OUCH! Januar 2022

SANS SECURITY AWARENESS

OUCH!

Vaš mesečni bilten za podizanje svesti o bezbednosti informacija

Napadi putem tekstualnih poruka - prepoznajte ih i sprečite

Šta su to napadi putem tekstualnih poruka?

To su napadi za koje sajber kriminalci koriste SMS ili druge servise za razmenu tekstualnih poruka u nameri da vas prevare i navedu da uradite nešto što ne bi trebalo. Ovi napadi poznati su i kao smišing (što predstavlja kovanicu od reči SMS i *phishing*). Tako na primer, mogu pokušati da vas navedu da im odate podatke o vašoj platnoj kartici, da pozovete određeni telefonski broj kako bi prikupili informacije o vašem bankovnom računu, ili vas mogu nagovoriti da popunite onlajn upitnik kako bi ukrali vaše podatke o ličnosti. Kao i u slučaju fišing napada za koje se koristi elektronska pošta (mejl), sajber kriminalci često igraju na kartu vaših emocija kako bi vas, stvarajući osećaj hitnosti ili pobuđujući vašu radoznalost, požurili da načinite grešku. Međutim, ono što napade putem tekstualnih poruka čini posebno opasnim je činjenica da tekstualne poruke, za razliku od mejla, oskudevaju u dodatnim informacijama i tragovima na osnovu kojih biste mogli da primetite da nešto nije u redu.

Često ovaj tip prevare započinje tako što dobijete tekstualnu poruku koja vas obaveštava da ste osvojili ajfon, i sve što je potrebno da bi vam on bio isporučen je samo da kliknete na link i popunite anketu. Realnost je da taj telefon ne postoji, a da anketa služi za krađu vaših ličnih podataka. Drugi primer bi bila tekstualna poruka u kojoj se navodi da paket nije mogao biti isporučen i koja sadrži link do veb sajta na kome se traži da popunite informacije potrebne za uspešan završetak isporuke, uključujući i podatke o vašoj platnoj kartici kako biste navodno pokrili troškove usluge. U nekim slučajevima, ovi sajtovi mogu od vas čak tražiti da instalirate mobilnu aplikaciju koja će zaraziti vaš uređaj i preuzeti kontrolu nad njim.

Sajber kriminalci ponekad kombinuju napade putem telefonskog poziva i tekstualnih poruka. Na primer, možete dobiti hitnu tekstualnu poruku u kojoj vas vaša banka navodno pita da li odobravate transakciju koja deluje sumnjivo. Poruka od vas traži da se izjasnite sa DA ili NE. Ako odgovorite, to će sajber kriminalcu dati do znanja da ste voljni da se angažujete i pozvaće vas telefonom pretvarajući se da zove iz odeljenja za prevare vaše banke. Zatim će tokom razgovora pokušati da od vas izmami informacije o vašim finansijama i platnim karticama, pa čak i o vašem nalogu i lozinci za pristup banci.

Prepoznajte i sprečite tekstualne napade

U nastavku je dato nekoliko pitanja koja bi trebalo da sebi postavite kako biste uočili najčešće znake koji ukazuju da se radi o napadu:

- Da li poruka kreira veliki osećaj hitnosti, požuruje vas ili primorava da preduzmete akciju?

- Da li vas poruka upućuje na veb sajtove na kojima se traže vaši podaci o ličnosti, platnoj kartici, lozinkama ili drugim osetljivim informacijama?
- Zvuči li poruka previše dobro da bi bila istinita? Ne, niste besplatno dobili novi ajfon.
- Da li vas veb sajt ili usluga na koju ukazuje link iz poruke primoravaju da izvršite plaćanje nestandardnim metodama kao što su bitkoin, poklon kartice ili Western Union prenos novca?
- Da li vam poruka traži da dostavite kod za multifaktorsku autentifikaciju koji je poslat na vaš telefon ili generisan u aplikaciji vaše banke?
- Da li poruka izgleda kao da je poslata pogrešnom broju? U tom slučaju ne odgovarajte na nju i ne pokušavajte da kontaktirate pošiljaoca, jednostavno je obrišite.

Ako dobijete poruku od zvanične organizacije koja vas na taj način na nešto upozorava, potvrdite to direktno sa tom organizacijom. Pritom nemojte koristiti broj telefona koji se nalazi u takvoj poruci, već umesto njega upotrebite zvaničan, pouzdan broj telefona te organizacije. Na primer, ako dobijete tekstualnu poruku od vaše banke u kojoj se navodi da postoji problem sa vašim bankovnim računom ili platnom karticom, obratite se direktno banci tako što ćete je pozvati na broj telefona naveden na njenom veb sajtu, na izvodu o transakciji, ili na poleđini vaše platne kartice. Zapamtite da vas većina državnih organa, uključujući poresku upravu i policiju, nikada neće kontaktirati korišćenjem tekstualnih poruka, već će to činiti jedino putem staromodnog pisma poslatog poštom.

Na kraju, znajte da ste sami sebi najbolja odbrana od napada putem tekstualnih poruka.

Gost urednik

Džef Lomas je detektiv u istražiteljskoj sajber grupi policije u Las Vegasu i predavač na obuci SANS SEC487 koja se bavi prikupljanjem i analizom otvorenih podataka (OSINT). Džef istražuje visokotehnološki finansijski kriminal, uključujući kompromitaciju poslovne elektronske pošte, smišing, ransomver, kao i složene slučajeve krađe kriptovaluta i pranja novca.

Dodatni materijal

Ne dajte se upecati: https://www.sans.org/newsletters/ouch/stop-that-phish/
Socijalni inženjering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Telefonski napadi i prevare (višing): https://www.sans.org/newsletters/ouch/vishing

Preveli za zajednicu: Dragan Ristić i Gordana Živanović