Publicația dumneavoastra lunară de sensibilizare asupra securității informatice

Escrocherii personalizate

Prezentare generală

Criminalii cibernetici continuă să inventeze metode noi și creative de a păcăli oamenii. Un nou tip de escrocherii câștigă popularitate – escrocheriile personalizate. Atacatorii găsesc sau cumpără informații despre milioane de oameni, apoi folosesc acele informații pentru a-și personaliza atacurile. Mai jos vă arătăm cum funcționează aceste escrocherii și vă vom prezenta un exemplu des întâlnit. Cu cat știți mai multe despre aceste escrocherii, cu atât este mai ușor să le observați și să le opriți.

Cum funcționează?

Înșelătoriile prin e-mail sau telefon nu sunt noi, infractorii cibernetici încercând să păcălească oamenii de ani de zile. Exemplele includ “Ați câștigat la loto” sau infama escrocherie cu prințul nigerian. Însă, în cazul acestor escrocherii, infractorii nu vizează pe cineva anume. Ei doar creează un mesaj generic și îl trimit către milioane de oameni. Deoarece aceste escrocherii sunt generice, ele sunt de obicei ușor de observat. O înșelătorie personalizată este diferită, infractorii cibernetici făcând cercetări preliminare și creând un mesaj personalizat pentru fiecare victimă. Ei fac acest lucru prin găsirea sau achiziționarea unei baze de date cu nume, parole, numere de telefon sau alte detalii. Aceste informații sunt ușor de accesat datorită multitudinii de site-uri care au fost deja atacate (hacked). De asemenea, pot fi disponibile pe site-uri de socializare sau în documente oficiale publice. Criminalii vizează apoi toate persoanele despre care au informații.

Atacatorii cibernetici folosesc frica sau constrângerea pentru a vă forța să le dați bani. Atacul funcționează in felul următor. Găsesc sau cumpără informații despre utilizatori și parole obținute de pe site-urile deja „hacked”. Găsesc informații despre contul dvs. într-o astfel de bază de date și vă trimit (dvs. și tuturor celorlalți găsiți în baza de date) un e-mail cu câteva detalii personale, inclusiv parola originală pe care ați folosit-o pe site-ul hacked. Atacatorii menționează parola dvs. ca și “dovadă” ca v-au spart computerul, ceea ce, desigur, nu este adevărat. Mai pot susține apoi că, în timp ce v-au accesat computerul, v-au surprins vizionând pornografie online. Și vă amenință că, dacă nu ii plătiți, vor arăta familiei și prietenilor dvs. dovezile jenante.

Tertipul este că, în aproape toate situațiile de genul acesta, hacker-ii nu v-au spart sistemul. Nici măcar nu știu cine sunteți sau ce site-uri ați vizitat. Ei încearcă pur și simplu să folosească câteva detalii personale pe care le au despre dvs., să vă

sperie că v-au spart computerul și să vă constrângă să-i plătiți. Țineți cont că se pot folosi aceleași tehnici și pentru înșelătorii prin telefon.

Ce ar trebui să fac?

Fiți conștient(ă) ca genul acesta de e-mailuri sau apeluri telefonice sunt escrocherii. Este normal să vă speriați când cineva are informații personale despre dvs. Cu toate acestea, nu uitați că expeditorul minte. Atacul este parte dintr-o campanie automatizată pe scară largă, nu o încercare de a vă viza în mod direct. Este din ce în ce mai ușor pentru infractorii cibernetici să găsească sau să cumpere informații personale, așa că așteptați-vă la mai multe escrocherii personalizate pe viitor. Aveți mai jos câteva indicii pentru a le recunoaște.

- **De fiecare dată când primiți un e-mail, un mesaj sau un apel telefonic extrem de urgent, fiți suspicioși. Dacă cineva folosește emoții precum frica sau urgența, atunci încearcă să vă grăbească să faceți o greșeală.**
- **Când cineva vă solicită plata în BitCoin (monedă virtuală), carduri cadou sau alte metode nedetectabile.**
- **Când primiți un e-mail suspect, căutați pe Google dacă alte persoane au raportat astfel de atacuri.**

În cele din urmă logica este cea mai bună apărare. Cu toate astea însă, vă recomandăm să utilizați întotdeauna o parolă unică și lungă pentru fiecare dintre conturile dvs. online. Nu vă puteți aminti toate parolele? Utilizați un program de gestiune a parolelor. În plus, activați verificarea în doi pași („two-step verification") ori de câte ori este posibil.

Versiunea în limba română

Ubisoft este o companie de jocuri. Un creator de lumi, dedicat îmbogățirii vieților jucătorilor cu experiențe de joc originale și memorabile. Aflați mai multe la: https://www.ubisoft.com/en-us/.

Editor invitat

Lenny Zeltser *este un veteran al securității cibernetice. Creează soluții anti-malware la Minerva Labs și predă cursuri de securitate informatică la Institutul SANS. Experiența lui include și gestiunea de servicii de securitate și consultanță. Urmăriți-l pe* zeltser.com/blog *și pe Twitter* @lennyzeltser.

Resurse

Inginerie socială:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_ro.pdf
Opriți atacurile phishing:	https://www.sans.org/sites/default/files/2018-04/201804-OUCH-April-Romanian_0.pdf
Căutați-vă online:	https://www.sans.org/sites/default/files/2019-01/201901-OUCH-January-Romanian.pdf
Programele de gestiune a parolelor:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_ro.pdf