OUCH! Jul 2022

Čuvajte se, fišing napadi postaju sve napredniji

Fišing napadi su postali najčešći metod koji sajber napadači koriste da pronađu žrtve, bilo da ih traže u njihovom poslovnom ili privatnom okruženju. Tradicionalno, kod ove vrste napada koriste se elektronske poruke koje sajber kriminalci šalju svojim potencijalnim žrtvama sa ciljem da ih navedu na grešku, tj. da urade nešto što ne bi trebalo, na primer da otvore maliciozni prilog iz mejla, kliknu na maliciozni link ili odaju svoju lozinku. Iako se ovakvi tradicionalni fišing napadi događaju i danas, sajber kriminalci sve češće pokreću i napredne fišing napade u kojima se koriste prilagođene poruke koje je nešto teže otkriti. Pored mejla oni koriste i druge tehnologije kao što su tekstualne (SMS) poruke, društveni mediji, pa čak i telefonski pozivi, a sve sa ciljem da vas prevare. U nastavku su opisane najnovije prevare i kako ih možete uočiti.

Sajber napadači vredno istražuju

Tradicionalne fišing mejlove je lakše otkriti jer se najčešće kreiraju kao generičke poruke poslate milionima nasumičnih mejl adresa. Sajber napadači koji sprovde ovakve napade nisu mogli da znaju ko će postati njihova žrtva; jedino su bili svesni da što više mejlova pošalju, više ljudi će se upecati. Često se ovi jednostavniji fišing napadi prepoznaju kao mejlovi koji deluju čudno, počinju generičkim tekstom „Dear Customer“, sadrže gramatičke greške, zvuče previše dobro da bi bili istiniti (kao što je nigerijska prevara u kojoj vam se nude milioni dolara).

Današnji sajber napadi su daleko sofisticiraniji. Kako bi prilagodili napad, sajber napadači temeljno istražuju svoje potencijalne žrtve Umesto da pošalju mejl koji za cilj ima krađu identiteta na pet miliona adresa, ili da mejl kreiraju tako da izgleda kao generička poruka koju šalju korporacije, napadači sada poruke šalju na manji broj adresa (mnogo manjem broju ljudi) i prilagođavaju ih tako da potencijalnim žrtvama izgledaju kao da dolaze od nekoga koga žrtva poznaje. Pri kreiranju napada koriste se sledeće metode:

- istraživanje LinkedIn profila, informacija koje sami objavljujemo na društvenim mrežama, informacija koje su o nama dostupne javno ili su pronađene na dark vebu.
- kreiranje poruka tako da izgledaju kao da dolaze od rukovodstva, saradnika ili dobavljača koje poznajemo i sa kojima radimo.
- sagledavanje naših hobija i kreiranje poruka u kojima će se pretvarati da sa nama dele zajednička interesovanja.
- provera da li smo nedavno bili na nekoj konferenciji ili da li smo se upravo vratili sa putovanja, a zatim kreiranje poruke u kojoj se pozivaju na ta naša putovanja.

Sajber napadači pored mejla aktivno koriste i druge kanale komunikacije za slanje istih poruka, kao što su SMS poruke, pa čak i direktno pozivanje telefonom.

Kako da prepoznate napredne fišing napade

S obzirom da sajber napadači odvajaju značajno vreme da pažljivo istraže svoje potencijalne žrtve i osmisle napade, napredne fišing napade je teže uočiti. Srećom, dobra vest je da je to i dalje moguće, ali bitno je da znate šta treba da tražite. Pre nego što preduzmete akciju na koju vas sumnjiva poruka navodi, uvek sebi postavite sledeća pitanja:

1. Da li poruka kod vas izaziva pojačan osećaj hitnosti? Da li se od vas traži da zaobiđete bezbednosne politike vaše kompanije? Da li vas požuruju, kako biste nepromišljeno napravili grešku? Što je veći pritisak ili osećaj hitnosti, veća je verovatnoća da je u pitanju napad.
2. Ima li poruka uopšte smisla? Da li bi vam generalni direktor vaše kompanije poslao poruku u kojoj hitno traži pomoć? Da li je očekivano da će vaš pretpostavljeni tražiti da požurite i odmah kupite poklon kartice? Zašto bi banka tražila vaše lične podatke koje o vama sigurno ima? Ako se poruka deluje čudno ili neprikladno, moguće je da je reč o napadu.
3. Da li vam je poruka u vezi sa poslom stigla od bliskog kolege ili možda od pretpostavljenog, ali sa lične adrese elektronske pošte kao što je @gmail.com?
4. Da li ste mejl ili SMS poruku primili od nekoga koga poznajete, ali je formulacija, ton ili potpis u poruci pogrešan i neuobičajen?

Ako se poruka čini čudnom ili sumnjivom, možda je reč o napadu. Ako želite da potvrdite da li je mejl ili SMS poruka legitimna, jedna od opcija je da pozovete pošiljaoca (osobu ili organizaciju) koristeći pouzdan broj telefona..

Znajte da ste sami svoja najbolja odbrana. Ne sumnjajte u svoj zdrav razum.

Gost urednik

Fil Hofman je IT konsultant u penziji sa 40 godina iskustva, fokusiran na infrastrukturu i bezbednost. On je dugogodišnji saradnik i urednik OUCH! biltena, a hobiji su mu tehnologija, biciklizam i fotografija.

Dodatni materijal

Socijalni inženjering: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Tri najčešće prevare na društvenim mrežama: https://www.sans.org/newsletters/ouch/top-three-social-media-scams/
Napadi putem tekstualnih poruka - prepoznajte ih i sprečite: https://www.sans.org/newsletters/ouch/spot-and-stop-messaging-attacks/
Telefonski napadi i prevare (višing): https://www.sans.org/newsletters/ouch/vishing/
Potražite informacije o sebi na internetu: https://www.sans.org/newsletters/ouch/search-yourself-online/

Preveli za zajednicu: Dragan Ristić i Gordana Živanović