SOCIALNO INŽENIRSTVO - USPEŠEN NAPAD ZAGOTOVLJEN

Milan Gabor

Inštitut za varnost podatkov in informacijskih sistemov, ViRIS d. o. o.,
e-pošta: milan@viris.si
URL: http://www.viris.si

Povzetek: *Analiza uspešnih napadov na informacijske sisteme in uspešni napadi na različne baze podatkov kažejo, da je bila večina napadov uspešnih zaradi tipa napadov. Ti tipi napadov so bili v veliki večini primerov kombinacija tehnične pomanjkljivosti dela informacijskega sistema in uspešnega napada s socialnim inženirstvom. Vsak posameznik s svojimi objavami na medmrežju pušča lastno sled, ki se ji da z uporabo pametnih iskalnikov enostavno slediti. Tako lahko iz prstnih odtisov posameznika na medmrežju ugotovimo cel kup navad in tako na enostaven način zgradimo posameznikov profil. Ko imamo profil lahko s ciljanim napadom uspešno izvedemo socialni napad. Z nekaj poznavanjem psihologije in delovanje človekovega obnašanja lahko na enostaven način zavedemo žrtve napada, da nam zaupajo in s tem pridobimo dodatne informacije, ki so v veliko pomoč pri poznejšem nadaljevanju napada. Razmah socialnih omrežij je takšno zbiranje informacij še olajšal, saj je veliko informacij o potencialnih tarčah samo en klik miške stran.*

1. UVOD

Socialno inženirstvo oziroma »social engineering« je tip napada, ki ne cilja neposredno informacijske sisteme, ampak ciljajo napadalci predvsem ljudi, ki so povezani neposredno ali posredno s tarčami. Ti tipi napadov niso tehnike, ki bi bila nove ali posledica hitre rasti informacijskih tehnologij, saj imajo svoje korenine v sociološkem vedenju ali psiholoških značilnosti ljudi. Opredelili bi ga lahko kot netehnični način napada na podatke ali informacijske sisteme z izkoriščanjem človeških slabosti kot so na primer zaupljivost in naivnost [1].

Pri tem napadu je primarni cilj, da skušamo z zbiranjem informacij o žrtvi socialnega napada pridobiti čim več takšnih podatkov, ki nam bodo potem pri napadu zelo koristile. S takšnimi informacijami si bomo pridobili zaupanje žrtve in v takšni fazi zaupanja obstaja velika verjetnost, da nam žrtev izda določene informacije, ki potem lahko koristijo pri sami izvedbi napada na informacijska sredstva. Seveda je smiselno pridobiti čim več podatkov, saj so napadi potem še uspešnejši. Koristni so tudi podatki, ki jih je danes enostavno pridobiti iz različnih družbenih omrežij, saj lahko služijo kot osnova za začetek pogovora o kakšnih skupnih temah ali interesih.

Pri izvajanju takšne vrste napadov je pomembno imeti v mislih, da je veliko poudarka na psihologiji človeka in je zato seveda priporočljivo poznati delovanje človeške psihe. Poleg poznavanja psihologije človeka, igrajo pomembno vlogo tudi druge lastnosti kot na primer iznajdljivost, dobre komunikacijske sposobnosti in predvsem izjemna sposobnost opazovanja.

Pri sledenju različnih virov na to temo, je mogoče opaziti, da so pri izvajanju teh napadov zelo učinkovite predstavnice ženskega spola. Seveda je za to tudi kriva številčnejša populacija moških predstavnikov na IT področju in se poskusi socialnih inženirk pogosto končajo zelo uspešno, saj so moški predstavniki vedno pripravljeni pomagati nemočnim ali nevednim ženskam. Dodatne točke pri tem seveda prinese tudi dober in privlačen izgled.

Slika 1: Humorni razlog zaradi katerega deluje socialno inženirstvo

Pomemben je tudi življenjski krog napada s socialnim inženirstvom [1], ki ga je na kratko mogoče opisati v nekaj točkah:

- zbiranje informacij,
- vzpostavitev odnosa,
- izkoriščanje odnosa,
- izvedba zastavljenega cilja.

Nekatere klasične tehnike socialnega inženirstva, ki jih je mogoče uporabiti so na primer [1]:

- s pomočjo telefona,
- vohunjenje čez ramo,
- brskanje po smetnjaku,
- ribarjenje na različne načine.

Poznamo kar nekaj uspešnih ljudi, ki so bili z izkoriščanjem takšnih tipov napadov zelo uspešni. Eden izmed njih je vsekakor Kevin Mitnick, ki so ga organi pregona tudi na koncu ujeli. Sam je v svojih knjigah opisal svoje izkušnje in kako je koristno uporabljal različne tehnike napadov. Seveda pa zunaj obstaja najbrž kopica ljudi s podobnimi sposobnostmi, vendar tega ne obešajo na veliki zvon. Vprašanje, ki se poraja je tudi to, da če smo bili tarča takšnega napada, ali bomo kdaj sploh zvedeli zanj.

2. VIRI PODATKOV ZA USPEŠEN NAPAD

Vir podatkov, kjer lahko danes najdemo različne podatke, je vsekakor svetovni splet. Iz lastnih izkušenj pa za uspešno zbiranje podatkov v večini primerov zadostuje že samo telefonska številka. Če je ta telefonska številka objavljena v imeniku, lahko pridobimo ime in priimek naročnika in njegov naslov. Potencialno lahko pridobimo podatke še o drugih telefonskih številkah. Ime in priimek vpišemo v Google in pridobimo še zadetke v katerih se te kombinacije imena in priimka nahajajo. Tako lahko počasi zgradimo sliko o osebi, njegovih navadah, hobijih in kar je najpomembnejše tudi o njegovih kontaktih ali z njim povezanimi osebami. Velikokrat je bolj priročno posredni napad preko katerega znanca kot pa direktni napad na tarčo. Seveda je pri tem pomembno vedeti, da se s tem poveča tudi potreba po zbiranju informacij in seveda sočasno tudi trajanje takšnega napada, saj je najprej treba uspešno pridobiti podatke od tega prejšnjega člena v verigi.

Zelo priročna mesta za zbiranje podatkov:

- Google,
- Facebook,
- telefonski imeniki,
- različni forumi,

- druga socialna omrežja.

Poleg tehničnega poznavanja, so zelo pomembne psihološke sposobnosti, ki recimo bolj tehničnim ljudem manjkajo. Tako je dobro poznati psihologijo človeka, da se lahko predvidijo nekatere njihove reakcije in se lahko glede na te reakcije že pripravijo tudi ustrezne akcije in dejanja. Sposobnosti, ki jih morajo uspešni napadalci imajo lahko povzamemo v naslednjih točkah:

- zelo dobra sposobnost opazovanja,
- dobre komunikacijske sposobnosti,
- sposobnost hitrega prilagajanja in hipnih reakcij,
- široko poznavanje različnih področij oziroma dobra razgledanost,
- spodobnost igranja različnih vlog.

3. ORODJA

Kljub temu, da se pri socialnih napadih uporablja manj orodij kot na primer testiranju programske opreme z zato namenjenimi orodji, so vsaj nekatera orodja dobrodošla. Tako lahko takšna orodja poenostavijo samo simulacijo napada z uporabo socialnega inženirstva in naredijo takšne simulacije precej enostavne. Večina orodij ima pripravljene predvsem module za lažjo pripravo lažnih spletnih strani. Drugi pomemben modul je modul za napade z uporabo elektronske pošte. Za večino napadov ta dva modula zadostujeta in z njuno uporabo lahko brez težav simuliramo napade na ljudi.

Tako je vredno pri orodjih omeniti predvsem:

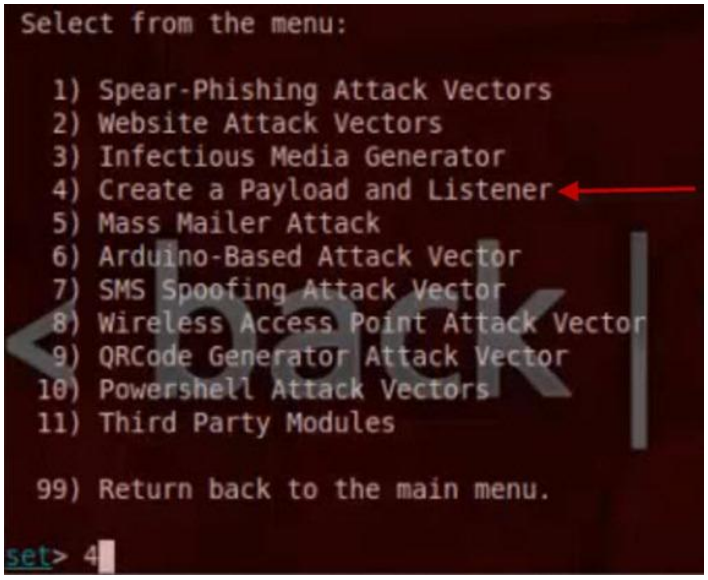
- SET [3],
- Metasploit Pro [4].

Orodje SET je prostodostopen, medtem ko je Metasploit Pro plačljivo komercialno orodje. Metasploit Pro ima sicer tudi prostodostopno različico, vendar pri tej različici napad s socialnim inženirstvom ni omogočen. Tako lahko z uporabo orodja SET generiramo različne tipe napadov in to orodje je v skupnosti eno izmed najbolj priljubljenih, saj omogoča široko paleto napadov in se hkrati razvija s precejšnjo hitrostjo. Nenehno se dodajajo tudi novi moduli, ki omogočajo nove funkcionalnosti in hkrati tudi nove vrste napadov.

Omeniti velja, da je to orodje del večine distribucij, ki se uporabljajo za testiranje varnosti. Seveda pa samo orodje ni dovolj. Orodje je le platforma, ki omogoča simulacijo napadov, kako uspešno se bo to orodje izkoristilo je v veliki meri odvisno od samega uporabnika in njegovih sposobnosti na področju socialnega inženirstva.

Z orodjem SET je mogoče izvajati naslednje napade:

- preko lažnih elektronskih spletnih strani,
- z lažnimi elektronskimi sporočili,
- z generatorji datotek za USB ključe,
- napadi na brezžične tehnologije.



Slika 2: Špartanski vmesnik orodja SET

4. KJER JE LAHKO 1+1=3||4

To v naslovu poglavja imenujemo hekerska matematika. Ta hekerska matematika je malce drugačna od navadne matematike, saj v njej ne veljajo navadne zakonitost nam dobro poznane matematike. Če poskušamo razložiti zakonitost hekerske matematike, lahko ugotovimo, da 1 pomeni manjšo pomanjkljivost ali ranljivost, ki je lahko tehnične narave. Podobno velja za drugo enico. Ti dve manjši ranljivosti, ki ni nujno, da sta sploh povezani, lahko v rokah sposobnih hekerjev dajo na koncu večjo vrednost kot je vrednost v tradicionalni matematiki.

Naj ponazorimo to matematiko s konkretnim primerom. Recimo, da ima spletna stran podjetja X manjšo ranljivost, ki se jo da izkoristiti. Ta spletna stran se nahaja na spletnih strežnikih, ki ponujajo gostovanje spletnih strani in ni znotraj korporativnih strežnikov podjetja X. Poleg te ranljivosti obstaja recimo ranljivost v konfiguraciji elektronske pošte podjetja X. V tem primeru je vseeno kje se poštni strežniki nahajajo in ni potrebe, da bi se morali nahajati v korporativnem omrežju podjetja X.

Iznajdljivi napadalci lahko s kombinacijo teh dveh pomanjkljivosti, ki ni nujno, da sta označeni z visoko stopnjo kritičnosti, izvršijo zelo učinkovit napad. Z uporabo elektronske pošte, lahko pripravijo zelo avtentično elektronsko sporočilo, ga pošljejo v imenu nadrejene osebe svojim podrejenim. V sporočilu je opis nove storitve na lastnih spletnih straneh in povezava kaže na njihovo stran. S strani prejemnikov elektronske pošte v tem primeru ni nič čudnega, saj se pošiljatelj ujema, ujema se tudi njegov stil elektronske pošte in tudi povezava v elektronskem sporočilu kaže na spletno stran podjetja X.

Vsebina elektronskega sporočila se lahko enostavno glasi: »Dodali smo novo funkcionalnost na naših spletnih straneh. Prosim, preizkusite to funkcionalnost. Naša spletna stran bo mogoče od vas zahtevala vpis uporabniškega imena in gesla. Prosimo vas, da to pravilno vpišete«.

Rezultat takšnega napada je 100 uspešnost.

5. SLOVENSKI NAPADI

Slovenija kljub svoji majhnosti in čudnemu jeziku, ki ga govorimo, ni imuna tudi na takšne vrste napadov. Velika večina takšnih napadov ostane vsaj v medijih neopažena, saj pri nas ni zakonske podlage, ki bi nalagala upravljavcem dolžnost, da morajo v primeru odtujitve podatkov, obvestiti prizadete stranke in javno objaviti, da so bili podatki odtujeni.

Ciljanih socialnih napadov najbrž v Sloveniji ni veliko, vendar ko se zgodi, lahko ugotovimo, da so lahko vrednosti v EUR precej visoke. Tako je bilo letos v mesecu marcu izvedenih v primeru, ki ga bomo navedli, 12 hišnih preiskav in odvzeta prostost 5 osebam. Višina denarja, ki ga je kriminalna združba uspela ukrast z

računov podjetij je znašala skoraj 2 milijona EUR. Okrog 900 tisočakov je kriminalni združbi preko 25 mul uspelo pridobiti, ostalo so inštitucije, ki so preiskovale ta primer, uspele zadržati.

Ta napad je trajal kar nekaj časa, saj korenine segajo v avgust 2012, ko je Banka Slovenije objavila posebno opozorilo glede previdnosti pri poslovanju preko elektronskega bančništva. Tarče so bile večinoma finančno računovodsko osebe, saj imajo v večini primerom tudi dostop do elektronskega bančništva in možnost izvrševanja transakcij.

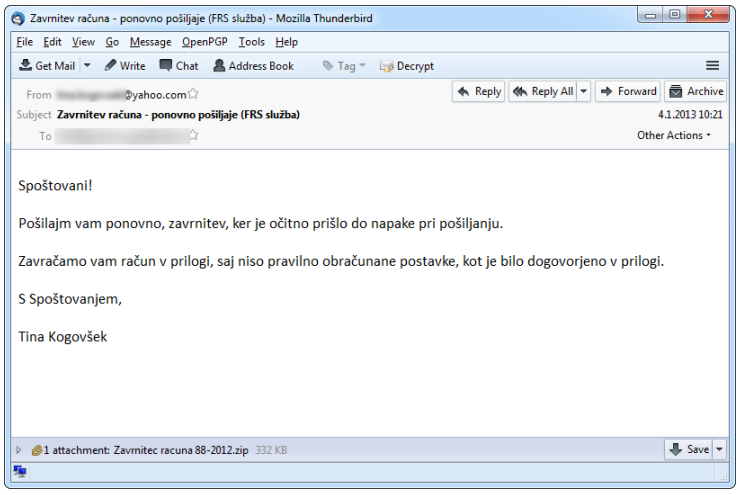
Sam napad pa ni bil preveč sofisticiran, saj je bila osnova elektronsko sporočilo, ki je vsebovalo priponko. Z zagonom datoteke iz priponke, je uporabnik na svoj računalnik namestil t.i. RAT program (Remote Administration Toolkit), ki je napadalcu omogočil oddaljeni dostop do žrtvinega računalnika in prevzem popolne kontrole nad računalnikom. Tako je imel napadalec dostop do sistema, lahko prestrezal vnos preko tipkovnice. Napadi so tipično potekali ob petkih ali pred kakšnimi prazniki.

Pri tem napadu pa je mogoče iz medijev povzeti in izluščiti dva tipična problema. Prvi, najpomembnejši je seveda bil ta, da so pametne kartice s certifikati ostale po uporabi v čitalcih. Napadalci so prej s prestrezanjem vnosov preko tipkovnice uspeli prestreči PIN pametne kartice in potem brez težav izvrševali ali pripravili ustrezne transakcije za prenos denarja na račune mul. Drugi problem pa je bil, da se teh delovnih postaj ni zaklepalo ali ugašalo po odhodu z delovnega mesta. Tako so lahko napadalci po končanem delovniku brez težav oddaljeno upravljali z računalniki in tako uspeli uspešno pokrast veliko količino denarja.

Glede na to, da je bilo mogoče pridobiti nekatere primere ponarejene elektronske pošte s katero so uspešno izvršili te napade, je zanimivo analizirati na kako enostaven način je mogoče priti do nadzora nad celotnim računalnikom. V nadaljevanju sta prikazana dva primera elektronskih sporočil s katerimi so napadalci poskušali prepričati žrtve, da so odprle pripete datoteke.

Tako lahko na hitro opazimo nekaj pomanjkljivosti ob katerih bi osveščeni uporabniki zastrigli z ušesi:

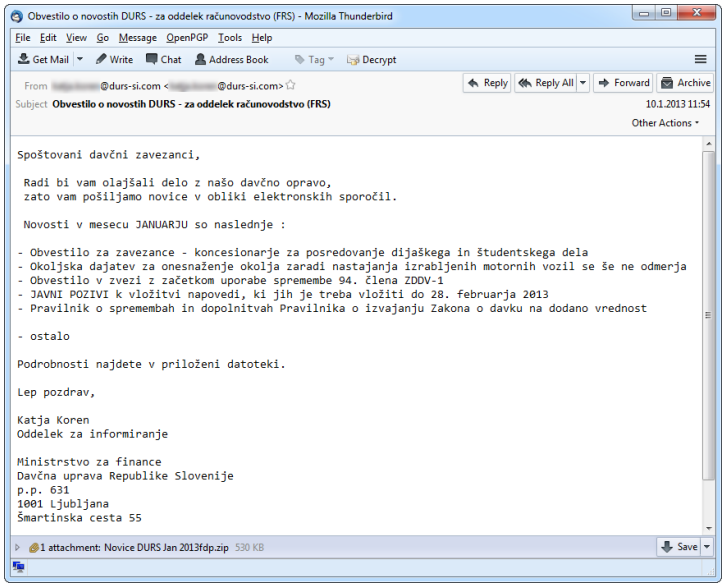
- elektronska pošta je prišla z naslova @yahoo.com,
- vsebuje kar nekaj slovničnih napak,
- priponka vsebuje netipično datoteko.



Slika 3: Prikaz enostavnega napadalnega elektronskega sporočila [5]

Drugi primer elektronske pošte je že bolj sofisticiran in kaže na evolucijo pri napadalcih, saj najbrž v prejšnjih primerih uspeh ni bil tolikšen kot so pričakovali. Tako lahko na tem primeru ugotovimo naslednje:

- registrirana domena durs-si.com, kar spominja na pravo domeno durs.si in tudi v imeni DURS-a,
- precej formalna oblika elektronske pošte,
- precej dober in verodostojen podpis.



Slika 4: Prikaz bolj izdelanega napadalnega elektronskega sporočila [5]

Na teh dveh primerih lahko vidimo, kako se tudi napadalci prilagajo pri napadih z uporabo socialnega inženirstva. Iz osnovne elektronske pošte so uspeli razvit skoraj avtentično elektronsko pošto. Še posebej je zanimivo, da velika večina žrtev pade na tem, da če dobijo dobro elektronsko pošto s strani DURS-a, jo je potrebno odpreti in preveriti.

Na tem primeru je tudi lepo vidna evolucija napadalcev.

6. ZAKLJUČEK

Zavedati se je potrebno, da 100 % varnosti ni. Varen sistem ali računalnik je tisti, ki je odklopljen iz omrežja in spravljen nekje v sefu. Je pa seveda takšen sistem ali računalnik tudi skoraj popolno neuporaben.

Mnenja sem, da je trenutno najboljša kombinacija poleg digitalnih potrdil na pametnih karticah seveda, dvonivojska avtentikacija. To dvonivojsko avtentikacijo omogoča zdaj že večina najbolj popularnih storitev, kot so na primer Gmail, Twitter in Facebook. Z enostavno konfiguracijo varnostnih nastavitev si lahko to možnost omogočimo. V tem primeru tudi če napadalec ugotovi geslo, še vedno potrebuje dostop do mobilne naprave, kjer prispe drugi del podatkov.

Poleg vsega pa se lahko zoperstavimo socialnemu inženirstvu edino z varnostnim ozaveščanjem in učenju na konkretnih primerih. Simuliranje napadov z uporabo takšnih tehnik tudi ni slaba ideja, čeprav se jih večina naročnikov varnostnega testiranja otepa. S simulacijo se lahko uporabnikom na konkretnem primeru pokaže, kaj se lahko naredi s takšnimi tipi napadov. Zato lahko tudi z veliko verjetnostjo rečemo, da ko napad na tehnologijo ne uspe, napad na ljudi skoraj vedno uspe. Z večjo ozaveščenostjo, pa se ta verjetnost bistveno zmanjša.

7. LITERATURA

[1] MARKO HÖLB “”,Monitor 2009, http://www.monitor.si/clanek/socialno-inzenirstvo/123589/.

[2] https://www.trustedsec.com/downloads/social-engineer-toolkit/

[3] http://www.metasploit.com/

[4] Novica CERT, http://www.cert.si/obvestila/obvestilo/article/slovenian-police-cracks-down-on-a-gang-netting-almost-2-million-EUR-from-companies-via-e-banking-hac.html.

[5] SI-CERT