Socijalni inženjering

Uvod

- Postoje mnoge tehnike i propusti koje zlonamerni korisnici mogu iskoristiti za probijanje sigurnosti neke organizacije.

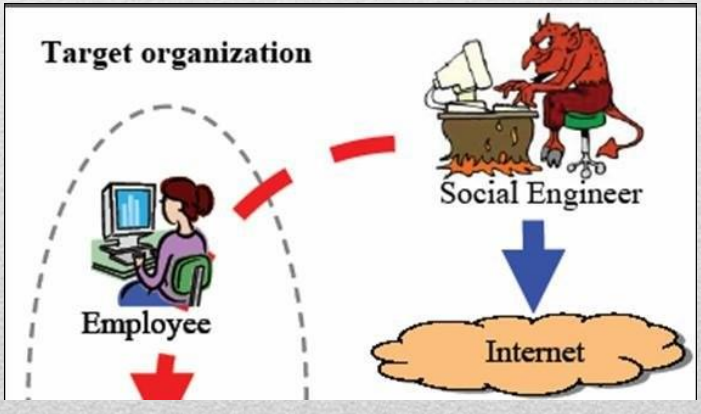
- Socijalni inženjering uključuje razne tehnike, od jednostavne krađe zapisanih lozinki do stvaranja i izvođenja složenih scenarija.

Osnove socijalnog inženjeringa

- Tehnike socijalnog inženjeringa mogu se klasfikovati u dve osnovne kategorije:
  - **Napadi usmereni na osobe**
  - **Napadi korišćenjem računarskih tehnologija**

Napadi socijalnog inženjeringa

- Napadi socijalnog inženjeringa odvijaju se kroz četiri faze :
  - *Prikuplanje informacija*
  - *Stupanje u kontakt sa žrtvom*
  - *Korišćenje veze sa žrtvom*
  - *Postizanje krajnjeg cilja*



Socijalni inženjeri

- Socijalni inženjer je bilo koja osoba koja koristi tehnike socijalnog inženjeringa, a neke od kategorija su:
  - *Hakeri*
  - *Osobe koje izvode "Penetration Test"*
  - *Špijuni*
  - *Osobe koje žele ukrasti identitet*
  - *Nezadovoljni radnici*
  - *Prodavci*
  - *Obični ljudi*

Prikupljanje informacija o žrtvama

- Socijalni inženjeri prikupljaju informacije o žrtvama tako da koriste sledeće ljudske osobine prilikom prikupljanja informacija:
  - *Poverenje*
  - *Želja osoba da nekom pomognu*
  - *Želju za određenom materijalnom koristi*
  - *Znatiželju*
  - *Strah od nepoznatog ili gubitka*
  - *Nemarnost*
  - *Ignorisanje pravila*

Prikupljanje informacija o žrtvama

- **Fizički pristup** - napadač se fokusira na fizička obeležja
- ***Psihološki pristup*** - napadač se fokusira na praćenje ponašanja korisnika

Cilj socijalnog inženjeringa

- Osnovni cilj socijalnog inženjeringa je povećati prava pristupa sistemu ili informacijama s mogućnošću:
  - *Izvođenje prevara*
  - *Upada u mrežu*
  - *Industijskog špijuniranja*
  - *Krađe identiteta*
  - *Jednostavnog narušavanja sistema ili mreže*

“PHISHING” NAPAD

- ‘**Phishing**’ je oblik sajber-kriminala zasnovan na metodama društvenog inženjeringa.

- Naziv ‘phishing’ je namerna greška u pisanju reči ‘fishing’ (pecanje), a podrazumeva krađu podataka sa računara korisnika i kasnije korišćenje tih podataka za krađu novca.

- Jedan od najčešćih načina krađe identiteta

Definisanje Phishing-a

- Phishing je pokušaj da se u elektronskoj komunikaciji prikupe osetljive informacije, kao što su korisnička imena, lozinke i detalji o kreditnoj kartici. Uobičajeno se obavljaju putem e-mail-a ili instant messaging-a,često upućuje korisnike da unose lične informacije na lažni veb sajt, čiji izgled je identičan legitimnom sajtu.
- Phishing je primer tehnike socijalnog inženjerstva koji se koriste za prevare korisnika. Lažne stranice često imaju izgled socijalne veb stranice, aukcijske stranice, banke, stranice za online plaćanje ili IT administratora.

IZVOĐENJE “PHISHING” NAPADA

- Za izvođenje ovih napada koriste se tehnike obmana.

- Osnovni postupci koji se koriste za preusmeravanje na lažirane web stranice spadaju u metode manipulacije hipervezama (hyperlink).

PHISHING PORUKA I PHISHING NAPAD

Phishing napadi se mogu pojaviti u obliku:

-Generičkih poruka koje je veoma lako uočiti

i

-Posebnih poruka koje se sastoje od prethodno prikupljenih podataka o žrtvi.

Posebne poruke su obično namenjene pojedincima na visokom pozicijama, kako bi se putem njihovih podataka ostvario pristup većoj količini poverljivih podataka.

(npr. napadač se predstavlja kao banka i navodi da je žrtva potrošila veliku količinu novca, da će kartica biti ukinuta ukoliko se ne javi, da će se naplatiti ogromna kamata na izmišljeni dug,…)

Tipovi phishinga-Spear phishing

- Phishing pokušaji koji su usmereni ka nekoj specifičnoj individui ili kompaniji se zovu spear fishing. Za razliku od phishing-a „na veliko“, spear phishing-napadači često sakupljaju i koriste lične informacije o svoj meti sa ciljem da povećavaju njihovu verovatnoću uspeha.
- Groupa-4127 (Fanci Bear) je koristila taktiku spear phishing-a kako bi ciljala naloge za e-poštu vezane za predsedničku kampanju Hillari Clinton 2016. godine. Napali su i dobili pristup više od 1.800 Google naloga.

- Klon phishing je vrsta phishing napada, pri čemu je legitimna i prethodno isporučena e-pošta koja sadrži vezu ili link imala njegovu adresu i adrese primalaca uzeta i iskorišćena za kreiranje gotovo iste ili klonirane e-pošte. Poslate stvari ili linkovi u okviru e-pošte zamenjeni su zlonamernim verzijama, a zatim su poslat sa lažne adrese e-pošte koja je napravljena da izgleda da dolazi od prvobitnog pošiljaoca. Može da tvrdi da je resend (ponovno slanje) od originalne adrese ili ažurirana verzija originala.

Klon phishing

Whaling

- Pojam „whaling“ se odnosi na spear-phishing napade koji su usmereni direktno na više rukovodioce i druge mete visokog profila. U ovim slučajevima, sadržaj će biti napravljen kako bi se ciljao neki viši menadžer i njegova uloga u kompaniji. Sadržaj e-pošte za napad može biti neko pitanje kojima se viši menadžment bavi, kao što je žalba nekog klijenta.

- Većina metoda phishing napada se koriste nekom vrstom tehničke prevare dizajnirane da naprave da link u e-mail-u vodi do lažnog web sajta.
- Loše napisani URL-ovi ili korišćenje poddomena su najčešći trikovi.

Link manipulacija

Filter evazija

- Phisheri ponekad koriste slike umesto teksta da bi ih anti-phishing filter teže detektovao.
- Zbog toga,sada postoje mnogo moderniji anti-phishing filteri koji mogu da otkriju sakrivene poruke unutar slika koristeci OCR (optical character recognition – prepoznavanje optičkih znakova).

Socijalno inženjerstvo

- Korisnici mogu biti podstaknuti da kliknu na različite vrste neočekivanih sadržaja iz različitih tehničkih i društvenih razloga. Na primer, zlonamerni prilog bi se mogao maskarirati kao najobičniji Google dokument.

- Alternativno, korisnici mogu biti uznemireni lažnim vestima, kliknuti na link i postati zaraženi.

- U telefonskom phishigu, phisher će putem telefona zvati korisnike i tražiti im da pozovu neki broj. Njegova svrha je da dobije od vas neke privatne informacije (vezane za npr. Račun u banci). Telefonski phishing se mahom obavlja sa lažnom identifikacijom pozivaoca.

Vishing(Voice Phishing)

- Još jedan napad koji se uspešno koristi je prosljeđivanje klijenta na legitimnu veb stranicu banke, a zatim postavljanje iskačućeg prozora na vrhu stranice koji traži neki vid akreditacije; na taj način mnogi korisnici banaka svojevoljno predaju svoje osetljive informacije.
- Zli blizanci (evil twins) su phishing tehnika koju je teško otkriti. Phiser stvara lažnu bežičnu mrežu koja izgleda slično legitimnoj javnoj mreži koja se može naći na javnim mestima kao što su aerodromi, hoteli ili kafići. Kad god se neko prijavi na lažnu mrežu, prevaranti pokušavaju da uhvate njihove lozinke i / ili podatke o kreditnoj kartici.

Druge tehike

- Tabnabbing iskorišćava pregledanje interneta sa više otvorenih kartica. Ovaj metod tiho preusmerava korisnika na mesto zaraženo nekim virusom. Ova tehnika radi obrnuto većini phishing tehnikama jer ne šalje direktno korisnika na lažni sajt, već umesto toga učita lažnu stranicu na jednom od otvorenih kartica pregledača.
- Smishing(SMS Phishing) je Phishing koji je obavljen putem SMS poruka. Putem SMS-a phiseri ce ljudima slati poruke koje sadrže link za neki lažni sajt, putem kojeg će oni pokušati da otkriju vaše lične informacije.

Kako izbeći phishing?

- Nikad ne odgovarajte na elektronske poruke koje traže lične podatke;
- Nikad ne sledite linkove koje se nalaze unutar sumnjivih i neočekivanih e-mail poruka;
- Uvek proverite da li adresa na koju unosite poverljive podatke odgovara legitimnoj;
- Proverite da li Web stranica preko koje unosite poverljive podatke koristi HTTPS protokol (Web adresa finansijskih institucija trebala bi počinjati sa https:// umesto sa http://);
- Budite u toku, pratite informacije o phishingu na internetu – sigurnosna edukacija je najefikasnija odbrana od pokušaja phishinga.

Kako se zaštititi od PHISHING-a?

Phishing je u stalnom porastu, a samim tim i rizici u E-banking-u. Iz tog razloga se razvijaju mnoge vrste zaštita protiv Phishinga koje se na tržištu pojavljuju kao samostalni programi, ili se ugrađuju u antivirusni softver ili u same aplikacije za E-banking.

Najsigurniji način je da korisnici budu oprezni i pre svake prijave na svoj nalog pogledaju URL adresu sajta. Hakeri obično hostuju svoje lažne stranice na besplatne hostove i koriste besplatne domene, najčešće se koriste .tk i .co.cc. Takođe korisnici treba da provere da li ispred URL adrese stoji HTTPS i ko je izdavač licence. A pre svega proveriti da li je domen originalni.
Većina Antivirusa ima web štit koji će sprečiti učitavanje stranica za koje se sumnja da su lažne ili sadrže malvere i viruse.

- Ljudi se mogu obučiti da prepoznaju pokušaje phishinga i da se bave njima kroz različite pristupe. Takvo obrazovanje može biti efektivno, posebno tamo gde obuka naglašava konceptualno znanje i daje direktne povratne informacije. Mnoge organizacije obavljaju redovne simulirane phishing napade i tako spremaju osoblje. Ljudi mogu preduzeti korake kako bi izbegli pokušaje phishing-a modifikovanjem njihovih navika pretraživanja. Kada vam se neko obrati oko računa koji treba da bude "verifikovan" (ili bilo koju drugu temu koju koriste phisher-i), razumna je mera predostrožnosti da kontaktirate kompaniju sa kojeg e-pošta očigledno potiče da proverite da li je e-pošta legitimna.

Kako izbeći i zaštiti se od phishinga

- Skoro sve legitimne e-mail poruke od kompanija za njihove klijente sadrže informacije koje nisu lako dostupne ostalima. Neke kompanije, na primer PayPal, uvek se obraćaju svojim korisnicima njihovim korisničkim imenom u e-poštu, tako da ako e-pošta adresira primaoca na generički način ("Dragi PayPal korisniče") verovatno će biti pokušaj phishing-a.

- E-pošta od banaka i kompanija za kreditne kartice često uključuje parcijalne brojeve računa. Međutim, nedavno istraživanje pokazalo je da javnost obično ne pravi razliku između prvih nekoliko cifara i poslednjih nekoliko cifara broja računa - značajan problem jer su prvih nekoliko cifara često ista za sve klijente finansijske institucije .

- „Anti-Phishing Working Group“ izrađuje redovni izveštaj o trendovima u napadima sa phishing-om.

- Najpoznatije organizacije koje se bore protiv phishinga su Anti-Phishing Working Group (APWG) i PhishTank.
  je komercijalna organizacija i izdaje besplatne
  mesečne izveštaje s detaljnim analizama, dok je PhishTank neprofitna organizacija pod pokroviteljstvom OpenDNS-a i sve njihove informacije su slobodne za upotrebu.

- Velike kompanije poput Googlea, Microsofta i Symanteca imaju vlastita rešenja za otkrivanje phishing napada. Najpoznatije primene su Googleov phishing filter u Mozilla Firefoxu i Chromeu, te Microsoftov phishing filter u Internet Exploreru. Opera koristi PhishTankov popis phishing stranica.

PHARMING

- Pharming je jedan od načina manipulacije korisnicima na Internetu, kojim hakeri izvođenjem

  DNS cache poisoning napadaju žrtvu, i bez njenog znanja i saglasnosti je preusmeravaju na lažnu web stranicu koja izgleda potpuno isto kao i originalna, tako da zrtva najčešće nije u stanju ni da posumnja da se nešto loše desava.

Kada žrtva otkuca svoje korisničko ime i lozinku, te informacije vise nisu privatne a napadač ostvaruje pristup zrtvinom računaru i njenim ličnim podacima.

Šta je PHARMING napad?

- Web sajtovi obično koriste imena domena za svoje adrese, dok je njihova stvarna lokacija određena IP adresom. Kad korisnik otkuca ime domena u svom Internet pretraživaču i pritisne Enter, ime domena se prevodi u neku IP adresu preko DNS servera.

- Internet pretraživač se tada povezuje na server sa tom IP adresom i preuzima podatke sa veb strane. Nakon što korisnik poseti željeni web sajt, DNS ulaz za taj sajt se često pamti u korisnikovom računaru u DNS kešu. Na taj način, računar ne mora da pristupi DNS serveru svaki put kad korisnik želi da poseti veb sajt.

Šta je PHARMING napad?

- Za sprovođenje nekih pharming napada koriste se posebni virusi upućeni Email-om koji prepisuju lokalne host fajlove na napadnutim kompjuterima. Host fajl pretvara URL adrese u numeričke nizove koji su razumljivi za računar, tako da ugroženi host fajl uzrokuje da korisnik bude usmeren ka pogrešnom sajtu, čak i ako korektno ukuca URL adresu legitimne Web lokacije.

- Mnogo opasniji su pharming napadi koji se realizuju preko kompromitovanja domain name sistema (DNS) jer se na taj način odjednom može obuhvatiti veliki broj žrtava. Ukoliko se DNS, koji pretvara Web i e-mail adrese u numeričke nizove, izmeni tako da sadrži lažne informacije o tome koja Web adresa odgovara kojem nizu brojeva, svi korisnici koji otkucaju odgovarajuću (ispravnu) Web adresu biće preusmereni na lažnu.

Šta je PHARMING napad?

- DNS poisoning mogu da izvedu samo vrsni eksperti, što mnoge odgovorne ljude iz antivirusnih kompanija navodi na zaključak da ta tehnika pharminga neće biti previše često korišćena. S druge strane, može se čuti mišljenje da je potencijalna materijalna korist koja se ukazuje više nego dovoljan mamac organizovanim grupama da se pozabave ovom granom hi-tech kriminala.

Kako se zaštititi od PHARMING-a

- Pharming bi mogao da bude stavljen pod kontrolu ukoliko bi Web čitači autentifikovali identitete pojedinih sajtova. Kada bi korisnik pomoću odgovarajućeg alata mogao da vidi da je sajt banke fizički lociran u Indiji, teško da bi se tek tako odlučio da bezbrižno ukuca svoje podatke u ponuđeni formular.

- Finansijske organizacije, koje su uvek među prvima na meti phishing i pharming napada, već razvijaju napredne tehnike autentifikacije I sifrovanja poruka korisnika, kao što su jednokratne lozinke kojima se proverava autentičnost korisnika nakog njegovog pokušaja prijave (log-ina) u sistem.