Devolutions

Hameçonnage : pourquoi le phénomène s'aggrave et comment le combattre

LA TECHNOLOGIE N'EST PAS LA SEULE CHOSE QUI ÉVOLUE ET QUI CHANGE NOS VIES

Récemment, mon collègue Marc-Olivier s'est penché sur les tendances TI de 2021. Malheureusement, la technologie n'est pas la seule chose qui évolue et qui change nos vies : les cybermenaces progressent pour nous compliquer la vie. Et un des exemples les plus terrifiants, c'est l'hameçonnage.

Évidemment, l'hameçonnage n'est pas un phénomène nouveau. En fait, il remonte à 1996. Alors que de nombreuses tendances apparues à l'époque ont depuis longtemps été reléguées aux oubliettes, l'hameçonnage n'a pas seulement survécu, mais il a connu une véritable explosion. Considérez ce qui suit :

- Près de 1,5 million de nouveaux sites d'hameçonnage sont créés chaque mois.
- Les attaques par hameçonnage ont représenté plus de 80 % des incidents de sécurité signalés en 2020.
- L'hameçonnage était le type de cybercriminalité le plus courant en 2020.
- Une analyse de plus de 55 millions de courriels montre qu'un courriel sur 99 est une attaque par hameçonnage.

Et ceux qui pensaient – ou peut-être qui espéraient – que les pirates allaient ralentir la cadence pendant la pandémie ont été déçus. Ils ont plutôt accéléré leurs attaques. Par exemple, en avril 2020, Google a bloqué un nombre impressionnant de 18 millions de logiciels malveillants et de courriels d'hameçonnage liés à la COVID-19. Et tout au long de la pandémie, des pirates informatiques aux États-Unis, au Canada, au Royaume-Uni et ailleurs se sont fait passer pour des organismes gouvernementaux et prétendaient offrir une aide financière et des informations sur les vaccinations et les thérapies liées à la pandémie (et continuent de le faire).

C'est vrai que de nos jours, de nombreuses tentatives d'hameçonnage ne sont pas seulement flagrantes, mais elles sont souvent (involontairement) ridicules. En effet, il suffit de jeter un coup d'œil à nos dossiers de pourriels pour voir des tentatives vraiment pathétiques de vol de nos informations personnelles. Évidemment, nous n'avons pas à nous inquiéter de ces tentatives. Alors, pourquoi les experts en cybersécurité sont-ils de plus en plus préoccupés par l'hameçonnage? Parce que toutes les tentatives d'hameçonnage ne sont pas faibles et donc facilement évitables. Certaines sont étonnamment subtiles et sophistiquées, par exemple :

- Hameçonnage polymorphe
- Hameçonnage qui utilise des sites HTTPS
- Hameçonnage en tant que service
- Hébergement de pages de renvoi d'hameçonnage sur des services infonuagiques publics
- Hameçonnage qui utilise des noms de domaine avec des fautes de frappe
- Hameçonnage utilisant des fonds de page d'envoi inversés

Examinons de plus près chacune de ces innovations et voyons pourquoi elles sont vraiment préoccupantes :

Hameçonnage polymorphe

Les outils de sécurité de courriels basés sur la signature analysent les éléments du courriel comme le nom et l'adresse de l'expéditeur, l'objet, le corps et la signature. Ils les comparent ensuite à une base de données de

campagnes d'hameçonnage connues. Si une correspondance est trouvée, le courriel est bloqué, signalé ou transféré vers un dossier pourriel (en fonction de la configuration de l'outil).

Pensez-y comme à un groupe de policiers qui a une photo exacte d'un criminel recherché. Tôt ou tard, les agents vont croiser le criminel et l'arrêter. Mais que se passe-t-il si ce criminel modifie son apparence? Il pourrait échapper à toute détection. C'est essentiellement ce que tente de faire l'hameçonnage polymorphe.

L'hameçonnage polymorphe modifie légèrement un élément du courriel qui est examiné par les outils de sécurité basés sur les signatures, dans le but de passer entre les mailles du filet et d'atteindre finalement les victimes. Par exemple, si l'outil est à l'affût d'un contenu spécifique dans le corps d'un courriel, les pirates le modifieront juste assez pour que l'outil ne tire pas la sonnette d'alarme et ne claque pas la porte.

En général, les attaques d'hameçonnage polymorphes commencent de manière assez modeste et ciblent un petit groupe d'employés. Une fois qu'un employé est accroché, c'est-à-dire qu'il considère par erreur le courriel comme légitime (souvent en cliquant sur un lien qui l'amène à une page de connexion bidon), les pirates utilisent cet accès pour lancer des attaques d'hameçonnage polymorphe plus larges contre d'autres employés du même réseau.

Ce qui rend l'hameçonnage polymorphe particulièrement sournois et trompeur, c'est qu'une fois les attaques lancées, les comptes compromis ne peuvent pas être mis sur une liste noire, parce qu'ils proviennent tous de la même organisation. Et plus le nombre de comptes compromis augmente, plus il devient difficile de contenir ce type d'attaque.

Hameçonnage qui utilise des sites HTTPS

Les pirates utilisent également de plus en plus les sites HTTPS pour mener des attaques d'hameçonnage. La logique sous-jacente est simple : de nombreux utilisateurs supposent automatiquement, lorsqu'ils voient la petite icône de verrouillage dans la barre d'adresse de leur navigateur, que le message qu'ils reçoivent est fiable et sûr.

Ce que ces utilisateurs ne comprennent pas, c'est qu'il existe toutes sortes de services de certification gratuits qui accordent un label de confiance à un site Web. De plus, les navigateurs actuels considèrent tous les sites HTTPS comme sûrs sans effectuer de vérification supplémentaire. Alors que les professionnels de l'informatique et de l'InfoSec savent qu'il existe tout un spectre de « sécurité » – allant d'un niveau de sécurité faible à un niveau de sécurité élevé – la plupart des utilisateurs non techniques considèrent cette notion comme binaire : soit un site est sécurisé, soit il ne l'est pas. Et s'il a un petit cadenas, c'est qu'il est entièrement sécurisé.

Malheureusement, les pirates profitent de cette mauvaise perception. Selon le rapport ENISA Threat Landscape 2020, 74 % des sites d'hameçonnage ont adopté le HTTPS au cours du dernier trimestre de 2020. Et si ce n'était

pas une raison suffisante pour s'inquiéter, les pirates utilisent également des sites légitimes qui ont été compromis pour héberger des pages d'hameçonnage, ce qui rend encore plus difficile la détection des activités malveillantes.

Hameçonnage en tant que service

Nous avons entendu parler du logiciel en tant que service (parfois mieux connu sous l'appellation en anglais de ***software-as-a-service*** ou SaaS), d'infrastructure en tant que service et de plateforme en tant que service. Eh bien, faites maintenant place à l'hameçonnage en tant que service (ou PhaaS pour phishing-as-a-service).

Désormais, les pirates peuvent s'abonner à des kits PhaaS sur le dark Web à des prix allant de 50 $/mois à 100 $/mois (US). Il y aurait plus de 5 000 kits PhaaS disponibles et la plupart d'entre eux comprennent un ou plusieurs mécanismes d'évasion comme le codage des caractères HTML, le chiffrement du contenu, le blocage des inspections, les URL dans les pièces jointes, l'injection de contenu et l'hébergement légitime dans le nuage (que nous examinons dans la section suivante). Voici ce qu'a déclaré Cyren, fournisseur de services de sécurité, qui a mené des recherches approfondies sur ce type d'hameçonnage :

On peut tracer une ligne droite entre la disponibilité de ces kits et plateformes d'hameçonnage clés en main et la croissance des attaques d'hameçonnage évasif, soit des attaques d'hameçonnage qui utilisent des tactiques pour confondre la détection des systèmes de sécurité du courriel. La réalité d'aujourd'hui est que nous voyons davantage de campagnes d'hameçonnage évasif entre les mains d'un plus grand nombre d'attaquants, avec moins d'efforts et à moindre coût que par le passé, car les développeurs d'attaques d'hameçonnage techniquement sophistiquées ont adopté un modèle commercial SaaS pour permettre même au criminel le plus amateur d'usurper des sites Web ciblés avec un haut degré d'authenticité et des tactiques d'évasion intégrées.

Hébergement de pages de renvoi d'hameçonnage sur des services infonuagiques publics

Les entreprises ne sont pas les seules à utiliser le nuage pour étendre leur empreinte et concrétiser leur vision : les pirates informatiques utilisent le même mode opératoire innovant pour mener des attaques d'hameçonnage.

Par exemple, en 2020, des pirates avaient exploité l'infrastructure des services infonuagiques publics d'Amazon et d'Oracle pour héberger de fausses pages de renvoi. Ils ont utilisé des comptes compromis pour cibler les utilisateurs d'Office 365 – principalement des cadres de niveau C dans des PME – avec de fausses notifications de messages vocaux et d'annonces Zoom. Lorsqu'un utilisateur peu méfiant cliquait sur le lien du courriel, il était redirigé par plusieurs proxys, dont des équilibreurs de charge AWS, vers un site Web légitime, mais compromis.

Et ce n'est pas tout : les pirates ont également la capacité de détecter les connexions entrantes provenant d'un environnement ***sandbox*** (une machine virtuelle isolée dans laquelle un code logiciel potentiellement dangereux peut s'exécuter sans affecter les applications locales ou les ressources réseau). Si elle est détectée, la connexion est automatiquement redirigée vers un site légitime et, de ce fait, la sonnette d'alarme ne se déclenche pas.

Hameçonnage qui utilise des noms de domaine avec des fautes de frappe

Une autre technique d'hameçonnage avancée consiste à utiliser des noms de domaine contenant une coquille (également connue sous le nom de typosquattage). Les pirates exploitent la ressemblance des scripts de caractères pour construire et enregistrer de faux noms de domaine qui ressemblent beaucoup à la version originale et authentique.

Par exemple, les pirates ont créé un faux site Web Adobe.com qui utilisait la petite lettre latine b avec un point en dessous (code hexadécimal Unicode : U+1E05) au lieu de la lettre b normale (code hexadécimal : U+0062). Les pirates ont aussi fait le site HTTPS (une tactique de plus en plus populaire, comme nous l'avons vu précédemment). Au lieu de télécharger le fichier d'installation d'Adobe Flash Player, les utilisateurs ont reçu le cheval de Troie Beta Bot.

En plus, les chercheurs ont constaté que certaines attaques de typosquattage avaient été injectées à l'aide d'un chargeur inoffensif pour un fichier d'icône. Ce dernier chargeait une version copiée de la favicône du domaine frauduleux, ce qui permettait finalement aux pirates d'utiliser le skimmer Javascript connu sous le nom d'Inter.

Hameçonnage utilisant des fonds de page de renvoi inversés

Une technique d'hameçonnage plus récente consiste à inverser les images qui servent d'arrière-plan aux pages de destination. Pourquoi les pirates font-ils ça? Parce que c'est un moyen créatif d'éviter la détection des pages de destination comme suspectes ou malveillantes par les différents outils de sécurité qui analysent le Web à la recherche de sites d'hameçonnage. Comme le souligne la société de cybersécurité WMC Global :

Alors que les logiciels de reconnaissance d'images s'améliorent et deviennent plus précis, cette nouvelle technique vise à tromper les moteurs de balayage en inversant les couleurs de l'image, ce qui fait que le hachage de l'image diffère de l'original. Cette technique peut entraver la capacité du logiciel à signaler cette image.

Combattre l'hameçonnage

Il n'existe pas de solution miracle permettant d'éliminer à 100 % l'hameçonnage. Tant qu'il y aura des communications numériques d'un type ou d'un autre, il y aura des pirates qui tenteront d'exploiter ces canaux pour voler des informations privées, confidentielles et exclusives.

Il existe cependant des mesures pratiques et stratégiques que les organisations peuvent mettre en place – et, compte tenu des enjeux et des impacts potentiels, doivent mettre en place plus tôt que tard :

- Formez les employés à la détection des courriels malveillants. Une façon de soutenir cet objectif est d'organiser des campagnes d'hameçonnage simulées – qui peuvent donner des résultats surprenants (dans le sens d'inquiétant et d'excitant). Par exemple, en 2020, 14 % des travailleurs de l'assurance ont échoué à ce genre de test.
- Exigez de tous les employés qu'ils choisissent des mots de passe forts et uniques pour leurs comptes. L'utilisation d'un gestionnaire de mots de passe réputé est fortement recommandée.
- Mettez en place ou renforcez votre système d'authentification multifacteur pour réduire le risque de prise de contrôle des comptes.
- Mettez en place une passerelle de courriel sécurisée qui automatise le filtrage antipourriel, anti-logiciels malveillants et basés sur des politiques (remarque : comme nous l'avons vu plus haut, ces outils ne garantissent pas l'arrêt de toutes les tentatives d'hameçonnage avancées, mais ils constituent néanmoins une pièce importante du casse-tête).
- Pour augmenter la capacité d'identification et de blocage des pourriels, mettez en place un SPF (*Sender Policy Framework*), DMARC (*Domain-based Message Authentication, Reporting & Conformance*) et DKIM (*Domain Keys Identified Mail*).
- Détectez les anomalies au niveau du réseau pour les courriels entrants et sortants.

En résumé

L'hameçonnage a évolué de façon spectaculaire au cours du dernier quart de siècle. Les pirates ont amélioré leur jeu, parce que la valeur des données volées n'a jamais été aussi grande. En fait, les cybercriminels de haut niveau peuvent gagner environ 2 millions de dollars US par année, ce qui les place au même niveau que les PDG les mieux payés.

Pour éviter d'être victimes d'hameçonnage, les utilisateurs individuels et les organisations dans leur ensemble doivent être éduqués, vigilants et équipés de technologies avancées. Non, ça n'éliminera pas complètement l'hameçonnage. Mais ça rendra le lac dans lequel les pirates pêchent beaucoup moins profond.