Le bulletin mensuel de sensibilisation à la sécurité pour vous

Escroqueries personnalisées

Vue d'ensemble

Les cybercriminels continuent de proposer de nouvelles façons créatives de duper les gens. Un nouveau type d'escroquerie gagne en popularité: il s'agit d'escroqueries personnalisées. Les cybercriminels recherchent ou achètent des informations sur des millions de personnes, puis les utilisent pour personnaliser leurs attaques. Ci-dessous, nous vous montrons comment fonctionnent ces escroqueries et vous guidons à travers plusieurs exemples courants. Plus vous en savez sur ces escroqueries, plus il vous sera facile de les repérer et de les arrêter.

Comment cette escroquerie fonctionne?

Les escroqueries par courrier électronique ou par appel téléphonique ne sont pas nouvelles, les cybercriminels tentent en effet de duper les gens de cette manière depuis des années. Les exemples incluent le «Vous avez gagné à la loterie» ou les escroqueries d'un Prince nigérian. Cependant, avec ces escroqueries traditionnelles, les cybercriminels ne savent pas à qui ils s'adressent. Ils créent simplement un message générique et l'envoient à des millions de personnes. Parce que ces escroqueries sont justement génériques, elles sont généralement faciles à repérer. Une arnaque personnalisée est différente, les cybercriminels effectuent d'abord des recherches et créent un message personnalisé pour chaque victime visée. Pour ce faire, ils recherchent ou achètent une base de données de noms de personnes, mots de passe, numéros de téléphone ou autres détails personnels. Ce type d 'information est facilement disponible en raison de tous les sites Web qui ont été piratés. Ces informations sont également couramment disponibles sur les sites de médias sociaux et dans les archives gouvernementales accessibles au public. Les criminels ciblent ensuite toutes les personnes sur lesquelles ils disposent d'informations.

Les cybercriminels ont souvent recours à la ruse ou à l'extorsion pour vous forcer à leur donner de l'argent. L'attaque fonctionne comme suit. Ils trouvent ou achètent des informations sur les identifiants de connexion et les mots de passe des personnes obtenus à partir de sites Web piratés. Ils trouvent les informations de votre compte incluses dans une base de données et vous envoient (ainsi qu'à tous les autres utilisateurs de la base de données) un e-mail contenant des informations personnelles vous concernant, y compris le mot de passe d'origine utilisé sur le site piraté. Le criminel qualifie votre mot de passe de «preuve» du piratage de votre ordinateur ou de votre appareil, ce qui n'est bien sûr pas vrai. Le criminel affirme ensuite que pendant qu'il piratait votre ordinateur, il vous a surpris en train de regarder de la pornographie en ligne. Il vous fait alors parvenir un courrier électronique par lequel il vous menace de partager avec votre famille et vos amis ces activités embarrassantes si vous ne payez pas ses frais d'extorsion.

Le problème, c'est que dans presque toutes les situations de ce type, le cybercriminel n'a jamais piraté votre système. Il ne sait même pas qui vous êtes ni quels sites Web vous avez visités. L'escroc tente simplement d'utiliser les quelques données

personnelles dont il dispose sur vous pour vous faire peur en vous faisant croire qu'il a piraté votre ordinateur ou votre appareil, et pour vous amener à lui donner de l'argent. Rappelez-vous, les criminels peuvent utiliser les mêmes techniques pour une arnaque téléphonique également.

Que dois-je faire?

Il s'agit d'abord d'identifier les courriels ou les appels téléphoniques comme étant une arnaque. C'est naturel d'avoir peur quand quelqu'un détient des informations personnelles sur vous. Cependant, rappelez-vous que l'expéditeur ment. L'attaque fait partie d'une campagne de masse automatisée et ne vise pas à vous cibler directement. Il est aujourd'hui beaucoup plus facile pour les cybercriminels de trouver ou d'acheter des informations personnelles, alors attendez-vous à d'autres escroqueries personnalisées comme celles-ci à l'avenir. Voici quelques indices que vous pouvez repérer.

⚠

- **Chaque fois que vous recevez un e-mail, un message ou un appel téléphonique extrêmement urgent, soyez très suspicieux. Si quelqu'un utilise des émotions comme la peur ou l'urgence, il essaie de vous pousser à commettre une erreur.**
- **Quand quelqu'un demande un paiement en BitCoin, par cartes-cadeaux ou par d'autres méthodes introuvables.**
- **Lorsque vous recevez un courrier électronique suspect, effectuez une recherche sur Google pour voir si d'autres personnes ont signalé des attaques similaires.**

Le problème, c'est que dans presque toutes les situations de ce type, le cybercriminel n'a jamais piraté votre système. Il ne sait même pas qui vous êtes ni quels sites Web vous avez visités. L'escroc tente simplement d'utiliser les quelques données personnelles dont il dispose sur vous pour vous faire peur en vous faisant croire qu'il a piraté votre ordinateur ou votre appareil, et pour vous amener à lui donner de l'argent. Rappelez-vous, les criminels peuvent utiliser les mêmes techniques pour une arnaque téléphonique également.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Lenny Zeltser *est un vétéran de la cybersécurité. Il conçoit des solutions anti-malware à Minerva Labs et donne des cours de sécurité au SANS Institute. Son expérience intègre également des services de sécurité gérés et du conseil. Suivez-le sur* zeltser.com/blog *et sur Twitter* @lennyzeltser.

Sources

Ingénierie sociale :	https://www.sans.org/u/MUU
Stop au phishing :	https://www.sans.org/u/MUZ
Cherchez-vous en ligne :	https://www.sans.org/u/MV4
Gestionnaire de mots de passe :	https://www.sans.org/u/MV9

Comité de rédaction : Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Traduit par : Marilyn Combet