Phishing : SaaS et webmails deviennent les premières cibles

L'Anti-Phishing Working Group (APWG) vient de publier son dernier rapport pour le premier trimestre 2019 qui consacre une nouvelle tendance pour le phishing.

Pour la première fois, la plus grande part (36%) des attaques de ce type ont ciblé des plateformes software as a service (SaaS) et des webmails, devançant la catégorie des services de paiement qui totalise 27 % des attaques enregistrées au cours de la période.

« Les hameçonneurs sont intéressés par le vol de logins vers les sites SaaS parce qu'ils fournissent des données financières et des données sur le personnel, qui peuvent être utilisées pour le spear phishing", analyse Greg Aaron, chargé de recherche principal pour l'APWG.

HTTPS utilisé comme leurre

Le nombre total de sites d'hameçonnage détectés au premier trimestre était de 180.768, ce qui représente une hausse sensible par rapport au quatrième trimestre 2018 (138 328 sites recensés). L'autre enseignement du rapport de l'APWG est la sophistication croissante des attaques par phishing.

Désormais, les cybercriminels ont massivement recours à des sites piégés utilisant le protocole HTTPS afin de tromper plus efficacement leurs victimes en leur faisant croire qu'elles visitent un site digne de confiance.

Selon les statistiques de PhishLabs citées dans le rapport, 58 près de 60% des sites de phishing répertoriés au premier trimestre utilisaient l'HTTPS.

Des techniques de phishing plus sophistiquées

Les techniques de phishing ne cessent de se sophistiquer. Zscaler a récemment relevé cinq nouvelles techniques sophistiquées dites « d'évasion » et d' « anti-analyse ».

– **Accès unique à la page de phishing** : Chaque fois qu'un client visite ces pages de phishing, son adresse IP est vérifiée par rapport à la liste des adresses IP des clients qu'il a visités précédemment. En fonction des résultats de cette vérification, l'accès à la page de phishing est soit accordé, soit un message « Page introuvable » s'affiche, soit le client peut être redirigé vers d'autres sites.

– **Vérification du Proxy à l'aide de services en ligne** : Récemment, de nombreux kits de phishing comprenaient une liste codée d'adresses IP, d'agents utilisateurs et de noms d'hôtes, tous

blacklistés, que les chercheurs en sécurité et les entreprises de sécurité utilisent. Si le client tente de se connecter avec une adresse IP ou un agent utilisateur sur cette liste noire, le contenu de phishing ne sera pas diffusé. Dans certains cas, en plus de la liste des adresses IP codées, l'adresse IP du client est vérifiée à l'aide de certains services en ligne pour déterminer s'il s'agit ou non d'un proxy.

– **Création d'un nouveau répertoire de noms aléatoires à chaque visite** : certaines campagnes de phishing créent systématiquement un nouveau répertoire de noms aléatoires et la page de phishing est hébergée sur ce répertoire aléatoire

– **Création d'un nouveau fichier de noms aléatoires à chaque visite** : Quelques kits de phishing créent un nouveau fichier de noms au hasard à chaque visite, ce qui rend difficile l'identification du site comme étant un site de phishing.

– **Valeurs aléatoires pour les attributs HTML à chaque visit**e : Pour rendre une page de phishing difficile à analyser et à détecter, les valeurs de page des attributs HTML sont générées de manière aléatoire à chaque visite.