OUCH! | Decembar, 2018

SANS SECURITY AWARENESS

OUCH!

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Da, vi ste meta sajber napada

Uvod

Mnogo ljudi pogrešno veruje da oni nisu meta sajber napadača, i da oni, njihovi sistemi ili nalozi nemaju nikakvu vrednost. Takvo uverenje je daleko od istinitog i opravdanog. Ako na bilo koji način koristite tehnologiju, bilo da je to na poslu ili kod kuće, budite sigurni da vi imate vrednost za sajber kriminalce. Srećna okolnost je da već imate najbolju odbranu od ovih napada koja postoji – vas same.

Zašto ste vi meta

Postoje različite vrste sajber napadača na internetu danas, i svi oni imaju različite motive. Zašto bi neko od njih uopšte želeo da napadne baš vas? Zato što im to pomaže da postignu svoj cilj. U nastavku su dva uobičajena primera sajber napadača i razloga zašto bi ciljali vas.

Sajber kriminal: Cilj napadača u ovom slučaju je da izvuku što više novca. Zahvaljujući sve dostupnijem Internetu, oni veoma lako mogu da ciljaju bilo koga na svetu. Pritom, nebrojeni su načini na koje od vas mogu zaraditi novac. Primeri uključuju krađu novca sa vaših bankovnih računa, kreiranje kreditne kartice na vaše ime i slanje računa vama na naplatu, korišćenje vašeg računara za hakovanje drugih ljudi, ili hakovanje vaših naloga na društvenim mrežama i onlajn igricama i njihovu prodaju drugim kriminalcima. Lista načina na koje loši momci mogu da zarade na vama je skoro beskonačna. Postoje stotine hiljada ovih loših momaka koji se svakog jutra probude sa ciljem da svakog dana hakuju što je moguće više ljudi, uključujući i vas.

Specijalizovani napadači: Ovo su visoko obučeni sajber napadači, koji često rade za vlade, kriminalne organizacije ili konkurenciju koja kao metu ima kompaniju za koju radite. Možda mislite da vaš posao ne privlači toliko pažnje, ali iznenadili biste se kad biste znali koliko je on konkurenciji interesantan.

- Informacije s kojima radite na poslu imaju ogromnu vrednost za različite kompanije ili vlade.

- **Specijalizovani napadači mogu da vas ciljaju na poslu ne zato što žele da hakuju baš vas, već da vas iskoriste da hakuju vaše kolege ili druge sisteme.**
- **Ovaj tip napadača može kao metu napada da ima vas na poslu i zbog kompanija koje su vaši partneri ili s kojim sarađujete.**

Imam antivirus, bezbedan sam

Dobro, znači ja sam meta, nisam problem. Dovoljno je da instaliram antivirus i fajervol na mom računaru i zaštićen sam, zar ne? Nažalost, to nije tačno. Mnogi ljudi smatraju da ako instaliraju neke bezbednosne alate onda su zaštićeni. Nažalost, to nije u potpunosti tačno. Sajber napadači neprestano usavršavaju svoje veštine, i mnoge od njihovih metoda napada sada lako zaobilaze mere zaštite. Na primer, oni često kreiraju specijalni malver koji vaša antivirusna zaštita ne može da detektuje. Oni zaobilaze filtre vaše elektronske pošte pomoću prilagođenog fišing napada ili vas pozovu telefonom i na prevaru vam ukradu podatke o platnoj kartici, novac ili lozinku. Tehnologija igra važnu ulogu u vašoj zaštiti, ali konačno vi ste najbolja odbrana.

Na sreću, nije toliko teško biti bezbedan jer su za to dovoljni zdrav razum i neka osnovna pravila ponašanja. Ako primite mejl, poruku ili telefonski poziv koji je izuzetno hitan, neobičan ili sumnjiv, moguće je da je u pitanju napad. Da biste bili sigurni da su vaši računari i uređaji bezbedni ažurirajte ih redovno, tako što ćete omogućiti automatsko ažuriranje. Na kraju, koristite jake, jedinstvene lozinke za svaki vaš nalog. Vaša najbolja odbrana je svest o sajber bezbednosti. Niste sigurni odakle da počnete? Razmislite da se prijavite na mesečni bilten posvećen bezbednosti OUCH! dostupan na sans.org/ouch.

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

Met Bromili *(@mbromileyDFIR) se bavi rešavanjem incidenata i ekspert je za digitalnu forenziku sa više od 8 godina iskustva u rešavanju incidenata u kompanijama širom sveta. Pored toga, kao SANS instruktor za digitalnu forenziku i rešavanje incidenata, predaje na FOR508 i FOR572 kursevima.*

Dodatne informacije

Zaštitite se od malvera:	https://www.sans.org/u/L1J
Socijalni inženjering:	https://www.sans.org/u/L1O
Telefonski napadi i prevare:	https://www.sans.org/u/L1T
Pristupne fraze:	https://www.sans.org/u/L1Y
Poster - You Are a Target:	https://www.sans.org/u/L23