SANS SECURITY AWARENESS

OUCH!

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

Atacurile și escrocheriile telefonice

Generalități

Atunci când vă gândiți la infractorii cibernetici probabil vă imaginați un coordonator malefic stând după un calculator și lansând atacuri sofisticate prin Internet. Deși mulți dintre răufăcătorii de azi folosesc, într-adevăr, tehnologii precum email-ul sau programele de mesagerie instantanee, indivizii rău famați folosesc de asemenea și telefonul pentru a-și păcăli victimele. Există două avantaje semnificative ale utilizării telefonului. În primul rând, spre deosebire de email, există mai puține soluții tehnice de monitorizare a apelurilor telefonice care să poată detecta și opri un atac. Apoi, este mult mai ușor pentru răufăcători să transmită o emoție prin telefon, ceea ce face mult mai probabil să-și păcălească victimele. Să învățăm, așadar, cum să depistăm și să oprim aceste atacuri.

Cum funcționează atacurile prin telefon?

Mai întâi trebuie să înțelegeți ce urmăresc acești atacatori. De obicei vă vor banii, informații sau acces la calculatorul dumneavoastră, sau pe toate trei. Fac asta păcălindu-vă să faceți cea ce urmăresc. Răufăcătorii sună la telefon oameni din întreaga lume, creând o stare ce pare a fi o urgență. Vor să vă răvășească speriindu-vă, ca să nu gândiți limpede, apoi vă zoresc să faceți o greșeală. Unele dintre cele mai frecvente exemple sunt:

Cel care sună pretinde că este de la administrația financiară sau agenția națională de administrare fiscală spunând că aveți taxe neplătite. Apoi explică riscul de a ajunge în închisoare dacă nu plătiți imediat, apoi pun presiuni să plătiți aceste taxe cu un card bancar prin telefon. Aceasta este o escrocherie, căci multe administrații financiare, inclusiv ANAF, nu sună și nici nu trimit email cetățenilor. Toate înștiințările oficiale se trimit prin poștă.

Apelantul pretinde că este reprezentant al serviciului de suport tehnic Microsoft și vă spune că aveți calculatorul infectat. Odată ce v-au convins de asta, insistă să le cumpărați programul software sau să le dați accesul de la distanță la calculatorul dumneavoastră. Microsoft nu v-ar suna niciodată acasă.

Primiți un mesaj înregistrat pe căsuța de mesaje audio potrivit căruia contul bancar v-a fost blocat, și că trebuie să sunați la un anumit număr pentru reactivarea contului. Atunci când sunați sunteți întâmpinați de un sistem automat care solicită să confirmați identitatea dumneavoastră, întrebându-vă o mulțime de lucruri personale. Acesta nu este în realitate banca dumneavoastră, ei pur și simplu înregistrează toate informațiile personale pentru furt de identitate.

Protejați-vă

Cea mai bună defensivă pe care o aveți în fața apelurilor telefonice frauduloase sunteți voi înșivă. Țineți minte următoarele lucruri:

Ori de câte ori vă sună cineva pe un ton deosebit de urgență, cerându-vă insistent să faceți ceva, fiți extrem de suspicioși. Chiar și dacă apelul telefonic pare în regulă în primă instanță, dar apoi începe să sune ciudat, puteți să vă opriți și să spuneți „nu” oricând.

Dacă aveți senzația că un apel telefonic primit este o escrocherie, pur și simplu închideți. Dacă vreți să verificați dacă apelul a fost unul legitim, mergeți pe site-ul organizației (cum ar fi cel al băncii) și obțineți numărul de telefon al serviciului de relații cu clienții și sunați-i dumneavoastră direct. În acest fel știți sigur că vorbiți cu organizația adevărată.

Nu dați crezare niciodată numărului afișat al apelantului, răuvoitorii îl pot contraface, ca să arate ca și cum apelul vine din partea unei organizații legitime, sau are un prefix telefonic identic cu al dumneavoastră.

Nu permiteți unui apelant să preia temporar controlul asupra calculatorului dumneavoastră sau să vă păcălească să descărcați un program software. Așa vă infectează răufăcătorii calculatorul.

Dacă primiți un apel telefonic de la o persoană necunoscută, lăsați apelul să intre pe căsuța de mesaje vocale. În acest fel puteți verifica apelurile necunoscute atunci când aveți timp. Și mai bine, pe multe telefoane puteți activa implicit această funcție cu opțiunea “Nu mă deranja”.

Escrocheriile ce se folosesc de atacurile telefonice sunt în creștere. Dumneavoastră sunteți cea mai bună defensivă pe care-o aveți în detecția și stoparea lor.

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Editor invitat

Jen Fox *asigură instruirea asupra securității, servicii de analiză de risc și exerciții de inginerie socială din postura de Consultant Senior la compania All Covered. O puteți găsi pe Twitter la* @j_fox.

Resurse online

Informații pentru consumatori privitoare la Identitate, Confidențialitate și Securitate Online:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security

Raportați o tentativă de fraudă (în SUA): https://www.ftccomplaintassistant.gov/#crnt

Ingineria socială: https://www.sans.org/u/Fi5