuses. Les applications Android malveillantes sont de plus en plus nombreuses.

75 % des attaques de phishing véhiculées par des e-mails imposteurs comportent une adresse «répondre à» usurpée afin de faire croire aux destinataires que l'expéditeur est une personne représentant une autorité. Ce type de menaces est de plus en plus mature et spécialisé, et c'est l'un des principaux ciblant les entreprises aujourd'hui, qui leur auraient coûté 2,6 milliards de dollars au cours des deux dernières années selon les estimations.

Applications Android malveillantes

Les ransomwares se sont hissés aux premiers rangs des malwares privilégiés par les cybercriminels. Au 1er trimestre, 24 % des attaques par e-mail reposant sur des pièces jointes contenaient le nouveau ransomware Locky. Seul le malware Dridex a été plus fréquent.

L'e-mail reste le principal vecteur de menaces : le volume de messages malveillants a fortement augmenté au 1er trimestre 2016, de 66 % par rapport au 4ème trimestre 2015 et de plus de 800 % comparé au 1er trimestre 2015. Dridex représente 74 % des pièces jointes malveillantes.

Chaque grande marque analysée a augmenté ses publications sur les réseaux sociaux d'au moins 30 %. L'accroissement du volume des contenus générés par les marques et leurs fans va de pair avec une accentuation des risques. Les entreprises sont constamment confrontées au défi de protéger la réputation de leurs marques et d'empêcher le spam, la pornographie et un langage grossier de polluer leur message.

Les failles de Java et Flash Player continuent de rapporter gros aux cybercriminels. Angler est le kit d'exploitation de vulnérabilités le plus utilisé, représentant 60 % du trafic total imputable à ce type d'outil. Les kits Neutrino et RIG sont également en progression, respectivement de 86 % et 136 %. (ProofPoint)... [\[Lire la suite\]](#)

Article de Damien BANCAL



Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



[Contactez-nous](#)

Réagissez à cet article

Source : *Forte hausse des applications Android malveillantes – Data Security Breach*