Cybersécurité : l'évolution du phishing sur les mobiles

Alors que le hameçonnage ou phishing – technique de piratage qui permet aux hackers de voler les données personnelles des victimes – était jusqu'à présent indépendant du système d'exploitation ou du type d'appareil, on observe désormais une forte augmentation des sites de phishing spécifiques aux appareils mobiles.

Aujourd'hui, la conception d'une attaque par phishing devient de plus en plus facile grâce à des outils et des kits dédiés qui permettent aux hackers, même novices, de déployer des sites trompeurs en quelques clics. Pour autant, sa détection n'a pas progressé et le nombre d'attaques ne cesse d'augmenter.

Bien qu'il existe différents types d'attaques par phishing, ces dernières années le phishing trompeur ciblant spécifiquement les terminaux mobiles est le plus fréquemment utilisé et est devenu de plus en plus sophistiqué et difficile à repérer.

Une attaque par phishing trompeuse, c'est quoi ?

Elle est lancée par des hackers qui créent des sites Web – imitant des marques légitimes et réputées – et trouvent les moyens de détourner la navigation des internautes vers ces sites. Lorsqu'un utilisateur soumet ses informations confidentielles sur le site compromis, l'attaquant est alors en mesure de prendre le contrôle du compte de la victime.

La tendance à réutiliser les mêmes mots de passe sur plusieurs comptes amplifie la gravité de ce type d'attaque et leur propagation. On le sait, un seul mot de passe peut être la clé de tout un royaume des données.

Phishing sur ordinateur VS mobile, quelle différence ?

Le travail hybride a fait du périphérique mobile un élément crucial de la productivité. Il est devenu la norme pour de nombreuses entreprises qui essaient d'adapter leur infrastructure à cette nouvelle donne. Malheureusement, les employés qui travaillent à distance ne disposent pas de la même sécurité qu'au sein de l'entreprise, ce qui expose les données à de nombreuses attaques.

Lorsqu'une attaque par phishing est lancée sur un ordinateur de bureau, l'utilisateur a la possibilité de survoler le lien afin de voir où il redirige et d'éventuellement identifier une URL suspecte ou un expéditeur malveillant. En revanche, sur les écrans des mobiles, plus petits, l'affichage de l'URL n'est pas aussi évident et intuitif, rendant ce type d'attaque beaucoup moins perceptibles.

Aujourd'hui, s'appuyer sur les outils de sécurité existants pour détecter ces menaces de phishing avancées sur les appareils mobiles relève du défi. Les outils de sandboxing couramment utilisés ne

fournissent pas les informations nécessaires à une détection avancée, et les processeurs limitent souvent la capacité d'analyse pour chaque domaine visité. Il est souvent compliqué pour les utilisateurs d'installer et d'adopter des extensions de navigateur en conséquence les solutions de sécurité manquent d'informations.

En effet, si les extensions de navigateur – qui apportent une visibilité globale sur le contenu des sites web comme le html, les liens vers des ressources externes, l'url complète etc… – sont largement utilisées pour repérer les sites de phishing sur les ordinateurs, elles sont en général difficiles à installer sur des navigateurs mobiles.

Quelques exceptions dérogent à la règle – Safari et Firefox ont récemment annoncé cette fonctionnalité – mais la procédure reste plus compliquée que sur un navigateur de bureau, le catalogue d'extensions étant généralement réduit pour les mobiles.

Conscients de la situation, les hackers concentrent leurs efforts sur des attaques par phishing spécifiques au mobile en générant du contenu via deux stratégies: les sites web adaptatifs et réactifs.

L'essor du phishing mobile via les sites web adaptatifs (Adaptative Web Design)

Un site web adaptatif permet aux développeurs de créer plusieurs mises en page d'un même site afin de s'adapter à des dimensions d'écran spécifiques. Pour ce faire, ils vérifient l'agent utilisateur du terminal mobile et permettent au développeur d'afficher un contenu spécifique à certains appareils. Toutefois cela permet également aux sites web malveillants de berner l'attention des analyseurs de trafic de bureau ou de phishing.

Ainsi, sur un ordinateur de bureau, un utilisateur peut être redirigé vers un site leurre ou vers une page d'erreur 404 tandis que sur le mobile, les victimes pourront voir un site de phishing valide, imitant parfaitement un site existant.

Autre exemple intéressant, un utilisateur peut être dirigé vers un site valide, quel que soit l'agent utilisateur, mais être redirigé vers un site de phishing uniquement si le site est accessible via un appareil mobile Android.

Bien que cette technique ait déjà été utilisée dans le passé avec des redirections différentes en fonction du système d'exploitation mobile, il s'agit d'un indicateur fort de l'exploitation d'une vulnérabilité du navigateur.

L'essor du phishing mobile via les sites web réactifs (Responsive Web Design)

Un site web réactif ajuste automatiquement la mise en page en fonction de la taille du navigateur, et non de la taille de l'écran. Au fur et à mesure que la taille du navigateur change, le site réorganise le contenu en conséquence afin de fournir à l'utilisateur une mise en page optimale.

La plupart des frameworks de développement web modernes génèrent du contenu réactif pour une expérience web cohérente sur tous les terminaux. Mais ce framework donne également aux attaquants un sérieux avantage en matière de phishing.

Le phishing mobile par les applications

L'utilisation d'applications compromises et malveillantes est également répandue. Sur des boutiques d'applications tierces ciblant les appareils iOS et Android, ces applications malveillantes utilisent fréquemment la tromperie et un langage intelligent pour manipuler les victimes afin qu'elles les installent sur leurs appareils mobiles.

Une fois l'application installée, l'utilisateur se laisse souvent prendre aux mêmes arnaques que celles trouvées sur les sites de phishing mobile, compromettant ainsi ses données et ses identifiants aux cybercriminels.

Récemment, FlyTrap, une campagne de malwares ciblant les utilisateurs d'Android a été découverte. Bien que cette application ait semblé légitime, elle a fini par voler les informations d'identification Facebook et les cookies de session des victimes pour prendre le contrôle de leurs réseaux sociaux.

La sécurité contre le phishing est essentielle

La détection du phishing est difficile et il n'existe pas de solution universelle. La plupart des systèmes existants s'appuient uniquement sur des crowdsourced lists (ou listes participatives provenant du public) et sur une technologie de sandbox standard. Mais bien que ces approches offrent une couverture décente sur un jour N, la plupart des sites de phishing ne sont actifs que pendant quelques jours.

Et ces systèmes hérités ne protègent en rien contre les attaques de phishing de type « zero day ».
La protection contre les attaques de type « zero day » est essentielle pour les entreprises. Une approche basée sur les listes de blocage est susceptible de protéger contre les campagnes à large cible, mais si une organisation est directement visée par une campagne de spear-phishing, les sites utilisés ne figureront sur aucune liste.

La plupart des solutions de phishing mobile existantes utilisent des services dans le cloud pour identifier les sites comme malveillants ou légitimes. Bien qu'efficace, il y a toujours un délai dans la classification, or la quantité limitée de traitement qui peut être effectuée sur chaque est une aubaine pour les attaquants. Ces couches de consultation se sont avérées simples à contourner par un hacker.

Selon une récente étude, sur 500 000 sites de phishing analysés, ceux étant spécifiques aux mobiles ont augmenté de 50%. Par ailleurs, courant 2021, 75% des sites de phishing analysés ciblaient spécifiquement les appareils mobiles[1].

Aux entreprises d'être vigilantes à l'avenir et de sécuriser pleinement leur environnement mobile avec des solutions alimentées par le machine learning, fournissant une sécurité sur l'appareil et

capable de détecter les attaques de type « zero day », même lorsque l'appareil n'est pas connecté à un réseau.

[1] *Source : Zimperium*