

La nouvelle génération d'attaques de phishing aux méthodes inattendues.
Internet

Posté par : JulieM

Publié le : 4/11/2022 13:00:00

Un rapport sur les menaces révèle les nouvelles sources principales de renvois vers de fausses pages de connexion, ainsi que l'augmentation des fausses applications cloud tierces exploitées pour tromper les utilisateurs.

Netskope, un leader du SASE (Secure Access Service Edge), dévoile aujourd'hui une nouvelle étude qui montre comment la prédominance des applications cloud a changé la façon dont les cybercriminels livrent les attaques de phishing pour voler des données.

Le rapport « Netskope Cloud and Threat Report: Phishing » détaille les tendances relatives aux méthodes de diffusion du phishing, telles que les fausses pages de connexion et applications cloud tierces conçues pour imiter les versions légitimes. Il analyse également les cibles de ce type d'attaques ainsi que l'hébergement des contenus frauduleux.

Bien que l'email reste le principal moyen d'acheminer des liens de phishing vers de fausses pages de connexion dans le but de voler des noms d'utilisateur, des mots de passe ou encore des codes d'authentification multifactor, le rapport révèle que les utilisateurs cliquent plus fréquemment sur des liens de phishing provenant d'autres canaux, notamment des sites internet et des blogs, des médias sociaux et des résultats de moteurs de recherche.

Le rapport décrit également l'augmentation du nombre de fausses applications cloud tierces conçues pour inciter les utilisateurs à autoriser l'accès à leurs données et à leurs ressources dans le cloud.

Les nombreuses origines du phishing

Traditionnellement considérée comme la principale menace de phishing, seules 11 % des tentatives d'attaques proviennent de services de messagerie Web, tels que Gmail, Microsoft Live et Yahoo.

Les sites Internet et les blogs, en particulier ceux hébergés sur des services gratuits, sont les sources les plus courantes en matière de phishing, avec 26 %.

Le rapport a identifié deux techniques principales : l'utilisation de liens malveillants par le biais de spams sur des sites web et des blogs légitimes, et l'exploitation de sites internet et de blogs créés spécifiquement pour promouvoir le contenu frauduleux.

Les renvois de moteurs de recherche vers des pages de phishing sont également devenus courants, car les cybercriminels exploitent les vides de données.

Ainsi, ils créent des pages centrées sur des termes de recherche peu courants et sur lesquelles ils peuvent facilement s'imposer dans les premiers résultats pour ces termes.

Parmi les exemples identifiés par le Threat Labs de Netskope dans l'exploitation de cette technique, figurent le mode d'emploi de fonctionnalités spécifiques de logiciels connus, les réponses à des questionnaires pour des cours en ligne ou encore les manuels d'utilisation de divers produits pour les entreprises et les particuliers.

« Les employés des entreprises ont été formés à repérer les messages de phishing dans les emails et les SMS. »

Les cybercriminels ont donc adapté leurs méthodes et incitent les utilisateurs à cliquer sur des liens de phishing dans des endroits moins attendus, explique Ray Canzanese, Threat Research Director du Threat Labs de Netskope.

Même si nous ne pensons pas forcément à la possibilité d'une attaque de phishing en surfant sur Internet ou sur notre moteur de recherche préféré, nous devons tous faire preuve du même niveau de vigilance et de scepticisme qu'avec les emails entrants. »

Cela suppose de ne jamais saisir d'informations d'identification ou de données sensibles dans une page après avoir cliqué sur un lien. Il faut toujours se rendre directement sur les pages de connexion. »

La montée en puissance des fausses applications Cloud tierces

Le rapport de Netskope révèle une autre méthode de phishing importante, qui consiste à inciter les utilisateurs à autoriser l'accès à leurs données et leurs ressources dans le cloud par le biais de fausses applications cloud tierces.

Cette tendance est particulièrement inquiétante car l'accès aux applications tierces est omniprésent et constitue une surface d'attaque considérable. »

En moyenne, les utilisateurs finaux des entreprises ont accordé à plus de 440 applications tierces l'accès à leurs données et applications Google, avec une entreprise ayant jusqu'à 12 300 plug-ins différents accordant aux données, soit une moyenne de 16 plug-ins par utilisateur.

Tout aussi alarmant, plus de 44 % de toutes les applications tierces accordant à Google Drive ont accès soit à des données sensibles, soit à toutes les données de Google Drive d'un utilisateur, ce qui incite les cybercriminels à créer de fausses applications tierces pour le cloud.

« La nouvelle génération d'attaques de phishing est à nos portes. Avec la prédominance des applications cloud et l'évolution de la nature de leur utilisation, des extensions Chrome ou d'applications, les utilisateurs sont invités à autoriser l'accès dans ce qui est devenu un vecteur d'attaque négligé, ajoute Ray Canzanese.

Cette nouvelle tendance des fausses applications tierces est un phénomène que nous surveillons et suivons de près pour nos clients. Nous nous attendons à ce que ces types d'attaques augmentent au fil du temps.

Les entreprises doivent donc s'assurer que les nouvelles voies exploitées, telles que les autorisations OAuth, sont limitées ou verrouillées. »

Les employés doivent également être conscients de ces attaques et examiner minutieusement les demandes d'autorisation de la même manière qu'ils examinent les emails et les SMS. »

Dans son rapport, le Threat Labs de Netskope présente des mesures concrètes que les entreprises peuvent prendre pour identifier et contrôler l'accès aux sites ou aux applications de phishing. »

L'adoption du modèle Secure Service Edge (SSE) avec une passerelle web sécurisée (SWG), l'activation du principe zero trust pour un accès aux données avec le moindre privilège et une surveillance continue, et l'utilisation de l'isolation du navigateur à distance (RBI) pour réduire le

risque de navigation pour les domaines nouvellement enregistrés font partie des principales mesures.

Les autres conclusions clés du rapport sont les suivantes :

Les employés continuent à cliquer et à être victimes de liens malveillants. Il est largement admis qu'il suffit d'un seul clic pour compromettre gravement une organisation.

Alors que la sensibilisation et la formation des entreprises au phishing ne cessent de gagner en importance, le rapport révèle qu'en moyenne 8 utilisateurs sur 1 000 dans l'entreprise ont cliqué sur un lien de phishing ou ont tenté d'accéder d'une autre manière à un contenu de phishing.

Les utilisateurs sont attirés par de faux sites Internet conçus pour imiter les pages de connexion légitimes. Les cybercriminels hébergent principalement ces sites internet sur des serveurs de contenu (22 %), suivis par des domaines nouvellement enregistrés (17 %).

Une fois que les utilisateurs ont entré des informations personnelles sur un faux site, ou lui ont accordé l'accès à leurs données, les cybercriminels sont en mesure de collecter les noms d'utilisateur, les mots de passe et les codes d'authentification multifacteur.

La situation géographique joue un rôle dans le taux d'accès au phishing. L'Afrique et le Moyen-Orient présentent le pourcentage le plus élevé d'utilisateurs accédant à des contenus de phishing; en Afrique ce taux est supérieur de plus de 33 % à la moyenne, et il est plus de deux fois supérieur à la moyenne au Moyen-Orient.

Les cybercriminels utilisent fréquemment la peur, l'incertitude et le doute (FUD) pour mettre au point des appâts de phishing et tentent également de tirer parti des grands sujets d'actualité. Au Moyen-Orient en particulier, ils semblent réussir à concevoir des leurres qui tirent parti des problèmes politiques, sociaux et économiques de la région.

Netskope fournit une protection contre les menaces et les données à des millions d'utilisateurs dans le monde.

Les informations présentées dans ce rapport sont basées sur des données d'utilisation anonymisées, collectées par la plateforme [Netskope Security Cloud](#), relatives à un sous-ensemble de clients Netskope ayant reçu une autorisation préalable.

Les statistiques présentées dans ce rapport sont basées sur la période de trois mois, allant du 1er juillet 2022 au 30 septembre 2022.