Phishing ou Hameçonnage : un crime cyber par l'appât

Pr Chérif DIALLO, CISSP
Professeur Assimilé (LAFMC CAMES)
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

"Le poisson ne voit pas l'hameçon, il ne voit que l'appât ; l'homme ne voit pas le péril, il ne voit que le profit."
Proverbe mandchou

Résumé: Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente une menace qui très courante sur internet. Il s'agit du phishing (ou hameçonnage) qui est une arnaque en ligne dans laquelle des cybercriminels se font passer pour des acteurs de confiance, pour inciter leurs victimes à partager leurs données sensibles ou à installer des logiciels malveillants (ou malwares). Le phishing est ainsi une cyberattaque qui utilise le courrier électronique déguisé comme une arme. L'objectif de l'attaquant est de tromper le destinataire en lui faisant croire qu'il reçoit un message important, comme celui de sa banque ou de sa société ; cette demande pourrait être pour eux de cliquer sur un lien ou de télécharger quelque chose. Après avoir collecté les données, les pirates informatiques utilisent les informations pour installer des logiciels malveillants sur des systèmes critiques. Après une brève définition, nous donnerons les types de phishing, les tendances actuelles de cette menace et les solutions avant de conclure.

Mots clés: Cybercriminalité, Phishing, Hameçonnage.

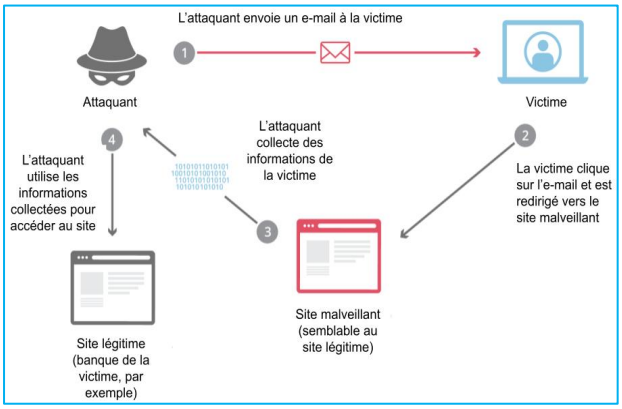
---

1. Définition

L'hameçonnage ou phishing est une forme d'escroquerie sur internet qui repose le plus souvent sur la contrefaçon d'un site internet. L'escroc se fait passer pour un organisme que vous connaissez (site marchand, banque, compagnie d'assurance, service des impôts, etc.), en utilisant le nom, le logo et la charte graphique de cet organisme. Il vous envoie un mail vous demandant généralement de "mettre à jour" ou de "confirmer vos informations suite à un incident technique", notamment vos coordonnées bancaires (codes personnels, numéro de compte, etc.). Les attaques de phishing de base consistent donc à inciter les utilisateurs à renseigner leurs données personnelles ou d'autres informations à caractère confidentiel. Les techniques utilisées pour cela sont multiples :

- Réception dans votre boîte mail d'un message d'alerte ou de promotion avec un contenu identique à celui d'une banque ou d'une entreprise pour vous inciter à cliquer sur un bouton qui masque un lien.
- Publication d'un faux communiqué (offre d'emploi, offre de visa, de bourse d'étude, etc.) d'un organisme en vous demandant de cliquer sur un lien puis de rentrer des informations personnelles.
- Faux SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

Une attaque de phishing peut donc cibler des utilisateurs précis, par exemple les personnes utilisant un produit spécifique, ou viser plus large avec des faux concours et des récompenses alléchantes. Dans les deux cas, les victimes devront renseigner leur nom, leur adresse email et, parfois, leur mot de passe et leurs coordonnées bancaires.



2. Types d'attaques de phishing

Il y a plusieurs types d'attaques de phishing, dont deux (Spray and pray, Spear-phishing) qui sont très populaires :

- **Spray and pray**. L'approche « Spray and pray » (autrement dit « Envoie et prie ») est l'attaque la moins complexe : elle consiste simplement à envoyer un email à des millions d'adresses à la fois. Ces messages cherchent généralement à générer un sentiment d'urgence, par exemple en se faisant passer pour une communication « importante » de votre banque ou d'un service populaire ou en vous félicitant, par exemple, d'avoir gagné un iPhone flambant neuf.
- **Spear-phishing**. Le spear-phishing (ou harponnage) est une méthode plus avancée. Contrairement à l'approche « spray and pray » qui est envoyée en masse, le spear-phishing cible des groupes spécifiques avec un message plus personnalisé. Par exemple, les hackers peuvent se concentrer sur les clients d'une marque précise et créer un email reproduisant l'image de cette marque. Ils sont capables de cibler des organisations spécifiques, des services ou des départements au sein de ces organisations, ou même des individus précis pour maximiser leurs chances de réussite et la quantité d'informations collectées. Les cyberattaques les plus sérieuses reposent généralement sur ce type d'approche.
- **Clone phishing.** Le clone phishing consiste à faire une copie, ou clone, d'un e-mail légitime et à remplacer ses liens ou ses pièces jointes afin d'inciter la victime à ouvrir un site web ou un fichier malveillant. Par exemple, en prenant un e-mail et en joignant un fichier malveillant portant le même nom que le fichier joint légitime, puis en renvoyant l'e-mail avec une adresse e-mail usurpée qui semble provenir de l'expéditeur d'origine, les attaquants peuvent exploiter la confiance basée sur la communication initiale pour piéger la victime.
- **Whaling.** Pour les attaques qui visent spécifiquement les cadres supérieurs ou d'autres utilisateurs privilégiés au sein des entreprises, le terme whaling est couramment utilisé. Ces types d'attaques sont généralement ciblées avec un contenu susceptible de nécessiter l'attention de la victime, comme une citation à comparaître ou d'autres problèmes qui concernent les dirigeants d'une entreprise.
- Un autre vecteur courant du Whaling est la diffusion d'e-mails frauduleux qui semblent provenir d'un cadre supérieur. Par exemple, une demande par e-mail provenant d'un PDG à un membre du service financier demandant son aide immédiate dans le cadre d'un transfert de fonds. Un employé situé à un échelon plus bas de la hiérarchie est parfois trompé en pensant avoir affaire à un supérieur. Cette position l'amène à ne pas vérifier l'authenticité de la demande et à transférer de grosses sommes d'argent à un escroc.

3. Tendances

Le phishing, la cyberattaque la plus populaire n'a pas cessé d'augmenter :

- 66% des entreprises ont été exposées au phishing en 2020.
- En 2020, le moteur Google a enregistré pas moins de 18 millions d'attaques phishing par jour.
- En tout, c'est 46.000 sites d'hameçonnage détectés chaque semaine.
- Google a découvert plus de 2.1 millions de sites de phishing en janvier 2021.

- Le phishing étant l'une des tactiques les plus populaires des pirates, les experts en cybersécurité suivent l'augmentation de l'utilisation du phishing dans le monde. Google a trouvé 27% de sites de phishing supplémentaires en janvier 2021 par rapport à janvier 2020. Ces sites Web étaient dédiés au vol de données personnelles, d'identifiants de connexion et de données médicales.
- Aujourd'hui, plus de 80 % des événements de cybersécurité impliquent des attaques de phishing.

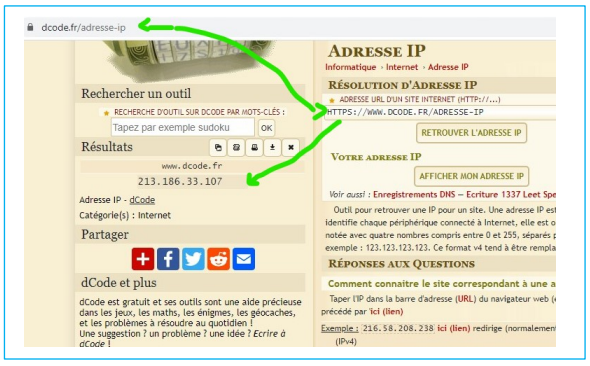
4. Solutions

Il est important de noter qu'il existe des mesures d'atténuation et des réponses appropriées aux attaques de phishing. D'abord, il est important de savoir reconnaître les tentatives de phishing :

- **Les messages sont trop beaux pour être vrais.** «Félicitations! Votre numéro de cellulaire a fait de vous un gagnant d'un concours Apple! Visiter ce site Web pour réclamer votre produit gratuit.» «Bravo, vous avez été sélectionné pour tester le futur iPhone 14!»
- **Le sentiment d'urgence.** On vous signale des problèmes au niveau de votre compte ou des transactions que vous avez faites.
- **Les erreurs dans les noms de domaine.** Par exemple: support@mailjet-com.com, http://capitalhouse.com.mx/.secure, ou bien log@aduciel.fr.

Ensuite, il y a votre réaction face à un message de phishing. Pour éviter et atténuer les dommages si vous êtes attaqué, suivez ces conseils :

- ne communiquez jamais d'informations importantes (numéro de carte bancaire, mot de passe, etc.) en cliquant sur un lien reçu par courrier électronique ;
- ne répondez jamais aux messages suspects : une banque ne vous demandera jamais de lui communiquer vos coordonnées bancaires par simple courriel. Et il est peu probable qu'un inconnu vous propose réellement de bénéficier d'un héritage ;
- partez toujours de la page d'accueil d'un site pour accéder aux autres pages, notamment celles où sont demandés des identifiants ;
- quand vous êtes sur un site sécurisé, comme un site bancaire, vérifiez que le chiffrement des données est activé : l'adresse du site doit commencer par "https://" (et non "http://") avec un petit cadenas affiché sur la gauche ou en bas de votre navigateur ;
- en cas de doute, prenez contact directement avec l'entreprise ou l'administration concernée par téléphone ;
- ne surtout pas ouvrir les pièces jointes, ne cliquez pas non plus sur les liens et ne répondez-pas ;
- s'il s'agit de votre messagerie personnelle, supprimez le message puis videz la corbeille.
- Au-delà de ces recommandations, il existe aussi des solutions logicielles pour éviter de tomber dans le piège :
    - des plateformes comme dcode (https://dcode.fr) permettent de retrouver une adresse ip depuis un lien de site ;
    - des outils en ligne comme hostip géolocalisation (https://hostip.info) offrent la possibilité de situer la ville dans laquelle le site est hébergé ;



    - l'outil Web Of Trust (WOT) protège des phishing en envoyant des message d'alerte à chaque fois qu'on est en face d'un site qui a une mauvaise réputation sur le net. Pour cela, il vérifie la réputation et les information de sécurité des site web en se basant sur les expériences des utilisateurs.
- Par ailleurs, il est aussi indispensable, pour la protection des données, de sécuriser son système d'exploitation pour bloquer toute tentative de pénétration :
    - protection par un par-feu (ou firewall) ;
    - utilisation de logiciel anti espion et anti spam ;
    - mise à jour régulière de la machine et des anti-virus.

- Pour les entreprises, un certain nombre de mesures peuvent être prises pour atténuer les attaques de phishing :
    - l'authentification à deux facteurs est la méthode la plus efficace pour contrer les attaques de phishing, car elle ajoute une couche de vérification supplémentaire lors de la connexion à des applications sensibles. L'authentification à deux facteurs repose sur le fait que les utilisateurs disposent de deux éléments : quelque chose qu'ils connaissent, comme un mot de passe et un nom d'utilisateur, et quelque chose qu'ils possèdent, comme leur smartphone. Même lorsque les employés sont compromis, l'authentification à deux facteurs empêche l'utilisation de leurs informations d'identification compromises, car celles-ci sont à elles seules insuffisantes pour entrer dans les applications ;
    - en plus d'utiliser l'authentification à deux facteurs, les entreprises doivent appliquer des politiques strictes de gestion des mots de passe. Par exemple, les employés devraient être tenus de changer fréquemment leurs mots de passe et ne pas être autorisés à réutiliser un même mot de passe pour plusieurs applications ;
    - les campagnes de sensibilisation peuvent également aider à réduire la menace d'attaques de phishing en encourageant les bonnes attitudes, telles que ne pas cliquer sur des liens de messagerie externes.

5. Pour finir

Les cyberattaques malveillantes deviennent chaque jour plus avancées et plus répandues. Les personnes aussi bien que les organisations ont besoin d'une gestion intelligente des menaces pour pouvoir se préparer à ces cyberattaques. Comme on l'a vu, l'hameçonnage est donc un cybercrime dans lequel une cible ou des cibles sont contactées par e-mail, téléphone ou SMS par une personne se faisant passer pour une institution légitime afin d'inciter des individus à fournir des données sensibles telles que des informations personnellement identifiables, des informations bancaires et de carte de crédit et des mots de passe. Les informations sont ensuite utilisées pour accéder à des comptes importants et peuvent entraîner un vol d'identité et des pertes financières.

Les attaques de hameçonnage ne cessent d'augmenter de jour en jour depuis la première plainte pour hameçonnage qui a été déposée en 2004 contre un adolescent californien qui avait créé l'imitation du site « America Online ». Avec ce faux site Web, il a pu obtenir des informations sensibles des utilisateurs et accéder aux détails de la carte de crédit pour retirer de l'argent de leurs comptes. Outre l'hameçonnage par e-mail et site Web, il existe également le "vishing" (hameçonnage vocal), le "smishing" (hameçonnage par SMS) et plusieurs autres techniques d'hameçonnage que les cybercriminels proposent constamment.

Généralement, les e-mails envoyés par un cybercriminel sont masqués afin qu'ils semblent être envoyés par une entreprise dont les services sont utilisés par le destinataire. Il faut garder à l'esprit qu'une banque ne demandera pas d'informations personnelles par e-mail ou ne suspendra pas votre compte si vous ne mettez pas à jour vos informations personnelles dans un certain délai. La plupart des banques et des institutions financières fournissent également généralement un numéro de compte ou d'autres informations personnelles dans l'e-mail, ce qui garantit qu'il provient d'une source fiable.