Nova-Tech
Imagine the Possibilities

LE PHISHING

ZIE MAMADOU COULIBALY

16/03/2018

Zié Mamadou Coulibaly (coulibalyziemama@gmail.com)

QU'EST-CE QUE LE PHISHING(HAMEÇONNAGE)

Le phishing est une technique frauduleuse utilisée par les pirates informatiques pour récupérer des informations sensibles, personnelles et/ou confidentielles (coordonnées bancaires, vol d'identité…) appartenant à des internautes. Bien que cette technique soit souvent utilisée pour voler des données à des fins malveillantes, les cybercriminels peuvent également avoir l'intention d'installer un programme malveillant sur l'ordinateur de l'utilisateur ciblé.

COMMENT PROCEDENT LES PHISHERS ?

Le mode opératoire de cette menace est le suivant : l'utilisateur reçoit un e-mail, un sms provenant, en apparence, d'une source digne de confiance, mais ce message le conduit à son insu sur un site Internet fictif infesté de programmes malveillants. Ces e-mails utilisent souvent des techniques ingénieuses pour capter l'attention des victimes.

Le spam et le phishing sont liés car ces emails frauduleux sont généralement envoyés en masse pour multiplier le nombre de victimes potentielles des pirates. De fait, l'email est le moyen le plus utilisé par les cyber-criminels pour prendre contact avec leurs cibles. Toutefois, le phishing peut utiliser d'autres moyens de communication que l'email. On observe par exemple des cas de phishing par SMS (smishing), VoIP (vishing), etc.

Dans le cas du smishing, la victime reçoit par SMS un message l'invitant à cliquer de toute urgence sur un lien. Ce lien amène alors sur un site malveillant. Quant au vishing, ce sont des appels passés par une personne se faisant passer pour un salarié de la banque, par exemple, et demandant de fournir des données personnelles pour de soi-disant vérifications.

Les emails trompeurs envoyés par les pirates contiennent généralement un lien vers des sites web contrefaits. De cette façon, les internautes pensent être arrivés sur un site web légitime. Confiants, ils entrent les informations demandées, qui tombent alors dans les mains des arnaqueurs du Net. Cet email inclut des liens vers un site web qui imite le site web de l'entreprise usurpée et sur lequel la victime est invitée à entrer ses données personnelles.

COMMENT VOUS PROTEGEZ ?

Les méthodes de sécurité traditionnelles sont souvent insuffisantes pour contrer ces attaques habilement personnalisées. Elles n'en deviennent que plus difficiles à détecter.

- Vérifiez la source des informations que vous recevez. Ne répondez pas aux messages électroniques qui vous demandent des informations personnelles ou confidentielles.
- Si vous recevez un email avec un lien et que vous voulez y accéder, entrez l'adresse manuellement dans le navigateur Internet plutôt que de cliquer sur le lien.
- Vérifiez que le site web sur lequel vous vous trouvez est sécurisé avant de fournir des données personnelles. La barre d'adresse doit commencer par https:// et un petit cadenas doit apparaître en bas de votre navigateur, dans la barre d'état.
- Vérifiez vos comptes en ligne régulièrement pour détecter les éventuels transferts ou transactions non autorisés.
- N'oubliez jamais que votre banque ne vous demandera jamais d'informations confidentielles via des moyens de communication non sécurisés comme les emails.

- La vérification de l'adresse web dans la barre d'adresse du navigateur web est la première parade. Ainsi, une attaque simple consiste à utiliser un nom de domaine très semblable (par exemple avec une faute grammaticale ou orthographique), comme https://sogecashnet-societegenerale.ch au lieu de https://sogecashnet.societegenerale.ci. L'attaquant aura préalablement acheté un nom de domaine proche de l'original, généralement une variante orthographique.
- Pour savoir si une URL correspond à une tentative de phishing, le site Isit Phishing propose de vérifier la page web.

CATURE DES 2 SITES

Image du vrai site : https://sogecashnet.societegenerale.ci.

Image du faux site : https://sogecashnet-societegenerale.ch

CONSEQUENCES DU PHISHING ?

- Usurpation d'identité et vol de données confidentielles des internautes. Avec de sérieuses pertes financières pour les victimes, voire l'impossibilité d'accéder à leurs comptes.
- Perte de productivité.
- Consommation excessive des ressources du réseau de l'entreprise (bande passante, messagerie saturée, etc.).

APPROCHE

Le pharming est une sorte de phishing particulièrement redoutable. Elle consiste à détourner le système de résolution des noms de domaines (DNS) pour amener les internautes sur de fausses pages web à leur insu.

Lorsqu'un utilisateur entre une adresse dans son navigateur, celle-ci est automatiquement convertie en adresse IP. Ce processus, appelé résolution de nom de domaine, est effectué par les serveurs DNS.

Cependant, certains types de logiciels malveillants sont conçus pour détourner le système local de résolution des noms de domaines, défini dans le fichier HOSTS placé sur l'ordinateur.

Ce fichier contient les informations pour résoudre certaines adresses IP auxquelles accède l'utilisateur de l'ordinateur. Ainsi, lorsque l'utilisateur entre le nom d'un site web,

l'ordinateur consulte d'abord le fichier HOSTS pour vérifier s'il n'y a pas déjà une adresse IP associée à ce nom. S'il ne trouve pas de correspondance dans le fichier, il consulte alors le serveur DNS du fournisseur d'accès à Internet.

Le pharming consiste à modifier le fichier HOSTS pour rediriger le nom de domaine d'une organisation légitime (votre banque, par exemple) vers des faux sites web qui imitent le véritable site web. Ainsi, les pirates peuvent dérober les informations confidentielles saisies par l'utilisateur sur ce site.

Contrairement au phishing classique, le pharming est une attaque qui opère dans la durée. Le fichier HOSTS modifié reste sur l'ordinateur, dans l'attente que l'utilisateur essaie d'accéder aux sites web visés par le pirate (services de banque en ligne, etc.)...