Mesečni bilten za podizanje svesti o bezbednosti informacija

Direktorske fišing prevare (CEO fraud)

Šta su direktorske fišing prevare?

Sajber napadači nastavljaju da unapređuju tehnike pecanja korišćenjem mejl poruka navodno poslatih od strane menadžmenta, koje su poznate kao direktorska fišing prevara (eng. CEO Fraud, ili Business Email Compromise (BEC)). Reč je o ciljanim napadima koji navode žrtvu da uradi nešto što ne bi trebalo. U najvećem broju slučajeva sajber kriminalci su zainteresovani za novac. Navedeni napadi su posebno opasni zbog činjenice da se sajber kriminalci, pre nego što zapravo pokrenu napad, prvo dobro upoznaju sa kompanijom koja je njihova potencijalna žrtva, kako bi fišing mejl bio što uverljiviji. S druge strane, sistemi IT bezbednosti i zaštite teško mogu da zaustave ove napade jer fišing poruka ne sadrži maliciozne priloge ni linkove koje bi ti sistemi mogli automatski da prepoznaju. U nastavku je detaljnije objašnjeno kako ovi napadi funkcionišu.

Sajber napadači koriste internet kako bi prikupili informacije o potencijalnoj žrtvi kao i o osobama sa kojima žrtva sarađuje. Na primer, ako ciljaju vas, onda će istražiti ko vam je šef ili poslovni partner s kojim radite. Napadači potom kreiraju i šalju mejl koji izgleda kao da ga je napisao neko od njih. U mejlu se od vas zahteva da hitno uradite nešto što je zapravo cilj napada, na primer da obavite prenos novca na račun na koji nikad ranije niste uplaćivali, ili da u odgovoru na mejl dostavite osetljive informacije ili dokumenta. U nastavku su dva primera ovakvih napada:

Prenos novca: Cilj sajber kriminala je novac. Sajber kriminalci istražuju kompaniju za koju radite sa namerom da pronađu koje osobe su u kompaniji zadužene za plaćanje računa i prenos novca. Potom kreiraju mejl i šalju ga ovim zaposlenima pretvarajući se da su njihov šef ili direktor. U mejlu se pod izgovorom hitnosti zahteva da se novac prebaci na neki nepoznat bankovni račun, čime se zaposleni požuruju da načine grešku i novac zapravo pošalju sajber kriminalcu.

Poreske prevare: Sajber kriminalci žele da pribave podatke o ličnosti osoba koje će iskoristiti da pokušaju poresku prevaru. Najbrži način da do ovih podataka dođu je krađa podataka o ličnosti svih zaposlenih u kompaniji. Sa tim ciljem napadači se prvo informišu o tome ko su zaposleni u Ljudskim resursima, a potom im upućuju lažni mejl, pretvarajući se da su njihov nadređeni rukovodilac ili možda neko iz pravnih poslova. Mejl sadrži zahtev da se hitno dostave podaci o zaposlenima kako bi im što pre bila prosleđena poreska rešenja. Zaposleni u Ljudskim resursima su uvereni da podatke šalju svom pretpostavljenom, a zapravo ih dostavljaju sajber kriminalcu.

Kako da se zaštitite

Šta da učinite kako biste se zaštitili? Zdrav razum je vaša najbolja odbrana. Očigledni znaci koji ukazuju na prevaru su:

Mejl je hitan i veoma kratak (često sadrži svega nekoliko rečenica), a u potpisu stoji da je poslat sa mobilnog uređaja.

Stvara se jak osećaj hitnosti, kojim vas pritiskaju da zanemarite ili zaobiđete korporativna pravila. Uvek poštujte uspostavljene politike i procedure, pa čak i ako deluje da je mejl napisao vaš šef ili čak izvršni direktor.

Mejl je poslovne sadržine, ali je poslat sa privatne mejl adrese, sa domena poput @gmail.com ili @hotmail.com.

Mejl izgleda kao da ga je poslao vođa tima, kolega ili poslovni partner koga znate ili sa kojim radite, ali je ton poruke takav da sumnjate da ga je zaista poslao taj neko.

Priložene instrukcije za plaćanje se razlikuju od onih koje ste dobili ranije, npr. traži se hitno plaćanje na neki novi bankarski račun.

Ako sumnjate da ste meta napada na poslu, prekinite odmah svaku interakciju sa napadačem i prijavite to vašem nadređenom rukovodiocu. Ako ste privatno bili meta napada i prenos novca je već izvršen, prijavite to odmah vašoj banci, a potom i policiji.

Verzija na srpskom

Telekom Srbija kao društveno odgovorna telekomunikaciona kompanija pomaže prevođenje i distribuciju ovog biltena kako bi se unapredila svest korisnika informaciono-komunikacionih tehnologija o bezbednosti informacija.

Gost urednik

Don Kavender *je bivši specijalni agent FBI, sa više od 22 godine iskustva na polju digitalne forenzike i sajber kriminala. U poslednje vreme se bavi otkrivanjem sajber kriminalnih organizacija sa pozicije koordinatora za direktorske fišing prevare grada Vašingtona. Sprovodi obuke i istraživanja u navedenim oblastima, aktivan je na Tviteru kao @don_cavender, a više možete saznati na njegovom profilu https://www.linkedin.com/in/donald-cavender.*

Dodatni materijal

Socijalni inženjering:	https://www.sans.org/u/HE3
Ne dajte se upecati:	https://www.sans.org/u/HE8
Zaštitite se od malvera:	https://www.sans.org/u/HEd
Obezbedite svoj nalog:	https://www.sans.org/u/HEi