Mesečni bilten bezbednosnih saveta za korisnike računara

OUCH!

U OVOM IZDANJU...

Sajber pecanje

Uvod

El. pošta je danas jedan od osnovnih načina komunikacije. Osim što je svakodnevno koristimo na poslu, takođe je koristimo i da ostanemo u kontaktu da svojim prijateljima i porodicom. Pored toga komunikacija putem el. pošte je način na koji većina kompanija potvrđuje i pruža svoje on-line usluge, poručivanje putem interneta ili slanje izvoda bankovnog računa. Obzirom da ogroman broj ljudi širom sveta zavisi od svog naloga za el. poštu, vremenom je postao jedna od glavnih meta sajber kriminalaca. U ovom izdanju objasnićemo sajber pecanje, jednu od najčešćih metoda sajber napada, i načine kako da zaštitite svoj nalog za el. poštu.

Gost urednik

Dr. Lance Hayden je generalni direktor Berkeley Research Group. Ekspert je za oblast bezbednosne kulture i ponašanja, i autor People-Centric Security: Transforming Your Enterprise Security Culture od McGraw-Hill-a. Možete ga pratiti i kontaktirati na www.linkedin.com/in/drhayden.

Sajber pecanje

Sajber pecanje podrazumeva napad kod koga se korišćenjem el. pošte ili drugim metodom komunikacije putem poruka, na primer društvene mreže, pokušava da se korisnik prevari i navede na određenu akciju, na primer da klikne na određeni „weblink“ ili otvori prilog. Ako postanete žrtva ovakvog napada rizikujete krađu svojih osetljivih podataka ili da vaš računar bude zaražen virusom. Sajber kriminalci ulažu velike napore da njihova el. pošta izgleda što uverljivije. El. pošta koju šalju može da izgleda kao da dolazi od nekog ili nečeg vama poznatog ili bliskog, na primer nekog vašeg prijatelja ili kompanije u koju imate poverenja. Da bi izgledala uverljivije u takvu el. poštu se obično dodaju logo ili falsifikovana adresa el. pošte kompanije. Takva el. pošta se onda šalje na milione naloga ljudi širom sveta. Unapred se ne zna ko će biti žrtva ovakvog napada ali se zna da na što više naloga se pošta pošalje to je veća mogućnost da se neko upeca. Sajber pecanje je slično ribolovu pomoću mreže, ne znaš unapred šta ćeš da upecaš, ali znaš da što je veća mreža, više ribe možeš da uloviš. Postoje nekoliko načina na koje kriminalci koriste sajber pecanje da bi ostvarili svoj cilj:

- **Žetva informacija (Harvesting Information)**: Cilj sajber kriminalaca je da prikupe lične informacije žrtve kao što su lozinke, brojevi kreditnih kartica ili podaci vezani za bankovne račune. Da bi to postigli šalju el. poštu koja sadrži „weblink“ koji vodi do Internet stranice koja izgleda legitimno. Na Internet stranici se traži da se

Sajber pecanje

unesu informacije o nalogu i lični podaci. Kako je Internet stranica lažna, sve što se unese biće na raspolaganju sajber kriminalcima.

- **Maliciozni „weblink“-ovi (Malicious Links)**: Cilj sajber kriminalaca je da preuzmu kontrolu nad uređajem žrtve. Da bi to postigli šalju el. poštu sa „weblink“-om. Ako se klikne na „weblink“, aktivira se preusmeravanje na Internet stranicu koje pokreće sajber napad na uređaj koji ako je uspešan, inficira sisteme uređaja.
- **Maliciozni prilozi (Malicious Attachments)**: Cilj sajber kriminalaca je isti, da inficiraju i preuzmu kontrolu nad uređajem žrtve. Ali umesto „weblink“-a uz el. poštu šalje se inficirani fajl, na primer dokument u Word-u. Otvaranje priloga aktivira napad, koji ako je uspešan može da obezbedi sajber kriminalcima kontrolu na uređajem žrtve.
- **Prevare (Scams)**: Neki napadi sajber pecanjem su ništa drugo do obične prevare samo u digitalnom obliku. Na primer, lažne poruke o dobitku na lutriji, dobrotvorne akcije koje trebaju donaciju, ili ponuda za pomoć oko transfera miliona dolara. Ako žrtva odgovori na bilo koji od ovakvih predloga ili obaveštenja, dobiće odgovor da je potrebno da prvo izvrši određeno plaćanje za usluge ili da im omogući pristup njenom bankovnom računu, i tako omogući da prebace novac.

Najbolja zaštita je zdrav razum. Ako el. pošta izgleda čudno, sumnjivo, ili previše dobro da bi bilo istina, moguće je da se radi o napadu sajber pecanjem.

Kako se zaštititi

U većini slučajeva, otvaranje i čitanje el. pošte ili poruke je u redu. Da bi sajber pecanje bilo uspešno potrebna je određena akcija, da nešto uradite. Na sreću postoje određene indicije koje mogu da ukažu da se radi o napadu sajber pecanjem. Najčešći primeri kako možete da prepoznate napad:

- El. pošta stvara atmosferu hitnosti, zahteva „hitnu akciju“ pre nego se desi nešto loše, na primer zatvaranje vašeg računa. Sajber kriminalci žele da vas požure da bi ste bez mnogo razmišljanja napravili grešku.
- Dobili ste el. poštu sa prilogom koju niste očekivali ili sam sadržaj pošte mami da otvorite prilog. Primeri mogu da uključuju el. poštu koja ukazuje na prilog sa detaljima nenajavljenih otpuštanja, podacima o platama zaposlenih ili pismo poreske uprave koje ukazuje da će te biti zakonski sankcionisani.
- Umesto da sadrži vaše ime, el. pošta sadrži opšti pozdrav kao „Poštovani korisniče“. Mnoge kompanije ili vaši prijatelji će vam se obratiti vašim imenom.

Sajber pecanje

- El. pošta zahteva veoma osetljive informacije, na primer brojeve kreditne kartice ili lozinke.
- El. pošta izgleda kao da je od zvanične organizacije, ali sadrži lošu gramatiku i pravopis, ili koristi lične adrese el. pošte kao što su @gmail.com, @yahoo.com, or @hotmail.com.
- „Weblink“ izgleda čudno ili ne kao što očekujete. Pređite mišom preko „weblink“-a bez klika i dobićete obaveštenje gde će vas „weblink“ stvarno preusmeriti. Ako se „weblink“ u el. pošti i u obaveštenju ne poklapaju, nemojte ga otvarati. Na mobilnim uređajima zadržite svoj prst duže na „weblink“-u i pojaviće se obaveštenje o stvarnoj destinaciji. Bezbednija solucija podrazumeva da kopirate destinaciju (URL) iz el. pošte u Internet pretraživač ili da sami otkucate destinaciju.
- Dobili ste el. poštu od nekoga koga znate, ali ton i smisao sadržaja ne zvuče kao da je od njega. Ako niste sigurni, pozovite pošiljaoca da proverite da li je pošta stvarno od njega. Za sajber kriminalce je veoma jednostavno da kreiraju poštu koja izgleda da je od vašeg prijatelja ili kolege.

Ako verujete da je el. pošta ili poruka napad sajber pecanjem, jednostavno je obrišite. Na kraju krajeva zdrav razum je vaša najbolja odbrana.

Saznaj Više

Prijavi se na OUCH! mesečni bilten bezbednosnih saveta za korisnike računara, pristupi prethodnim OUCH! izdanjima i saznaj više o SANS rešenjima u vezi svesnosti bezbednosti informacija na našoj internet prezentaciji http://www.securingthehuman.org.

Dodatne informacije

Društveni inženjering:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_se.pdf
Pet ključnih pravila za vašu bezbednost:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201410_se.pdf
Hakovan sam, šta sad?:	https://www.securingthehuman.org/ouch/2014#may2014
OnGuard Online:	https://www.onguardonline.gov/phishing
SANS tip dana:	https://www.sans.org/tip_of_the_day.php

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Preveo: Nenad Varinac