La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

Ingénierie Sociale

Vue d'ensemble

L'une des croyances populaires qu'ont beaucoup de personnes, c'est que les pirates utilisent surtout des outils puissants et des techniques poussées pour pirater les comptes et les ordinateurs de leurs cibles. Cela est faux. Les attaquants ont compris que la façon la plus simple de voler des informations, de pirater des comptes ou encore de pénétrer les systèmes c'est simplement de vous pousser à commettre une erreur. Dans cette newsletter, vous allez apprendre comment fonctionnent ces attaques, dites d'ingénierie sociale et surtout comment vous en protéger.

Editeur invité

James Lyne (**@jameslyne**) est à la fois un instructeur certifié SANS et est à la tête de la Recherche au sein de la société Sophos. Il fait de la rétro-ingénierie (Reverse Engineering) sur les dernières créations des pirates informatiques. Il est également l'auteur des cours SANS « Metasploit » (SEC580) et « Social Engineering » (SEC567).

Qu'est-ce que l'ingénierie sociale ?

L'ingénierie sociale est une attaque psychologique au cours de laquelle un attaquant vous influence pour vous faire réaliser quelque chose que vous ne devriez pas faire. Le concept de l'ingénierie sociale n'est pas nouveau, il existe depuis des millénaires. Les escrocs utilisent également ce type de techniques. Les pirates informatiques ont des méthodes bien plus efficaces car les outils d'aujourd'hui vous empêchent de les voir et ils peuvent très facilement prétendre être qui ils veulent. Ils peuvent cibler des millions de personnes à travers le monde, vous compris. De surcroît, ces méthodes permettent de contourner bon nombre de technologies. La façon la plus simple de comprendre ces attaques et comment vous en protéger, c'est de regarder les deux exemples ci-dessous.

Vous recevez un appel téléphonique d'une personne se déclarant être d'une société de support informatique, cela peut être votre fournisseur d'accès à internet ou encore Microsoft. Votre correspondant vous explique que votre ordinateur est en train de scanner activement internet et ils pensent qu'il est infecté par virus et qu'ils sont justement là pour vous aider à sécuriser votre machine. Ils utilisent ensuite beaucoup de termes techniques et vous font réaliser des tâches complexes souvent déroutantes afin de vous convaincre que votre ordinateur est infecté. Par exemple, ils peuvent vous demander si vous avez certains fichiers sur votre ordinateur et vous indiquent ensuite comment les trouver. Lorsque vous les trouvez, votre interlocuteur vous assure que ces fichiers prouvent que votre ordinateur est infecté, alors que ce sont souvent des

Ingénierie Sociale

fichiers systèmes que l'on peut trouver sur presque tous les ordinateurs du monde. Lorsqu'il vous a convaincu que votre ordinateur est infecté, il vous met la pression pour acheter leur anti-virus ou pour leur laisser la main à distance sur votre machine afin de régler le problème. Si vous achetez ce logiciel, non seulement celui-ci est faux, mais il s'agit d'un virus venant infecter pour de bon votre ordinateur. Si vous leur donnez un accès distant à votre machine, ils vont en prendre le contrôle, voler vos données pour en faire ce qu'ils veulent.

Le bon sens est votre principale arme pour identifier et arrêter presque toutes les attaques d'ingénierie sociale.

Un autre exemple parlant est celui de la fraude au président, celle-ci arrive principalement lorsque vous êtes au bureau. Il s'agit d'une attaque ou les pirates identifient via internet le nom de vos collègues ou de votre directeur. Les attaquants forgent ensuite un email prétendument de la part de la personne identifiée et vous l'envoie. Cet email vous demande une action urgente telle que l'envoi d'un virement ou l'envoi d'informations confidentielles. En général ces emails prétendent qu'il y a une urgence et qu'il faut absolument le faire quitte à ignorer les procédures de sécurité en place. Cela peut-être l'envoi des documents ou informations à une adresse en @gmail.com. Ce qui rend ces attaques particulièrement dangereuses c'est que les pirates sont très bien renseignés en amont. De plus, les anti-virus ou les firewalls ne peuvent pas détecter ce type d'attaques car il n'y a pas de virus ou malware.

Il faut garder en tête que les attaques par ingénierie sociale comme celle-ci ne sont pas limitées aux mails ou appels téléphoniques, mais qu'elles peuvent prendre d'autres formes telles que des SMS, des messages sur les réseaux sociaux, voire même en direct. Connaître les techniques des pirates et identifier les éléments clés de ce type d'attaque sont la meilleure défense que vous pouvez avoir.

Détecter et arrêter des attaques d'ingénierie sociale

Heureusement, bloquer ce type d'attaque est très simple. N'importe quelle action sortant de l'ordinaire ou qui vous semble suspicieuse peut-être un signe avant-coureur d'une attaque. Voici les éléments les plus courants pouvant vous mettre la puce à l'oreille :

- Une personne arguant d'une urgence absolue peut essayer de vous faire commettre une erreur.

Ingénierie Sociale

- Une personne vous demandant des informations auxquelles elle n'a pas accès ou alors auxquelles elle devrait avoir accès.
- Une personne vous demandant votre mot de passe. Aucun organisme ne vous le demandera jamais.
- Une personne vous demandant de ne pas respecter une procédure de sécurité pourtant obligatoire.
- Une occasion trop belle pour être vraie. Par exemple si vous recevez un mail ou un pop-up vous indiquant que vous avez gagné un IPad ou à la loterie même si vous n'avez jamais joué.
- Si vous recevez un email surprenant de la part d'un collègue ou d'un ami rédigé bizarrement. Un pirate peut avoir piraté leur compte et essaye de vous tromper. Afin d'être sûr n'hésitez pas à le contacter par un autre biais tel que le téléphone pour vérifier que c'est bien lui qui vous a écrit.

Si vous avez des doutes, il faut absolument couper toutes vos communications avec la personne. Si c'est une attaque survenant sur votre lieu de travail, communiquez avec le service informatique ou la sécurité immédiatement. Vous n'êtes peut-être pas le seul visé. La vigilance et le bon sens sont souvent votre meilleure défense.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients. Pour en savoir plus, veuillez vous référer aux liens suivants : http://www.answer.ch et http://answersecurity.com/

Sources

Phishing :	https://securingthehuman.sans.org/ouch/2015#december2015
L'arnaque au président :	https://securingthehuman.sans.org/ouch/2016#july2016
Les Ransomware :	https://securingthehuman.sans.org/ouch/2016#august2016
Les archives OUCH :	https://securingthehuman.sans.org/ouch/archives

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduit par : Marilyn Combet