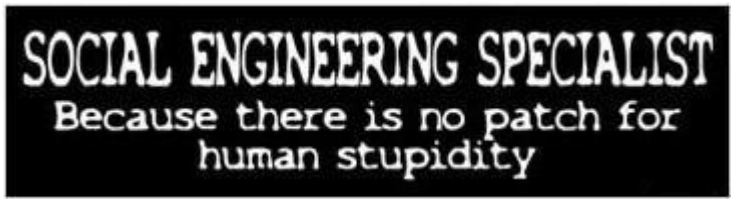


Le Social Engineering : une attaque de persuasion

Sommaire

Written by 599eme Man

1. Introduction

Le Social Engineering dit SE est une technique de manipulation psychologique humaine qui sert à obtenir "invisiblement" des informations d'une personne ciblée. Cela nécessite pas d'énormes connaissances informatiques, mais nécessite de s'adapter à la victime suivant le type de l'attaque du SE (Niveau de langage, apparence, charisme, persuasion, savoir mentir) c'est-à-dire apprendre à exploiter les failles humaines (confiance, manque d'informations).
Cette méthode, le SE, peut aussi servir aux personnes mal attentionné de vous infecter (Malware, Spyware, etc) ou encore servir au phishing qui est en partie une attaque de SE.

2. Méthode

2.1 Avantages/Inconvénients

- Forte discrétion donc faible détection
- Forte portée

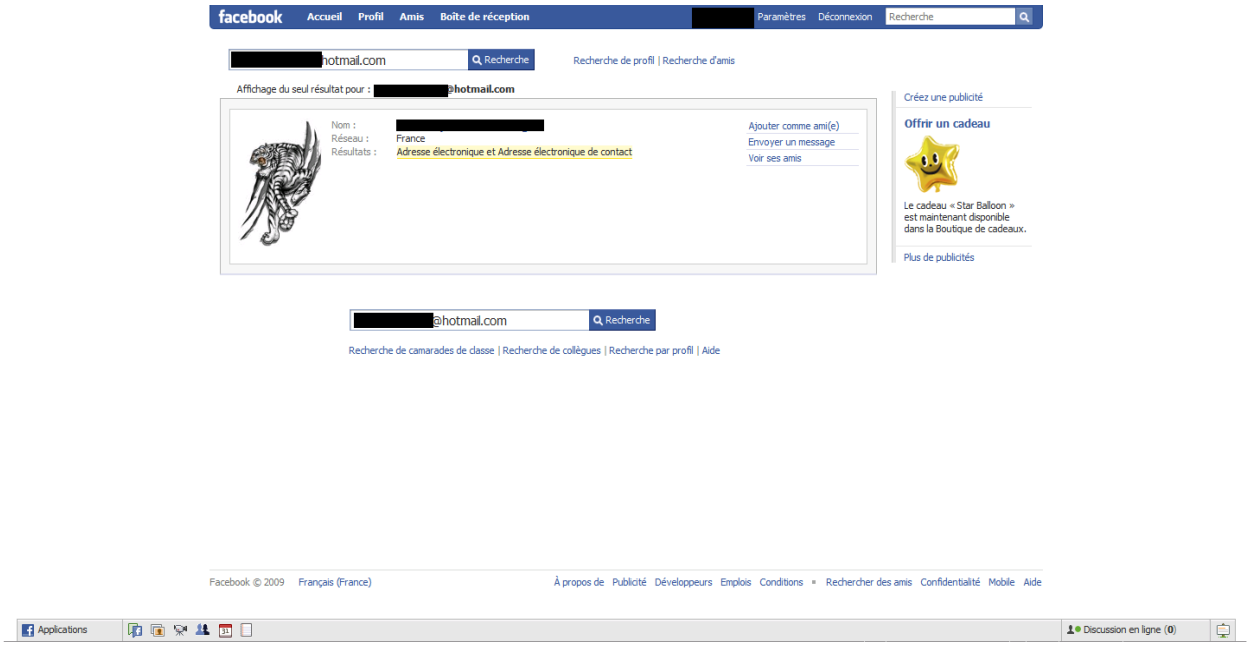
- Non garantis et non précis

2.2 Pratique

2.2.1 Internet

La méthode par internet est sans-doute la plus transparente. Elle permet d'obtenir diverses informations sur la cible (e-mail, nom, prénom, amis, numéro de téléphone, sites fréquentés). Vous pouvez utiliser divers outils comme Facebook, Myspace, Google qui peuvent fournir à partir de l'e-mail ou du nom-prénom des infos sur les amis, inscrit sur tel ou tel sites et d'autres infos complémentaires.

Exemples :



2.2.2 Téléphone et Courrier

Ces trois méthodes sont utilisés lorsque le pirate a préparé l'attaque. Elles nécessitent beaucoup de préparations pour la confiance, le dialogue, bien se mettre dans la peau du personnage et la façon d'obtenir les informations désirées en douceur et petit à petit. Il faut au préalable se renseigner sur la victime via la recherche sur internet ou par l'intermédiaire des amis ou des connaissances de cette victime.

Ces trois méthodes sont complémentaires pour une attaque parfaite : Coup de téléphone pour annoncer la chose tout en ayant usurpé une identité, si la victime ce doute de quelques choses et demande une confirmation : le courrier intervient (ce courrier doit être vraiment minutieux : s'inspirer d'une vraie lettre de votre usurpation).

2.2.3 Reverse Social Engineering

Le Reverse Social Engineering est une attaque face-à-face dans laquelle le pirate va convaincre que la victime a un problème et que lui peut le résoudre. Cela se passe en plusieurs étapes :

- S'être renseigné sur la victime
- Savoir si elle a un problème bénin ou si il y en a pas : le provoquer
- Intervenir comme réparateur (pub, mails, téléphone) en proposant un faible prix
- Gagner la confiances de la victime (avoir confiance en soi, fort charisme et flatter la victime)

2.3 Phishing

Le phishing est une usurpation qui consiste à se faire passer pour une société (Messenger, banques, paiement en lignes (paypal) etc.) pour pouvoir voler identifiant, numéro de carte bleue etc.
La façon d'appâter la victime jusqu'à la page de phishing s'appelle l'hameçon. L'hameçon est le plus souvent sous forme de mail ou de site proposant des services souvent incroyables.

Exemples :

Cher client de **SOCIÉTÉ GÉNÉRALE**

Le département technique de Société Générale procède à une mise à jour de logiciel programmée de façon à améliorer la qualité des services bancaires.

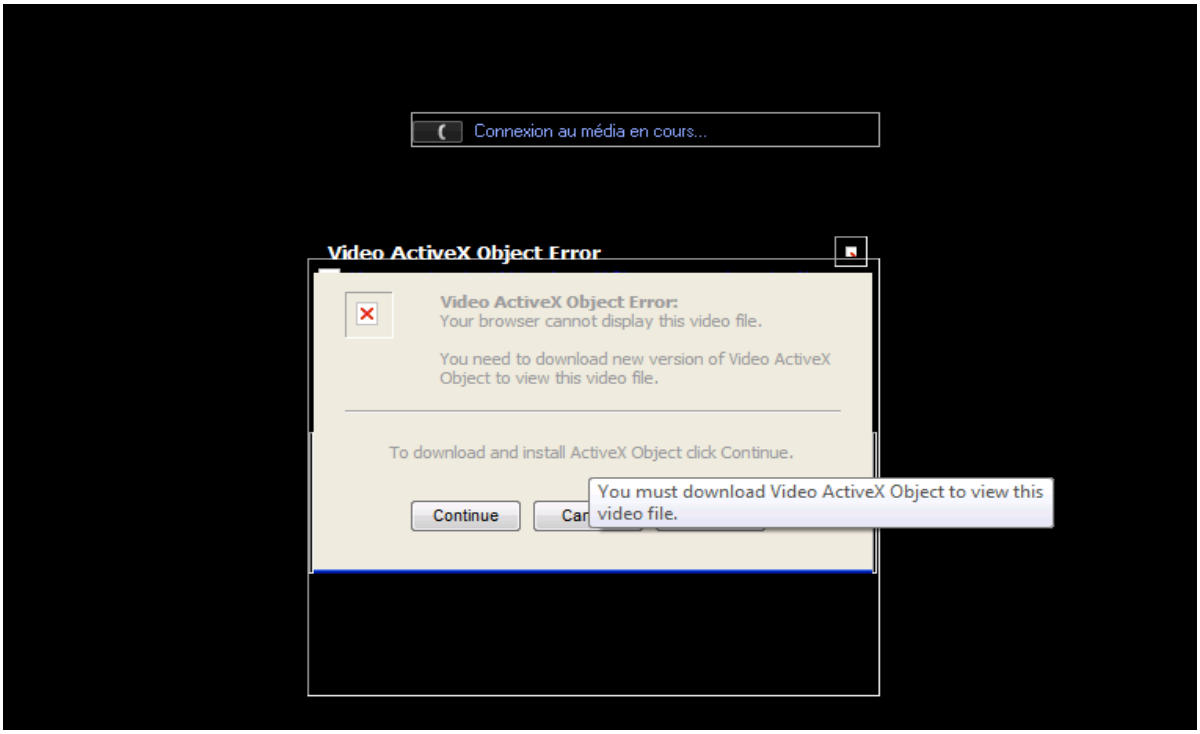
Nous vous demandons avec bienveillance de cliquer sur le lien ci-dessous et de confirmer vos détails bancaires.

http://www.[redacted]

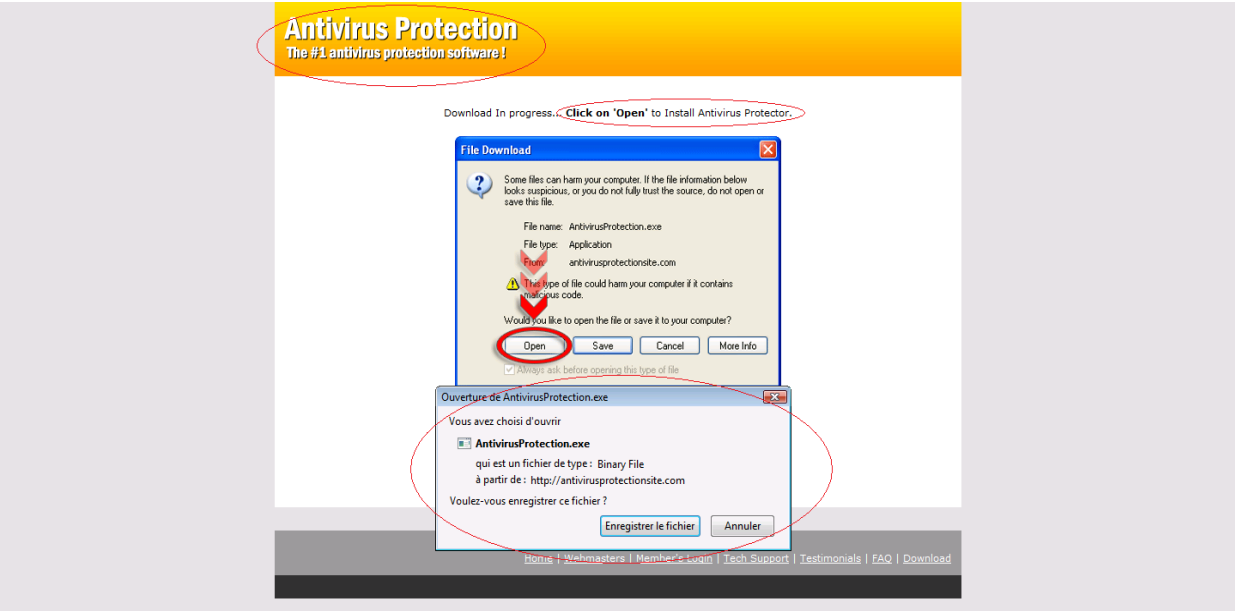
Nous nous excusons pour tout désagrément et vous remercions de votre coopération.

2.4 Malware/Spyware

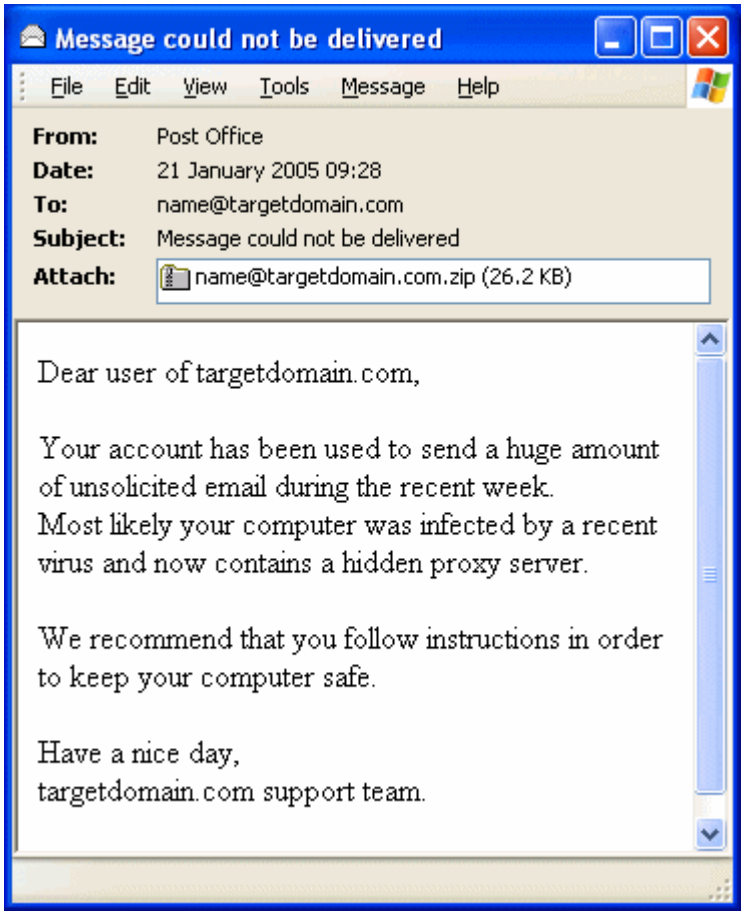
Souvent, les utilisateurs ne font pas attention et installent ce que les sites leur disent en dissimulant leurs spyware/malware en faux programmes. En majorités, ces logiciels sont dissimulés sous forme d'antivirus performant (rogue) ou de codec.



Les sites de rogues ont qu'un seul but : persuadé l'utilisateur que son ordinateur est infecté et qu'il nécessite un antivirus en urgence et ce site en fournit un pour vite se désinfecter du soit disant virus.



Tout comme le phishing, les malware/spyware peuvent être envoyés sous forme d'e-mail usurpé demandant une mise à jour de logiciel qui ont l'air anodin, mais qui en vérité peuvent cacher des trojans, virus, bot etc.



3. Protection

3.1 Détection

La détection est plus ou moins facile suivant le pirate. Les attaques de Social Engineering peuvent se résumer à de simples questions personnelles et précises (hors du travail) sur vous ou votre entourage qui pourraient servir à une attaque future sur vous ou votre entourage.

3.2 S'en Prémunir

S'en prémunir est très difficile. En effet, un bon pirate ne pourra pas se faire remarquer, il combinera des recherches sur internet, des questions à votre entourage puis posera des questions directement à vous sous différents horizons. Vous pouvez essayer de vous protéger de tout cela en ne donnant aucune information personnelles sur le net puis lors d'un coup de téléphone suspect de toujours demander le numéro de téléphone et en connaître sa provenance. Toutes les lettres, papiers pub vous incitants à appeler ou répondre avec des informations vous concernant devront être jetés.

Lorsque vous doutez d'être victime d'une attaques Reverse Social Engineering, vous devez vous renseigner un maximum sur la personne (Si cette personne travaille réellement pour la société dites) et la rencontrer dans l'enceinte de sa société.

Si vous faites partie d'une société, pour ne pas être victime, il faut prendre en compte tous les mouvements/habitudes, le langage et le quotidien du personnel. Si une de ces personnes est inconnue et ne vous inspire pas confiance, il faut faire attention aux renseignements que cette personne vous demandera.

4. Conclusion

Le Social Engineering est utilisé pour manipuler psychologiquement la victime pour lui faire faire des actions à but malveillantes dissimulés qu'elle n'aurait pas pu faire seule en l'incitant à cliquer, télécharger/ ouvrir et parler.

5. Bibliographie

- *Kevin Mitnick (Wiki:http://fr.wikipedia.org/wiki/Kevin_mitnick)*
- *Cybertraque (Film retraçant la vie de Kevin Mitnick en partie sur le Social Engineering)*
- *Burgers Gratuit (http://www.youtube.com/watch?v=cQtQg--PB0k)*
- *Mcdonald Gratuit (http://www.youtube.com/watch?v=27NX_MMIkLY&feature=related)*
- *Kevin Mitnick et William L. Simon, L'art de la supercherie, éditions Wiley/Campus Press, 6 mai 2003, 377 pages p. (ISBN 2744015709)*
- *Wiki:http://en.wikipedia.org/wiki/Social_engineering_(security)*

6. About Me

Author : 599eme Man
Contact : flouf@live.fr

Special Greetz : *Str0zen, Sheiry, Pr0h4ck3rz, J.Consultant, Gh0st911 and Stacker*