Divisions RH et comptabilité cibles favorites du phishing en France

On croit connaître toutes (ou presque) les méthodes d'attrape-nigaud des pirates, à commencer par le phishing, l'une des plus courante. Et pourtant… A en croire la nouvelle étude trimestrielle (août 2014) des laboratoires de recherche de MacAfee, **80% des employés de bureau dans le monde continuent à tomber dans les filets des campagnes de phishing**. Un taux qui s'élèverait à **92% en France**. La crédulité humaine reste donc l'un des moyens les plus efficaces pour infiltrer les réseaux des entreprises.

McAfee s'est appuyé sur un quiz (disponible en ligne) d'une dizaine de copies d'e-mail, légitimes ou non, web ou pour mobile, ayant circulé sur le réseau courant 2013, afin de tester la capacité des utilisateurs à déjouer les pièges du hameçonnage. LinkedIn, US Airways, eFax, Venmo, Standard Bank (Afrique du Sud), WellFargo (banque mobile), UPS, Paypal, Amazon, Ebay, American Express… locales ou internationales, **nombre de marques sont exploitées par les cybercriminels pour tromper leurs cibles**.

Les départements comptabilité et RH les moins méfiants

Les résultats sont édifiants, notamment en France. Ainsi, seuls 8% sont parvenus à identifier correctement les emails, à la fois suspects et légitimes. Un sur cinq (21%) ont bien identifié les cas de phishing mais a aussi écarté les courriels légitimes. Un moindre mal. Enfin, **79% se sont trompés au moins une fois** sur les emails de phishing, rapporte McAfee.

Plus inquiétant, pour une majorité d'entreprises en France, les services de comptabilité et des RH s'avèrent les moins méfiants avec des résultats inférieurs de 4 % à 9 % aux autres départements. Ennuyeux quand on sait que ces services ont accès aux données sensibles de l'entreprise. Comparées à l'échelle internationale, **seules 60% des tentatives de phishing sont détectés dans les couloirs des ressources humaines de l'Hexagone** contre 66% dans le reste du monde. Pire, 100% des employés RH français ont manqué au moins une tentative de détournement contre 79% en moyenne dans le reste du monde.

Les étudiants à la pointe de la suspicion

La tendance devrait néanmoins s'améliorer au fil des ans. Les étudiants (stagiaires et futurs salariés) se montrent efficaces à hauteur de 73%. Meilleurs encore que les ingénieurs des laboratoires de R&D (71%).

Il s'agit évidemment de moyennes sur un certain nombre d'entreprises et de tests que McAfee ne précise pas. Difficile de savoir si le résultat est effectivement représentatif de la réalité. En revanche, l'éditeur de solutions de sécurité filiale d'Intel indique avoir relevé **plus de 250□000**

nouvelles adresses Internet (URL) de phishing depuis le précédent rapport du 1er trimestre. Un chiffre comparable d'un trimestre à l'autre mais sensiblement au dessus des 200□000 du 4e trimestre 2013 bien que largement en deçà des plus de 400□000 adresses identifiées fin 2012. Les campagnes de phishing ne semblent donc pas répondre à une logique particulière.

Heartbleed toujours à l'oeuvre

Le reste du rapport de McAfee nous apprend notamment que des outils mis au point à des fins malintentionnées permettant de détecter la faille OpenSSL « Heartbleed » circulent toujours en quête de sites vulnérables afin d'en extraire en clair les données chiffrées. C'est notamment le cas de **Project Un1cOrn** *« qui a de bonnes chance de rester accessible en ligne longtemps encore »*, selon l'éditeur. Lequel a, pour sa part, identifié plus de 2□400 sites toujours faillibles à Heartbleed. Bien loin des 300□000 évoqués par un analyste.

Pour la petite histoire, nous avons obtenu un score de 70% de réussite au quiz des emails de phishing proposé par McAfee. Peut mieux faire. Et vous□?

crédit photo © mtkang – shutterstock

Lire également
Une entreprise sur trois victime du phishing
550 millions de données personnelles dérobées en 2013
Dragonfly : après Stuxnet, nouvelle attaque réussie contre les systèmes Scada