RICHARD Ulysse
GUICHARD Clément
BAWOL Mathis

Phishing

De nos jours, les attaques informatiques sont de plus en plus fréquentes. Dans le monde actuel, l'informatique se développe de plus en plus. De nombreuses techniques d'attaques sont mis au point chaque jour, dans le but de contrer les protections mis en place par l'utilisateur et ainsi obtenir des informations confidentielles en les piratant. L'une des attaques la plus fréquente est le Phishing ou hameçonnage en français. Elle est facile d'utilisation et permet de récolter beaucoup d'informations. En effet, le phishing est une technique de fraude visant à inciter les internautes à fournir des données personnelles (comptes d'accès, mots de passe, etc.) et/ou bancaires en se faisant passer pour un tiers de confiance. Cette technique implique l'utilisation de leurres par les fraudeurs et à vue le jour au début des années 90. L'un des premiers cas de phishing s'est déroulé en 1996 quand des hackers ont attaqués des utilisateurs d'AOL (American online), en leurs envoyant des messages et ainsi obtenir des informations confidentielles. Depuis ce jour, les attaques de phishing ont connu une croissance grandissante.

Quels sont les menaces du phishing et comment s'en protéger ?

L'hameçonnage par clonage est une technique employée par les escrocs pour créer des sites internet ou des pages de connexion frauduleuses. Ces pages sont minutieusement conçues pour imiter l'apparence et le fonctionnement de sites Web connus tels que des banques, des réseaux sociaux ou des services de messagerie. Lorsqu'un utilisateur reçoit un mail contenant un lien vers l'une de ces pages de clonage, le mail peut sembler provenir d'une source de confiance. Malheureusement, si l'utilisateur clique sur ce lien, il est redirigé vers la page de clonage. Là, il est invité à se connecter en utilisant ses identifiants et mots de passe habituels. Une fois que l'utilisateur a naïvement saisi ses informations, le pirate obtient toutes les informations de connexions et ainsi, il a accès à toutes les données sensibles de l'utilisateur sur le site officiel.

Cette pratique peut entraîner de graves conséquences, y compris le vol d'identité et la perte financière. Il est essentiel de rester vigilant et de vérifier attentivement la fiabilité des sites Web que vous visitez, ainsi que des mails et des liens que vous recevez, afin de vous protéger contre ce type d'arnaque en ligne.

L'hameçonnage téléphonique ou vishing (Voice et phishing) est une technique d'attaque par téléphone utilisé par les pirates pour obtenir des informations confidentielles tels que des coordonnées bancaires. Les escrocs jouent sur la culpabilité des victimes à leur fin et ainsi obtenir les informations souhaitées. Les informations les plus demandées sont principalement, les numéros de carte de crédit, les numéros de sécurité sociale, les mots de passe et d'autres données personnelles. Pour se faire les pirates sont font passer pour des institutions connues tels qu'une banque, une entreprise, une association… Pour faire apparaitre un numéro de téléphone crédible, les hackers utilisent du spoofing ou usurpation en français, ainsi la victime tombe dans le piège et décroche. Une fois cette étape réalisée, les pirates racontent des histoires crédibles et insiste pour donner l'impression d'urgence et ainsi la victime agit au plus vite pour résoudre le problème. Dans ces histoires, les pirates prétendent qu'il y a un problème avec le compte en banque ou la carte de crédit, du répondant.

De plus, les pirates peuvent utilisés la détresse des personnes pour atteindre leur but. Ainsi, ils peuvent demander de confirmer des informations personnelles ou dans le pire des cas, ils demandent un virement pour résoudre le problème.

Une attaque connue et très rependue, est l'anarque nigériane ou anarque 419, qui tient son nom directement du code pénal du Nigéria, de l'article 419. La technique utilisé par l'attaquant implique un attaquant qui envoie un mail, à la victime potentielle, contenant un message d'aide de la part d'un "Homme d'affaire" qui souhaite transférer de l'argent hors de son pays et en retour d'aide, il offrirait une partie de cette somme en échange.

Mais cette technique ne s'arrête pas là, en effet avec la montée en popularité des réseaux sociaux, le nombre de victimes ne fait qu'augmenter d'année en année. Les escrocs utilisent la cupidité des victimes et l'urgence de leur demande pour les forcer à agir sans réfléchir et les encouragent à communiquer des informations bancaires ou des frais initiaux pour faciliter le transfert d'argent. Une fois que la victime a payé ces frais, les escrocs disparaissent avec l'argent et ne transfèrent jamais les fonds promis.

Malheureusement, ces attaques sont très répandues dans le monde et touche de nombreuse personnes chaque année.

Dans cette première partie, nous avons pu vous expliquer le fonctionnement de différentes attaques et les dangers de celle-ci. Maintenant, nous allons voir comment s'en protéger et dans le pire des cas, comment agir contre celle-ci.

De nombreuses pratiques ont été mise en place pour détecter des attaques de phishing. Premièrement, il faut vérifier l'adresse mail de l'expéditeur. En effet, il faut se méfier si elle est inconnue ou suspecte. Les pirates utilisent souvent des adresse mail qui ressemble à celle des organismes connus tels que des banques. Néanmoins, ses adresses comportent de petites subtilités. Par exemple, une adresse légitime pourrait-être : "*serviceclient@votrebanque.com".* Un pirate quant à lui pourrait utiliser l'adresse suivante : *"serviceclient@votrebanquee.com".* Ici, l'erreur réside dans l'ajout du "e" à la fin de banque. Ensuite il faut vérifier l'orthographe du mail en question. Les pirates qui sont majoritairement étranger, rencontrent des difficultés avec la langue française, ce qui explique certaines fautes grossières que l'on peut retrouver dans les mails.

De plus, les mails douteux sont souvent créés pour que la victime agisse rapidement. En effet, cette technique incite la victime à ne pas faire attention à l'endroit où elle clique, tels qu'un lien. Ces liens revoient vers un site frauduleux crée par le pirate lui-même. Il ne faut évidemment pas cliquer sur les liens présents dans les mails suspect ainsi que les pièces jointes qui pourraient contenir des virus. De plus, les mails contiennent généralement des messages demandant des informations personnelles comme des numéros de sécurité sociale ou encore des numéros de cartes de crédits.

De même, nous pouvons nous protéger contre ses attaques en utilisant plusieurs astuces. Après avoir reçu un mail de phishing, la première étape consiste à la fermeture de la fenêtre du mail, ou du message. Dans la seconde étape, si la victime à cliquer sur des liens où a ouvert des pièces jointes, alors il faut qu'elle se déconnecte du ou des comptes qu'elle aurait pu créer. Cela peut éviter tout accès non autorisé du pirate. Ensuite, si la victime à divulguer ses identifiants de connexion et ses mots de passe, alors il faut les changer sans attendre. En effet, si cela n'est pas réalisé, alors le pirate aura accès au compte de la victime et pourra faire ce qu'il souhaite. Dans une troisième partie, il faut prendre contact avec l'institution concerné. Par exemple, si l'attaque de phishing déclarait venir d'une banque, il faudrait immédiatement contacter la banque en question afin de les informer de la situation. De plus, il faut aussi signaler l'arnaque aux autorités comme sur la plateforme 33 700 ou par SMS au 33700. Cela permet d'éviter que d'autres personnes tombent dans le même piège. Après avoir fait ses opérations, il faut ensuite que la victime surveille ses comptes bancaires, ou encore ses comptes en ligne. En effet, le pirate à possiblement enregistré les informations de connexion. De plus, il faut aussi que la victime effectue un scan de sécurité sur son ordinateur pour peut-être détecter la présence de virus. Il faut donc mettre à jour les logiciels de sécurité de l'ordinateur pour une meilleur protection.

La dernière étape pour se protéger contre le phishing est l'utilisation d'outils tiers tel que l'A2F, pour authentification a doubles facteurs qui permet à l'utilisateur d'ajouter une couche supplémentaire de sécurité. L'A2F a un fonctionnement très simple, en effet, cette

fonctionnalité demande à l'utilisateur un code envoyé par l'application en question sur un appareil autre, que ce soit par SMS ou sur une application telle que "google authenticator", qui génère un code unique toute les minutes et ainsi offrir une sécurité accrue.

De plus, mettre à jour ses applications permet de réduire le risque des attaques, grâce aux correctifs de sécurité qui protège les utilisateurs contre les vulnérabilités. De plus, l'installation d'applications représente un risque majeur pour l'intégrité de l'appareil. Ainsi, il faut s'assuré que l'application en question vienne d'une source fiable tels les app store officiel.

Une autre technique de sécurité importante est l'activation des notifications d'activités de son compte. Cela permet à l'utilisateur d'être mis au courant en instantané de chaque connexion ou modification lié à son compte. De plus, examiné les paramètres de confidentialités des applications ou autre, permet de limiter le nombre d'informations personnelles partagé avec le tier.

Pour terminer avec les mesures de protections tiers, l'utilisation d'application et d'extension tels que PrivacyBadger ou Ublock sur Firefox ou bien l'utilisation de service VPN qui ne récupère aucunes données personnelles tels que ProtonVPN permettent tous d'augmenter la sécurité sur internet.

En conclusion, l'hameçonnage, qu'il soit réalisé par clonage par téléphone ou par des escroqueries bien élaborées comme l'arnaque nigériane, représente une menace importante pour la sécurité en ligne. Ces attaques utilisent la crédulité des victimes pour obtenir des informations sensibles, entraînant ainsi des conséquences graves telles que le vol d'identité et la perte financière.

Heureusement, il existe des moyens de se protéger contre ces attaques. La vigilance est cruciale : vérifiez attentivement les adresses email, il ne faut jamais cliquer sur des liens suspects ou téléchargez des pièces jointes provenant d'expéditeurs inconnus.

L'authentification à deux facteurs (A2F) offre une couche supplémentaire de sécurité, tandis que les mises à jour régulières des applications et l'utilisation d'outils tiers tels que les bloqueurs de publicités et les services VPN renforcent la protection en ligne.