Vaš mese ni bilten za podizanje svesti o bezbednosti informacija

Personalizovane prevare

Uvod

Sajber kriminalci stalno smišljaju nove i kreativne načine da prevare ljude. Sve popularniji tip prevara su personalizovane prevare. Kod ovog tipa prevare sajber kriminalci pronalaze ili kupuju informacije o milionima ljudi, a zatim te informacije koriste da personalizuju svoje napade. U tekstu u nastavku saznaćete kako funkcionišu ove prevare i kako izgleda jedan tipičan primer. Što više znate o ovim prevarama, lakše ćete ih uočiti i zaustaviti.

Kako funkcioniše ovaj tip prevare?

Prevare putem elektronske pošte ili telefona nisu nove i sajber kriminalci ih koriste godinama unazad. Neki od poznatih primera ovih prevara su “You Won the Lottery” (Dobili ste na lutriji) ili ozloglašeni „Nigerijski Princ“. Međutim, u ovim tradicionalnim prevarama sajber kriminalci ne znaju na koga tačno ciljaju. Oni jednostavno naprave generičku poruku i pošalju je milionima ljudi. Budući da su ove prevare toliko široko rasprostranjene, one obično brzo postanu lako uočljive. Personalizovana prevara je drugačija, u tom slučaju sajber kriminalci prvo istražuju a zatim kreiraju prilagođenu poruku za svaku pojedinačnu žrtvu. Oni to čine tako što pronalaze ili kupuju baze podataka sa imenima ljudi, lozinkama, telefonskim brojevima ili drugim informacijama. Ove informacije su lako dostupne zahvaljujući veb sajtovima koji su hakovani. Takođe, do njih se može doći i preko društvenih mreža ili javno dostupnih sajtova državnih organa, agencija ili organizacija. Kriminalci zatim napadaju osobe čije informacije poseduju.

Jedan od uobičajenih trikova koji sajber kriminalci koriste kako bi vas naterali da im platite je zastrašivanje ili ucena. Napad se realizuje na sledeći način. Sajber kriminalci pronalaze ili kupuju informacije o nalozima i lozinkama sa hakovanih sajtova. U ovoj bazi podataka oni nalaze informacije o vašem nalogu i šalju vam, kao i svima ostalima u bazi, mejl koji sadrži vaše lične podatke, uključujući i originalnu lozinku koju ste koristili na hakovanom veb sajtu. Kriminalac se poziva na vašu lozinku kao “dokaz” da je hakovao vaš računar ili uređaj, što naravno nije istina. Zatim, kriminalac tvrdi da su vas, dok su hakovali vaš kompjuter, zatekli kako gledate pornografiju na internetu. U mejlu vam prete da će, ukoliko ne platite koliko traže, vašoj porodici i prijateljima poslati dokaze o vašim kompromitujućim aktivnostima na internetu.

U skoro svakoj situaciji poput ove, začkoljica je u tome da sajber kriminalac zapravo nikada nije hakovao vaš sistem. Oni čak i ne znaju ko ste i koje veb sajtove posećujete. Prevaranti jednostavno pokušavaju da iskoriste tih nekoliko ličnih podataka koje o vama imaju da bi vas uplašili i naveli da poverujete da su hakovali vaš računar ili uređaj, a sa ciljem da kroz prevaru na vama zarade. Imajte na umu, ove iste tehnike se mogu koristiti i za prevare putem telefonskog poziva.

Šta preduzeti?

Budite svesni da su opisani mejlovi ili telefonski pozivi čista prevara. Prirodno je da osećate strah kada neko poseduje lične podatke o vama. Međutim, imajte na umu da pošiljalac ne iznosi istinu. Napad je deo automatizovane masovne kampanje, i nije usmeren samo ka vama. Sajber kriminalcima je danas sve lakše da pronađu ili kupe lične podatke, tako da u budućnosti možete očekivati više personalizovanih prevara poput ovih. Neki od znakova koji upućuju na to da je u pitanju prevara su:

- **Kad god primite mejl, poruku ili telefonski poziv koji je izuzetno hitan, budite veoma oprezni. Ako neko koristi emocije poput straha ili osećaja hitnosti, on time pokušava da vas požuri da napravite grešku.**
- **Kada neko zahteva plaćanje u bitkoinima, poklon karticama ili drugim metodama koje se ne mogu pratiti.**
- **Kada dobijete sumnjivi mejl, proverite na Guglu da li su i drugi ljudi prijavili slične napade.**

Na kraju krajeva zdrav razum je vaša najbolja odbrana. Međutim, takođe preporučujemo i da uvek koristite jedinstvenu, dugačku lozinku za svaki vaš nalog na internetu. Ne možete da se setite svih vaših lozinki? Koristite menadžer lozinki. Osim toga, omogućite i verifikaciju u dva koraka kad god je to moguće.

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

Leni Zelcer *je veteran u oblasti sajber bezbednosti. On se bavi kreiranjem rešenja za zaštitu od malvera u kompaniji Minerva Labs i predaje na SANS Institutu. Leni je aktivan na Tviteru kao* @lennyzeltser *i autor je bloga o sajber bezbednosti* zeltser.com/blog.

Dodatne informacije

Socijalni inženjering:	https://www.sans.org/u/MUU
Ne dajte se upecati:	https://www.sans.org/u/MUZ
Potražite informacije o sebi na internetu:	https://www.sans.org/u/MV4
Menadžeri lozinki:	https://www.sans.org/u/MV9