OUCH! | Juillet 2016

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

OUCH!

Dans ce numéro...

La fraude au Président

Qu'est-ce que la fraude au Président ?

Les cybercriminels sont sournois, ils développent constamment de nouvelles méthodes en vue d'obtenir ce qu'ils veulent. Une de leurs méthodes les plus efficaces consiste à cibler des gens comme vous. Les Cyber attaquants ont appris que les gens ignorants sont le maillon le plus faible de toute organisation, ils ont cependant oublié que les personnes bien informées comme par exemple les lecteurs de la newsletter OUCH! peuvent être la meilleure défense d'une organisation.

Editeur invité

Angela Pappas est directrice de la formation et de la sensibilisation de la Sécurité de l'Information à Thomson Reuters. Dans le cadre de ses fonctions, Angela est responsable du programme dédié aux ambassadeurs, de leur formation en ligne et de l'éducation des employés sur le phishing.

Les cybercriminels ont développé une nouvelle attaque appelée « la fraude au Président », également connue sous le nom Business Email Compromise (BEC). Dans ces attaques, un cybercriminel prétend être un PDG ou un autre cadre supérieur de votre organisation. Les criminels envoient un e-mail au personnel pour essayer de les tromper en lui faisant faire quelque chose qu'il ne devrait pas faire. Ces types d'attaques sont extrêmement efficaces parce que les cybercriminels font des recherches pointues et pertinentes. Ils recherchent par exemple le site Web de votre entreprise afin d'obtenir des informations telles que l'endroit où elle se trouve, qui sont vos cadres, et peuvent également cibler d'autres organisations avec lesquelles vous travaillez. Les cybercriminels apprennent ensuite tout ce qu'ils peuvent au sujet de vos collègues par le biais de sites tels que LinkedIn, Facebook ou Twitter. Une fois qu'ils connaissent la structure de votre organisation, ils commencent à rechercher et à cibler les employés spécifiques. Ils choisissent ainsi leurs cibles en fonction de leurs objectifs spécifiques. Si les cybercriminels sont à la recherche d'argent, ils peuvent cibler le personnel du service des comptes fournisseurs. Si ils sont à la recherche d'informations fiscales, ils peuvent alors cibler le département des Ressources Humaines. S'ils veulent avoir accès à des serveurs de base de données, ils pourront ainsi cibler quelqu'un dans le service informatique.

Une fois qu'ils ont déterminé ce qu'ils veulent et qui ils vont cibler, ils commencent l'élaboration de leur attaque. Le plus souvent, ils utilisent le Spear phishing. Le phishing c'est quand un attaquant envoie un email à des millions de personnes dans le but de les inciter à faire quelque chose, comme par exemple ouvrir une pièce jointe infectée ou encore visiter un site Web malveillant. Le Spear phishing est similaire à l'hameçonnage (phishing); cependant, au lieu d'envoyer un courriel générique à des millions de

La fraude au Président

personnes, un email personnalisé ciblant un nombre restreint de personnes est envoyé. Ces courriels d'hameçonnage sont extrêmement réalistes et difficiles à détecter. Ils semblent souvent provenir de quelqu'un que vous connaissez, comme d'un collègue de travail ou peut-être même de votre patron. Les e-mails semblent réalistes car ils peuvent utiliser le même jargon que vos collègues utilisent; ils peuvent aussi utiliser le logo de votre organisation ou même la signature officielle d'un de ses dirigeants. Ces e-mails créent souvent un énorme sentiment d'urgence, vous demandant de prendre des mesures immédiates et de n'en parler à personne. L'objectif du cybercriminel est de vous précipiter à commettre une erreur. Voici trois scénarios courants:

La fraude au Président est une puissante attaque qui peut contourner la plupart de nos défenses de sécurité. En fin de compte, vous êtes notre meilleure défense.

- **Virement bancaire**: Un cybercriminel recherche de l'argent. Cela signifie qu'il va rechercher qui travaille dans le département en charge des comptes créditeurs ou l'équipe qui gère les finances de votre organisation. Les criminels conçoivent et envoient un email prétendant être leur patron; l'e-mail leur dit qu'il y a une situation d'urgence et de l'argent doit être transféré immédiatement sur un certain compte.

- **Fraude fiscale**: Les cybercriminels veulent voler des informations sur vos collègues afin qu'ils puissent usurper leur identité pour fraude fiscale. Ils recherchent votre organisation et déterminent qui gère l'information des employés, par exemple, quelqu'un dans les ressources humaines. De là, les cybercriminels envoient de faux emails prétendant être un cadre supérieur ou peut-être quelqu'un de droit, exigeant certains documents devant leur être fournis immédiatement.

- **Usurpation d'identité** : toutes les attaques relatives à des fraudes au Président impliquent non seulement l'utilisation d'email; cependant, d'autres méthodes comme le téléphone peuvent également être utilisées. Dans ce scénario, les criminels commencent par vous envoyer un courriel prétendant être un dirigeant, vous informant qu'un avocat prendra contact avec vous par téléphone concernant une question urgente. Le criminel vous appelle en se faisant passer pour un avocat. Le criminel crée ainsi un énorme sentiment d'urgence dans sa façon de s'exprimer, vous posant des questions confidentielles sensibles au facteur temps. Ce sentiment d'urgence vous incite à agir tout de suite.

La fraude au Président

Savoir se protéger

Alors, que pouvez-vous faire pour vous protéger vous et votre organisation? Le bon sens est votre meilleure défense. Si vous recevez un message de votre patron ou de votre collègue et que cela sonne faux, il peut s'agir une attaque. Les indices peuvent inclure un énorme sentiment d'urgence, une signature qui ne semble pas juste, une certaine tonalité à laquelle vous ne vous attendiez pas, ou encore le nom utilisé dans l'e-mail est différent de celui de la personne qui vous appelle en réalité. Un autre indice serait que l'attaquant utilise un numéro de téléphone ou une adresse e-mail que vous n'aviez jamais vue auparavant, ou encore qu'il utilise une adresse de courrier électronique très similaire mais pas exactement la même que celle de votre collègue ou votre patron. En cas de doute, appelez la personne à un numéro de téléphone de confiance ou rencontrez-la (ne pas répondre par e-mail) et confirmez avec elle s'il elle a bien envoyé l'e-mail. Ne contournez jamais les politiques ou les procédures de sécurité. Votre organisation peut en effet avoir des politiques qui définissent les procédures appropriées pour autoriser le transfert de fonds ou de la divulgation de renseignements confidentiels. Les demandes qui tentent de contourner ces politiques, quelle que soit leur source apparente, devraient être considérées comme suspectes et vérifiées avant toute action. Si vous recevez une telle demande et que vous n'êtes pas sûr de ce qu'il faut faire, communiquez avec votre superviseur, le service d'assistance ou avec l'équipe de sécurité de l'information tout de suite.

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

Ingénierie sociale :	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201411_fr.pdf
L'hameçonnage :	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_fr.pdf
Qu'est-ce qu'un Malware :	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_fr.pdf
La vérification en deux étapes :	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201509_fr.pdf
Conseil du jour :	https://www.youtube.com/watch?v=E5FEqGYLL0o

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