Les techniques de craquage de mots de passe (via le phishing)

.

1. Introduction

J'ai pendant plusieurs années été alerté par des mails, des messages et des notifications suspicieux.
Les informations de la télé et d'internet parlent de phishing, mais qu'est ce que-c'est? les techniques ont évolué au point de ne plus différencier le ver de l'hameçon? pourquoi en reçoit-on moins? Qui y a il de nouveau ?

Tout d'abord je tiens à expliquer les 5 techniques de phishing les plus courantes :

1. Abus de confiance – Pierre reçoit un email lui demandant de confirmer un transfert d'argent. A noter que l'email contient un lien envoyant vers un site qui s'apparente être celui de sa banque… mais en réalité il s'agit d'une copie, éditée, contrôlée et hébergée par des pirates. Une fois sur la page, Pierre entre normalement ses identifiants mais rien ne se passe et un message disant que le site est « temporairement indisponible » apparaît. Pierre étant très occupé, se dit qu'il s'en occupera plus tard. En attendant, il a envoyé ses codes d'accès aux pirates.

2. Fausse loterie – Pierre reçoit un email lui indiquant qu'il a gagné un prix. Habituellement Pierre n'y prête pas attention, car bien trop occupé. Toutefois, cette fois ci, l'email est envoyé par Alain, mentionnant une organisation caritative qu'ils soutiennent mutuellement. Pierre clique alors sur le lien, rien ne se passe à l'écran, mais un malware s'est installé sur son poste de travail.

3. Mise à jour d'informations – Pierre reçoit un email d'Alain lui demandant de regarder le document en pièce jointe. Ce document contient un malware. Pierre ne s'est rendu compte de rien, en ouvrant le document, tout semblait correct bien qu'incohérent par rapport à son travail. Résultat, le malware enregistre tout ce que fais Pierre sur son poste (keylogger) depuis des mois, ce qui met en danger tout le Système d'Information de l'entreprise facilitant le vol de données

19/07/2017

BANQUE POPULAIRE
BANQUE & ASSURANCE

Bonjour,

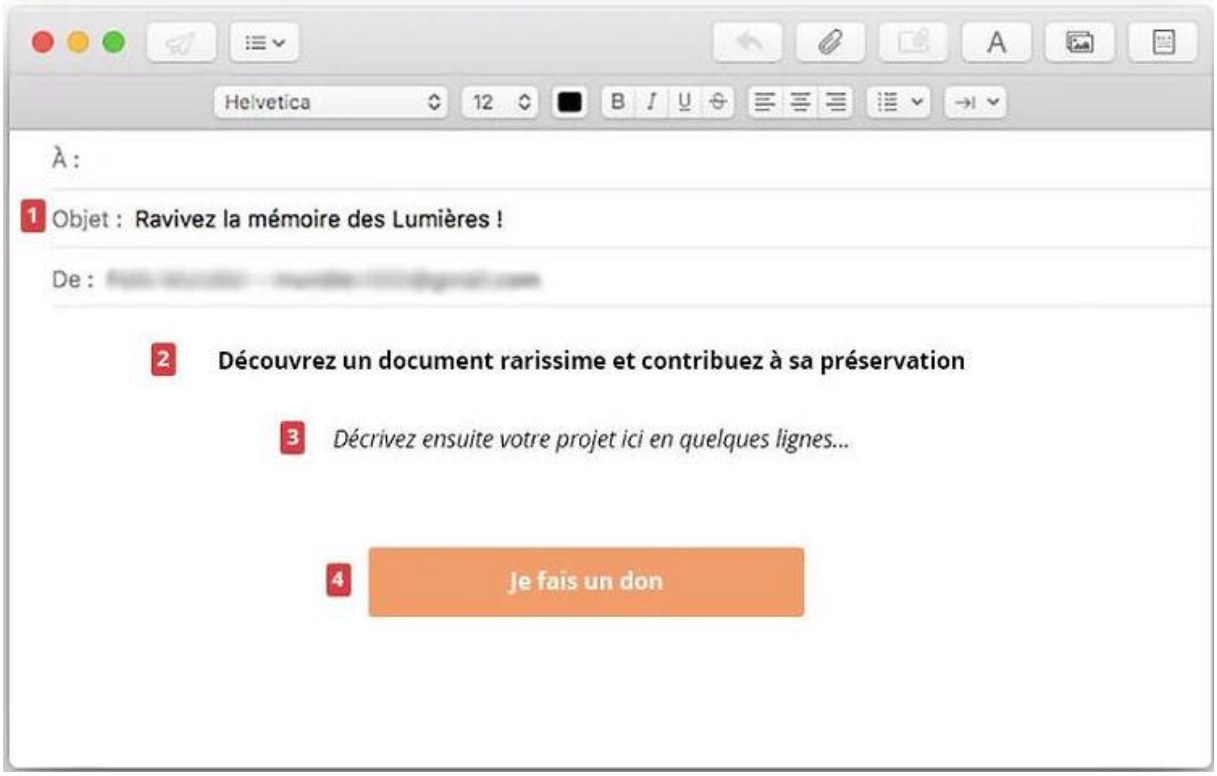
Le département technique procède à une mise à jour 2017 de logiciel, programmée de façon à améliorer
la qualité de nos services.
Nous vous demandons avec bienveillance de procéder à la mise à jour en cliquant sur le lien ci-dessous et de sécuriser votre PassCyberPlus:

19/07/2017 : Régler votre situation

Nous vous remercions pour la confiance que vous nous accordez et restons à votre disposition.

Cordialement
Directeur de la relation clients

4. **Appel à donation** – Pierre reçoit un email du frère d'Alain, lui disant qu'il est atteint d'un cancer et que sa couverture sociale s'est arrêtée. Voulant faire bonne impression auprès de son patron, Pierre clique sur le lien et se rend sur le site de donation dédié. Pierre décide de faire une donation de 100€ et entre ses informations bancaires. Le site précise même que le don est déductible des impôts… Trop tard, Pierre a donné ses informations et se fait débiter d'un montant bien supérieur… sans pouvoir le déduire de ses impôts !



5. Usurpation d'identité – Pierre reçoit un email d'Alain, lui demandant d'effectuer un virement auprès d'un fournisseur connu au sujet d'une avance concernant un dossier urgent. Pour Pierre, il s'agit d'une tâche de routine qu'il effectue aussitôt. L'argent est envoyé sur un compte étranger, intraçable et ne sera jamais retrouvé.

- D'accord mais pourquoi avoir choisi ce sujet en tant que veille technologique si cela existe depuis longtemps?

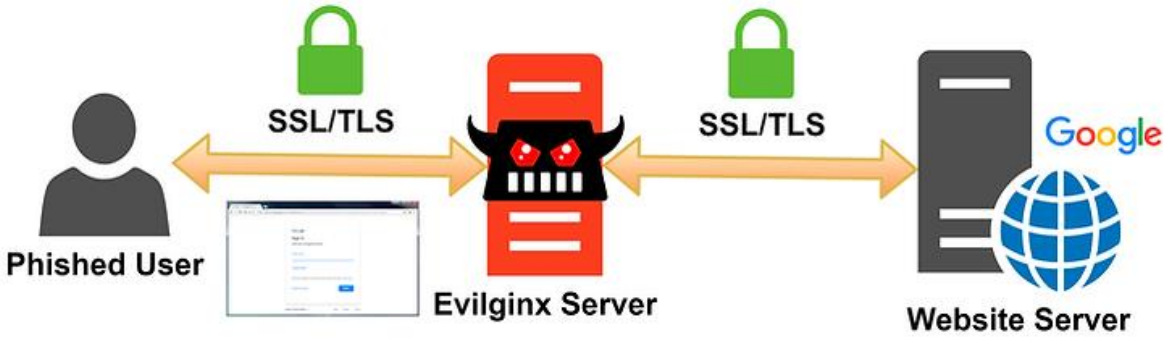
Tout simplement car aujourd'hui cette technique existe toujours et à même évoluer au point de ne plus distinguer le vrai du faux. Et comme j'aime à penser, la priorité pour un informaticien est de protéger les informations de l'entreprise. Une technique reposant sur une grande partie sur l'erreur humaine est une faille très importante. De plus les attaques de phishings ont augmenté de près de 250% par rapport à 2017.

Comment se protéger?

Et bien la meilleure méthode est d'avoir un par-feu configuré pour bloquer les sites frauduleux. Il faut surtout informer tous les collaborateurs des risques et des solutions pour ne pas tomber dans le piège. Par exemple, ne pas cliquer sur le lien d'un inconnu et regarder l'url des sites où vous rentrez des informations surtout type mots de passe. Surtout que 35% des français n'utilisent que 1 mot de passe pour tous leurs comptes (google, Facebook, jeux, info privée etc...) . Un plus est l'utilisation de signale spam qui est recommandée par la CNIL.

Une solution pouvant bloquer une bonne partie des "pécheurs" est la double authentifications. Néanmoins ce n'est pas pour autant que vous serez protégé. Car le pirate aura tout de même votre mot de passe et surtout certaine technique récente de phishing permet de passer la double identifications comme Evilginx2!

Evilginx2 est un logiciel qui va se poser en pont entre la victime et un site :



Le grand plus de cette technique est la possibilité de récupérer un cookie, qui va permettre au hacker de rendre inutile le facteur de double authentifications