Les cybercriminels ciblent l'humain plutôt que l'IT

Plutôt que d'exploiter les faiblesses des systèmes informatiques, les cybercriminels s'appuient de plus en plus sur les erreurs humaines pour arriver à leurs fins. Proofpoint (fournisseur américain de solutions de sécurité IT) s'appuie depuis plusieurs années sur ce postulat pour élaborer son rapport « The Human Factor », dont l'édition 2016 est riche en enseignements sur l'évolution des menaces.

L'une des grandes tendances se nomme *social engineering*. Les pirates y ont recours pour faire réaliser à leurs cibles des actions auparavant déclenchées via des vulnérabilités logicielles.

En premier lieu, l'exécution de code. Dans ce scénario, l'e-mail est un canal privilégié, tout comme les médias sociaux et les applications mobiles. Les campagnes se déroulent généralement à grande échelle, avec un objectif : convaincre les victimes potentielles d'ouvrir des liens ou des documents, de télécharger des fichiers, de désactiver certaines fonctions de sécurité…

Le volume des campagnes est souvent plus restreint lorsqu'il s'agit de pousser les utilisateurs à fournir des informations telles qu'un identifiant et un mot de passe. Au sommet de la pyramide, il arrive qu'une seule personne soit ciblée dans une entreprise, notamment parce qu'elle est susceptible de transférer des fonds.

S'adapter au rythme de travail des salariés

Pour ce qui est des opérations massives de phishing (des millions de messages envoyés en quelques minutes depuis des milliers de serveurs compromis), elles sont plutôt organisées par régions géographiques que par secteurs d'activité des entreprises visées.

Elles sont surtout adaptées aux rythmes de travail, avec un pic d'envois entre 9 h et 10 h du matin, lorsque l'employé arrive au bureau et avant que l'équipe IT ait eu une chance de détecter la menace.

En 2015 comme en 2014, les pirates préfèrent envoyer leurs e-mails le mardi et plus globalement en première partie de semaine. C'est d'ailleurs sur cet intervalle de temps que les cibles tombent le plus dans le panneau. Même stratégie sur les réseaux sociaux, avec une montée en volume au cours de la matinée et un pic entre 13 h et 14 h, au moment où l'activité « légitime » est au plus haut.

Sur ce canal, les faux comptes au nom de marques sont très fréquemment exploités : 40 % de ceux prétendument ouverts sur Facebook par une société du Fortune 100 sont frauduleux (20 % sur Twitter).

Pour attirer les victimes, on leur propose généralement des cadeaux, des remises ou des points de fidélité. La dimension du service client joue aussi, avec le cas typique de personnes qui disent avoir perdu leur mot de passe. Pour devancer les « véritables » entreprises, les cybercriminels n'hésitent

pas à agir en dehors des heures de bureau.

Le mobile et les apps bureautiques privilégiés

Les applications mobiles constituent un autre vecteur d'attaque. En examinant plusieurs *marketplaces* associées à Android, Proofpoint en a déniché plus de 12 000 (3 000 jeux, 2 200 dans la catégorie divertissement ; 1 000 dans l'éducation ; 400 dans les réseaux sociaux…) réunissant 2 milliards de téléchargements cumulés, précise *ITespresso.fr*.

Les terminaux Apple ne sont pas épargnés : 40 % des entreprises étudiées seraient touchées par au moins une application malveillante issue d'un kiosque tiers pour iOS, comme vShare, découvert en 2015 et qui fonctionne même avec des iPhone non « jailbreakés ».

En ce qui concerne les souches malveillantes liées aux campagnes de phishing avec pièces jointes, il s'agit, dans 74 % des cas, de chevaux de Troie bancaires. Ils se logent dans des macros (77 % de fichiers Word ; 22,5 % d'Excel ; 0,5 % pour le reste, dont PowerPoint et le PDF).

L'exploitation des macros avait nettement diminué depuis leur désactivation par défaut dans Office 2007. Mais les temps changent : grâce au *social engineering*, les pirates parviennent à mettre leurs cibles en confiance. Suffisamment en tout cas pour qu'elles acceptent de réactiver les macros.

Lorsque les e-mails de phishing contiennent une URL malveillante, celle-ci redirige le plus souvent – dans 74 % des cas en l'occurrence – vers de fausses pages de connexion. Les liens les plus cliqués sont ceux qui pointent vers des comptes Dropbox (23 %), Google Drive (22 %) et Adobe (18 %). Suivent Outlook Web Access et PayPal.

Sur la question du phishing ultra-ciblé, les e-mails semblent généralement provenir de hauts responsables de type DG ou directeur financier. Globalement, le phishing fonctionne mieux si l'e-mail a l'air d'être envoyé par un contact présent dans le carnet d'adresses du destinataire.

A lire aussi :

Les responsables IT sont-ils des hackers qui s'ignorent ?

Ingénierie sociale : les employés sont-ils le maillon faible de la cybersécurité ?

Crédit Photo : Ventura-Shutterstock