"Mladi za napredek Maribora 2016"

33. srečanje

Socialni inženiring na spletu in kako se mu izogniti

RAČUNALNIŠTVO

Raziskovalna naloga

Avtor: ANŽE MAVRIČ, MIHA FRANGEŽ

Mentor: BRANKO POTISK

Šola: SREDNJA ELEKTRO-RAČUNALNIŠKA ŠOLA MARIBOR

PROSTOR ZA NALEPKO

Maribor, 2016

Kazalo vsebine

Kazalo vsebine 2
Kazalo slik 3
Kazalo kode 3
1 UVOD 4
2 SOCIALNI INŽENIRING 4
3 VRSTE SOCIALNEGA INŽENIRINGA 5
3.1 Phishing 5
3.1.1 Zlonamerne dostopne točke 5
3.2 Pretexting 6
3.3 Baiting 6
4 PHISHING V PRAKSI 7
4.1 Priprava 7
4.1.1 Spletna stran 7
4.1.2 E-poštno sporočilo 9
4.2 Rezultati 10
4.3 Zaščita 11
4.3.1 Za uporabnike 11
4.3.2 Za administratorje 12
5 ZLONAMERNA DOSTOPNA TOČKA V PRAKSI 13
5.1 Priprava 13
5.2 Rezultati 14
5.3 Zaščita 15
5.3.1 Za uporabnike 15
5.3.1 Za administratorje 15
DRUŽBENA ODGOVORNOST 16
ZAKLJUČEK 16
Viri in literatura 17

Kazalo slik

Slika 1: Shranjevanje strani 7
Slika 2: URLji v CSS datotekah se ne shranjujejo pravilno 7
Slika 3: Struktura Facebookove prijavne strani 8
Slika 4: Opozorilo, ki se prikaže po prijavi 9
Slika 5: E-poštno sporočilo, ki sva ga poslala tarčam 9
Slika 6: Povezave lahko vodijo kamorkoli 11
Slika 7: Cilj povezave lahko hitro preverimo 11
Slika 8: EV SSL certifikat na strani NKBM 12
Slika 9: Spletna stran NKBM preko zaščitene povezave 15
Slika 10: Spletna stran NKBM, če bi bili na njo povezani po nezaščiteni povezavi 15

Kazalo kode

Koda 1: JavaScript koda za prikaz opozorila 8
Koda 2: Z RegEx zamenjavo hitro zamenjamo vse Facebookove povezave z našimi 10
Koda 3: `/etc/NetworkManager/NetworkManager.conf` 13
Koda 4: Hostapd konfiguracija (`./hostapd.conf`) 13
Koda 5: Dnsmasq konfiguracija (`./dnsmasq.conf`) 13
Koda 6: DNS naslovi (`./hosts.conf`) – preusmeritev Facebooka na lokalni strežnik 14
Koda 7: Postavitev NAT storitve 14
Koda 8: Zagon dostopne točke 14

1 UVOD

Namen te raziskovalne naloge je raziskati vrste in metode socialnega inženiringa. V začetku bova raziskala teorijo za posameznimi vrstami socialnega inženiringa. Ugotovila bova zakaj so posamezne metode tako učinkovite in razložila, kako jih prepoznati ter se jim izogniti.

Nekaj izmed teh bova tudi preizkusila v praksi, ter analizirala dobljene rezultate. Za te napade bova podrobno razložila postopek izdelave ter izpostavila vse pomanjkljivosti najinih izvedb. Na koncu bova tudi demonstrirala, kako deluje zaščita proti tovrstnim napadom.

2 SOCIALNI INŽENIRING

Socialni inženiring je način prevare, ki z izkoriščanjem človekovih lastnosti in navad, prepriča človeka, da stori nekaj, česar drugače ne bi. Na različne načine se uporablja na skoraj vseh področjih življenja, najbolj prepoznan pa je v svetu računalnikov ter svetovnega spleta.

V računalništvu se v glavnem uporablja za krajo dostopnih podatkov (npr. PIN kod, uporabniških imen, gesel ipd.). Za razliko od tradicionalnih načinov vdora v računalniške sisteme, se socialni inženiring ne zanaša na napake v programski opremi, ampak na psihološke ranljivosti v ljudeh, ki jo uporabljajo. To je glavni razlog, zaradi katerega je socialni inženiring pogosto bolj nevaren, kot varnostne napake v programih – človeške narave ni tako enostavno popraviti.

Na grobo lahko socialni inženiring delimo v dve kategoriji:

- **Preko računalnika** *(computer-based)*: prevarant uporabi računalniške tehnike, kot so kloniranje spletnih strani, elektronska pošta, WiFi dostopne točke ipd., da pridobi tarčine zasebne podatke. Zahtevajo srednje dobro poznavanje delovanja računalniških sistemov – vseeno dosti manj, kot za tradicionalne hekerske napade.
- **Z osebnim stikom** *(human-based)*: prevarant poskuša pridobiti zaupanje tarče, ter tako fizično pridobiti dostop do zaupnih podatkov (npr. iz tarčinega stanovanja, pisarne…). Te napade po navadi izvajajo ljudje, ki zelo dobro poznajo psihologijo in so odlični igralci. Takšni napadi so sicer vedno manj pogosti, so pa zato lahko zelo nevarni.

Obstaja veliko vrst socialnega inženiringa, v tej nalogi pa bova opisala ter preizkusile tiste, ki se najpogosteje uporabljajo za krajo podatkov na spletu.

3 VRSTE SOCIALNEGA INŽENIRINGA

3.1 Phishing

Phishing ali spletno ribarjenje je najpogostejša oblika socialnega inženiringa na spletu. Ime dobi po načinu s katerim dobiva tarče, saj napadalec povezave do zlonamerne spletne strani po navadi pošlje veliko ljudem in čaka, kateri se bodo »ujeli na trnek«.

Phishing napadi se po navadi začnejo e-poštnim sporočilom. Tega napadalec izdela tako, da izgleda podobno kot takšno, ki bi ga dobili od storitve, katere račun poskuša napadalec ukrasti (npr. Facebook ali spletna banka). Ti po navadi od uporabnika zahtevajo, da s klikom na povezavo potrdi svojo identiteto, posodobi varnostne nastavitve ali pa zamenja gesla. Ko tarča klikne na povezavo, pa ga namesto na pravo storitev, preusmerijo na napadalčevo kopijo strani, ki izgleda in deluje kot prava. Napadalec pa ima tako dostop do vseh podatkov, ki jih tarča v stran vpiše.

Zelo pogosto se pri tovrstnih napadih uporabljajo domene, ki so na prvi pogled zelo podobne domeni prave storitve (npr. face**ooo**k.com namesto face**oo**k.com ali pa facebook**.co** namesto facebook**.com**), z uvedbo mednarodnih domen (IDN), pa je zelo pogosta tudi uporaba tujih znakov, ki izgledajo enako kot znaki naše abecede, čeprav računalnik to vidi kot popolnoma drugo domeno (npr. f**ace**b**oo**k.com namesto f**ace**b**oo**k.com – čeprav naslov izgleda identično, so črke **a**, **c**, **e** in **o** v resnici znaki iz cirilice ter posledično zaznani kot čisto druga domena).

Da povečajo kredibilnost lažne strani pa napadalci pogosto uporabljajo tudi druge metode prikrivanja kot na primer posredniški ali *Man In The Middle* napadi, ponarejeni certifikati, ki jih namestijo na tarčin računalnik, v primerih vdorov v bančne račune in podobne storitve, pa pogosto svojo zgodbo podkrepijo s telefonskim klicom ali pismom.

3.1.1 Zlonamerne dostopne točke

Še posebej nevarna vrsta phishinga je t.i. *Evil Hotspot* napad. Pri tem napadu napadalec postavi javno Wi-Fi dostopno točko, na katero se povežejo tarče. Napad se najpogosteje izvaja na letališčih, avtobusnih postajah, v kavarnah in vseh javnih prostorih, na katerih ljudje pogosto iščejo odprta Wi-Fi omrežja.

Ko se tarča poveže na omrežje, ima napadalec popoln nadzor nad njenim brskanjem po internetu. Nešifrirane povezave lahko napadalec bere in spreminja, nešifrirane povezave pa lahko blokira in s tem tarčo prisili, da uporabi nešifrirano (tarča po navadi tega sploh ne opazi, saj na nešifrirano povezavo samodejno preklopi večina spletnih brskalnikov).

Zelo pogosta je tudi naprednejša oblika tega napada, pri kateri napadalec postavi dostopno točko z enakimi nastavitvami, kot obstoječa javna dostopna točka. Nato se poveže na pravo dostopno točko, ter z ponarejenim odjavnim paketom tarčam prekine povezavo z omrežjem. Napadalec nato poveča moč (ang. *gain*) svoje dostopne točke in ko se tarčin računalnik poskusi ponovno povezati, se nevede poveže na napadalčev računalnik.

Tak napad je še nevarnejši, saj tarča misli, da je še vedno povezana na dostopno točki, ki ji zaupa, zato je še manj previdna, kot če bi bila povezana na neko neznano.

3.2 Pretexting

Pretexting je oblika socialnega inženiringa, pri kateri se tarči napadalec lažno predstavi z namenom, da bi mu razkrila privatne informacije. Pri dobrih pretexting napadih, napadalec ustvari celotno novo identiteto. Tovrstni napadi zahtevajo ogromno priprave, saj mora biti lažna identiteta dovolj prepričljiva, da napadalcu tarča zaupa.

Pogoste lažne identitete so npr. bančni uslužbenci, inšpektorji, čistilci ter osebje za tehnično podporo.
Slednji so najpogostejši v primerih vdorov v računalniške sisteme. Če napadalec izve, da je neko podjetje pred kratkim imelo tehnične težave, se lahko predstavi kot uslužbenec ponudnika spletnih storitev, ter tako pridobi dostop do računalniških sistemov podjetja. Svojo identiteto lahko dodatno podkrepi s tem, da podjetje pred prihodom pokliče, ter se jim opraviči za tehnične težave, in jih obvesti, da bo v kratkem prispel serviser, ki bo težavo odpravil.

Zelo uporabna lažna identiteta je tudi čistilka, saj jih večina uslužbencev v večjih podjetjih sploh ne pozna, zato sploh ne bodo opazili, ko se bo napadalec lahko prosto premikal po prostorih polnih zasebnih podatkov.

V primeru napada na posameznika, pa so zelo pogosti lažni telefonski klici bančnih uslužbencev, ki zaradi »varnostnih razlogov« želijo preveriti številko bančnega računa.

3.3 Baiting

Baiting se zanaša na radovednost in nepazljivost ljudi. Je oblika, pri kateri napadalec pusti podatkovni medij (npr. USB ključ ali CD/DVD) na mestu, kjer ve, da ga bo nekdo našel. Večina ljudi najden medij priklopi v računalnik iz radovednosti ali pa za to, da bi ugotovili čigav je. To je zelo nevarno, saj je napadalec lahko medij okužil z virusom, ali pa je uporabil hujši napad na nivoju strojne opreme, kot na primer BadUSB.

Učinkovitost te oblike napada lahko vidite v primeru napada na obrambno ministerstvo ZDA leta 2008. Napadalci so na parkirišču pred stavbo pustili USB ključ, okužen z virusom. Tamkajšnji uslužbenec ga je pobral, ter ga vstavil v prenosnik, ki je bil povezan v centralnim strežnikom. Na strežnik se je iz USB ključa prenesel virus, ki ga je Pentagon odstranjeval kar 14 mesecev. Strokovnjaki so ta napad poimenovali »najhujši vdor Ameriških vojaških sistemov v zgodovini«.

Za praktični preizkus napada sicer nisva imela dovolj časa in definitivno ne dovolj USB ključev, o njegovi učinkovitosti pa pričajo številne raziskave podjetij, ki se ukvarjajo s preizkušanjem varnosti računalniških sistemov.

Eno izmed takih raziskav je leta 2011 opravila tudi Ameriška vlada, ki je ugotovila, da je USB ključe in CDje, najdene na parkiriščih v računalnik vstavilo kar 60 odstotkov ljudi, takšne z uradnimi logotipi pa kar 90 odstotkov ljudi.

Glavno nevarnost tovrstnih napadov najbolje povzame izjava Marka Rascha, direktorja omrežne varnosti pri Ameriškem računalniškem podjetju Computer Sciences Corp.:

»There's no device known to mankind that will prevent people from being idiots« (Human Errors Fuel Hacking as Test Show Nothing Stops Idiocy, 2011)

4 PHISHING V PRAKSI

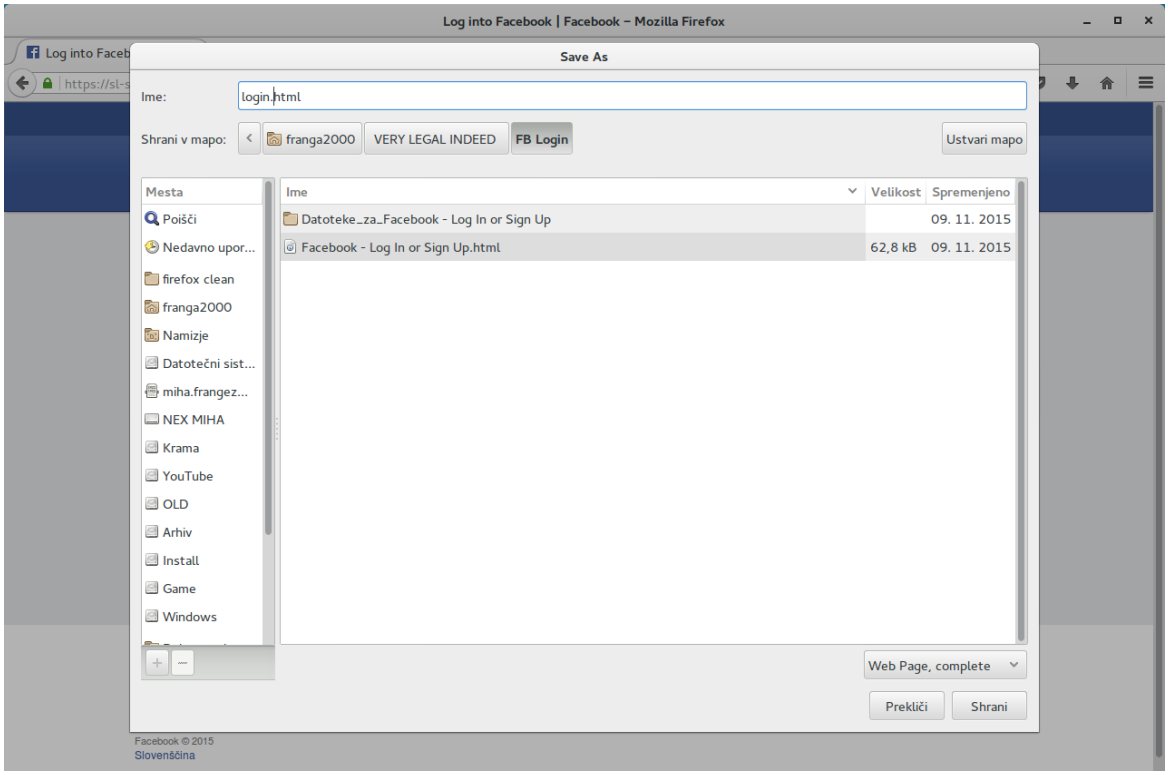
Za preizkus phishing napada v praksi, sva pripravila svojo phishing stran, ter jo poslala tarčam. Uporabila sva prijavno stran družabnega omrežja Facebook, tarčam pa sva jo podtaknila z ponarejenim E-poštnim sporočilom.

4.1 Priprava

Za napad potrebujemo spletni brskalnik s funkcijo shranjevanja strani, dober urejevalnik besedila (npr. Gedit ali Notepad++), spletni strežnik in e-poštni račun.

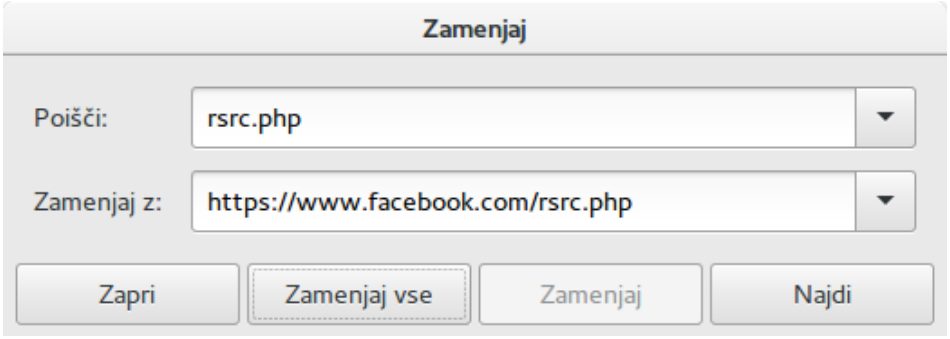
4.1.1 Spletna stran

Najprej sva morala Facebookovo prijavno stran kopirati. S Firefoxom sva odprla stran https://si-sl.facebook.com/login in s klikom **CTRL+S** shranila celotno stran.



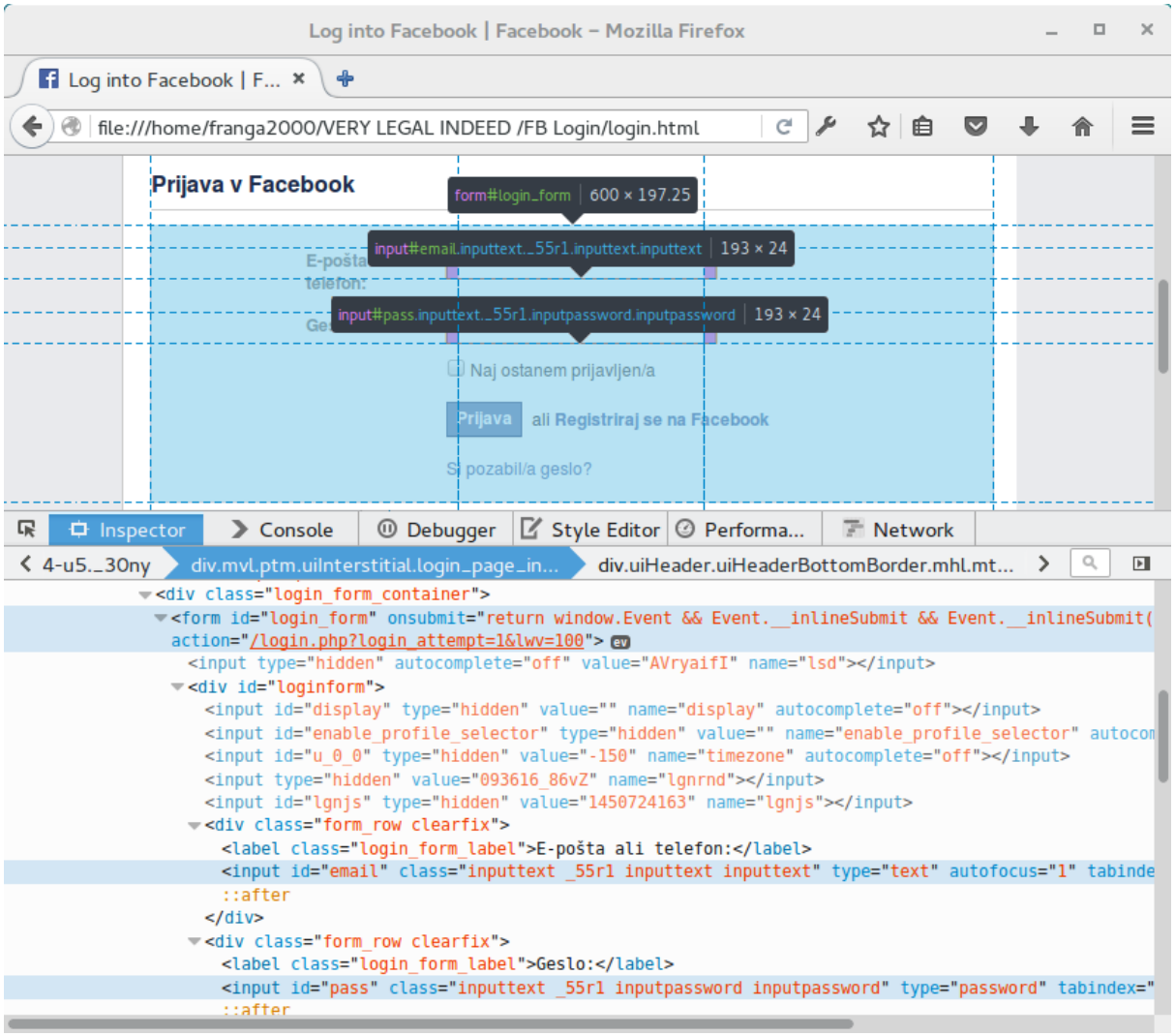
Slika 1: Shranjevanje strani

Zaradi napake v sistemu shranjevanja, se URL do Facebookovega logotipa v CSS datotekah ni shranil pravilno, kar sva hitro popravila z ukazom »Poišči in zamenjaj«:



Slika 2: URLji v CSS datotekah se ne shranjujejo pravilno

Nato sva s pomočjo Firefoxovih orodij za razvijalce pregledala izvorno kodo strani.



Slika 3: Struktura Facebookove prijavne strani

Tako sva ugotovila, da ima gumb za prijavo id oznako `u_0_2`, polja za e-poštni naslov in geslo pa `email` in `pass`. S temi podatki sva lahko napisala JavaScript kodo, ki ob prijavi uporabniku pokaže opozorilo z njegovim geslom.

```
$("u_0_2").onclick = function() {
    alert("Zdravo!\n\
Vaš email je: " + $("email").value + "\n\
Vaše geslo je: " + $("pass").value + "\n\
Lahko bi ga ukradel, ampak ga nisem.\n\
Tokrat...");
};
```

Koda 1: JavaScript koda za prikaz opozorila[1]

[1] Znak `$` v tem primeru ni jQuery, ampak bližnjica do `document.getElementById`

Slika 4: Opozorilo, ki se prikaže po prijavi

Čeprav v najinem primeru gesla uporabnikov nikoli niso zapustila njihovega računalnika, bi lahko v le nekaj vrsticah PHP in JS kode gesla shranila v datoteko na strežniku, tarčo pa preusmerila na pravo prijavno stran z sporočilom, da geslo ni bilo pravilno.

4.1.2 E-poštno sporočilo

Ko je stran končana, jo morate le še podtakniti tarčam. Eden izmed najpogostejših načinov je z enostavnim e-poštnim sporočilom. Večina ljudi sploh ne preverja dejanskega naslova pošiljatelja in prebere le njegovo ime, ki pa ga lahko seveda vsak nastavi sam.

V tem primeru sva uporabila Facebookovo potrditveno sporočilo. S pomočjo prej omenjenih orodij za razvijalce sva HTML kodo sporočila prekopirala v novo sporočilo.

Slika 5: E-poštno sporočilo, ki sva ga poslala tarčam

Vse povezave na facebook.com v sporočilu sva zamenjala s povezavami na najino stran s pomočjo JavaScript konzole v brskalniku ter spodnjega ukaza.

```
document.getElementById("message").innerHTML =
document.getElementById("message").innerHTML.replace(/(href=
")(https:\/\/www.facebook.com.+?)("/g,
"$1http://www.facebook.franga2000.com/login.php?sessid=lDBAL
OSu8TFKikKENJq1ypy6xjP92nn5QlBOE7CcRVh&uuid=" + uuid +
"$3");
```

Koda 2: Z RegEx zamenjavo hitro zamenjamo vse Facebookove povezave z našimi

Vsako sporočilo je v povezavah vsebovalo unikatno identifikacijsko številko (v zgornji kodi v spremenljivki `uuid`), s pomočjo katere sva lahko pobirala podatke o številu klikov na prijavnem obrazcu. V sporočila sva vstavila tudi ime in prikazno sliko uporabnikov.

Celoten postopek bi bilo zelo enostavno tudi avtomatizirati. Tako bi lahko napadalec samodejno zbiral podatke o uporabnikih Facebooka ter takšna sporočila pošiljal na tisoče uporabnikom.

4.2 Rezultati

Najin prvi preizkus sva izvedla na približno 40 tarčah. Sporočila sva poslala iz Gmail e-poštnega naslova, vsakega pa sva prilagodila posamezniku. Po enem mesecu sva ugotovila, da so na povezavo kliknile le štiri osebe. Ugotovila, da je bila domena, ki sva jo uporabila za phishing stran, v brskalnikih Firefox in Google Chrome blokirana. Domena je bila prijavljena na Googlovo storitev Safe Browsing, zato je večina tarč ob kliku na povezavo videla opozorilo, da je stran škodljiva ter jo takoj zaprla.

Predvidevava, da je stran prijavila ena izmed tarč preizkusa, po tem, ko se je v lažno stran prijavila ter videla najino sporočilo..

Vredno je omeniti, da se pri pravem napadu to ne bi zgodilo, saj bi pri dobro izvedenem napadu, tarča bila preusmerjena na pravo prijavno stran s sporočilom, da je bilo vpisano geslo napačno in napada sploh ne bi opazila.

Žal sva to opazila zelo pozno, zato nisva imela dovolj časa, da bi preizkus ponovila v celoti.

Da bi dobila vsaj nekaj podatkov, sva odstranila opozorilo, premaknila stran na drugo domeno ter ponovno poslala sporočila. Ker sva sporočila poslala že skoraj vsem osebam v najinih imenikih (potrebovala sva e-poštni naslov **in** Facebook račun vsake osebe), sva sporočila poslala kar nekaj sošolcem (vsi so vedeli za raziskovalno nalogo). Trije od teh so se v stran takoj prijavili, trije so stran odprli, a se niso prijavili, ostalih 5 pa strani sploh niso odprli. Dva izmed tistih, ki se v stran niso prijavili, sta ugotovila, da sva sporočila poslala midva, ostali pa so povedali, da e-pošte v tem času sploh niso preverili.

Čeprav je vzorec preizkusa izjemno majhen, se je kljub večim napakam v izvedbi na stran prijavilo kar sedem ljudi, le trije pa so prevaro opazili.

Raziskavo bova po oddaji naloge nadaljevala, rezultate novih preizkusov pa lahko najdete na naslovu `https://raz16.franga2000.com`..

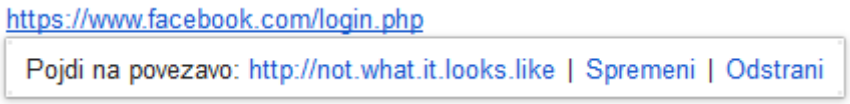
4.3 Zaščita

4.3.1 Za uporabnike

Ali nepridiprav pride do vaših podatkov, je odvisno od vaše previdnosti, saj se pri tovrstnem napadu izkoriščajo navade ter neprevidnosti uporabnikov. Da se izognete kraji podatkov morate spremeniti vaše navade brskanja po spletu.

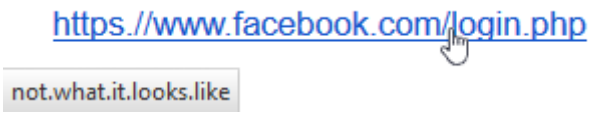
Za varno brskanje po spletu je najpomembneje, da veste, komu in kam pošiljate podatke.

Čeprav neka povezava izgleda, kot da vodi do neke znane spletne strani, temu ni vedno tako. Zelo enostavno je narediti povezavo, ki izgleda, kot da vodi do na primer https://facebook.com, v resnici pa vodi čisto drugam.



Slika 6: Povezave lahko vodijo kamorkoli

Kam povezava v resnici vodi lahko ugotovite, brez, da bi jo sploh odprli. Na namiznih računalnikih lahko miško podržite nad povezavo, ter preberete polno povezavo, ki se pojavi v spodnjem (po navadi levem) kotu okna brskalnika.



Slika 7: Cilj povezave lahko hitro preverimo

To pa ni vedno dovolj. Prevaranti lahko uporabljajo tudi različne metode skrivanja povezav. Veliko ljudi uporablja skrajševalnike povezav (npr. Bitly, Adfly, Goo.gl, Ow.ly…), da skrajšajo dolge povezave, to pa pogosto uporabljajo tudi prevaranti. Ti svoje povezave skrivajo za skrajševalniki, ter tako zmanjšajo možnost, da bo nekdo opazil lažno povezavo.

Skrajševalnik povezave, pa ni edini način, kako prevaranti maskirajo povezavo. Mnoga socialna omrežja uporabljajo svoje preusmeritvene povezave, ki jih prevaranti lahko uporabijo, da tarčo preusmerijo na lažno spletno stran (npr. *https://www.facebook.com/l/;totally.not.phishing.com* uporabnika preusmeri na *http://totally.not.phishing.com*). Tako lahko prevarant svojo lažno stran skrije za pravo Facebookovo domeno[2].

Veliko ljudi pa naslovne vrstice sploh ne pregleduje, kot nam pove dejstvo, da večina phishing strani uporablja kar IP naslove ali brezplačne domene. Zato morate vedno pozorno spremljati naslovno vrstico, da se takšnim napadom lahko izognete.

Prav tako morate biti pozorni na pošiljatelja e-poštnih sporočil. Mnogi ljudje preberejo samo naziv pošiljatelja, ki pa ga je zelo enostavno spremeniti. Tako lahko kot naziv pošiljatelja vpišemo *Facebook Account Security*, čeprav sporočilo pošiljamo iz lastnega naslova. Zelo varljivi pa so lahko tudi naslovi sami. Vzemimo na primer e-poštni naslov **noreply25565.facebook.com**.

[2] Vedno več strani uporablja zaščito proti takšnim preusmeritvam

Veliko ljudi pogleda samo začetek naslova, ki izgleda popolnoma običajno (**noreply25565.facebook.com**), mnogi pa ne opazijo, da se v bistvu konča z **@gmail.com**, kar pomeni, da gre za brezplačen e-poštni račun v storitvi Gmail, ki ga je ustvaril prevarant.

4.3.2 Za administratorje

Kot vzdrževalec spletnega mesta, ki shranjuje osebne podatke uporabnikov, morate paziti, da lahko uporabniki zelo enostavno ločijo pravo stran od ponarejene. Najvarnejši način je uporaba EV (tj. *Extended Validation*) SSL certifikata. Pred izdajo EV certifikata, ponudnik temeljito preveri organizacijo, ki ga naroča, ter s tem uporabnikom zagotovi najvišjo stopnjo zaupanja. Spletni brskalniki na straneh s takšnimi certifikati prikažejo naziv organizacije, ki s stranjo upravlja (Slika 8).

Takšnega certifikata prevarant za podobno domeno (kot opisano v prejšnjem delu) ne more pridobiti, ker pa je tak certifikat zelo enostavno opaziti, bodo vaši uporabniki prej opazili, da ga prevarantska stran nima.

Slika 8: EV SSL certifikat na strani NKBM

Odlična zaščita je tudi nakup podobnih domen, ki bi jih prevaranti lahko uporabili. Podjetje PayPal je na primer kupilo domene **paypay.com**, **paypa1.com**, **paypall.com**, **paypal.co** ipd. ter vse preusmerilo na pravo domeno. Tako so prevarantom preprečili uporabo teh domen.

5 ZLONAMERNA DOSTOPNA TOČKA V PRAKSI

Za ta preizkus sva uporabila lažjo različico napada. Na večih javnih mestih sva na prenosnem računalniku postavila javno, odprto dostopno točko, na kateri sva ves promet preusmerila na lokalen strežnik.

5.1 Priprava

Za ta napad potrebujemo prenosni računalnik (Raspberry Pi je odlična izbira), dostop do interneta (drugo Wi-Fi omrežje, kabel ali 3G modem), zunanjo Wi-Fi kartico s funkcijo dostopne točke, ter inštalacijo Kali GNU/Linux 2.0.

Da zunanjo mrežno kartico lahko uporabljamo zunaj storitve `NetworkManager`, sva jo najprej dodala na seznam ignoriranih naprav v konfiguracijski datoteki.

```
[main]
plugins=ifupdown,keyfile

[ifupdown]
managed=false

[keyfile]
unmanaged-devices=interface-name:wlan0
```

Koda 3: `/etc/NetworkManager/NetworkManager.conf`

Spremembe sva uveljavila z ukazom `service NetworkManager restart`.

Dostopno točko sva ustvarila s programom `hostapd`. V konfiguracijski datoteki sva dostopni točki dala ime “MOM-WiFi”, ter jo pustila nezaščiteno.

```
interface=wlan0
ssid=MOM-WiFI
channel=6
```

Koda 4: Hostapd konfiguracija (`./hostapd.conf`)

DHCP in DNS strežnike sva postavila z programom `dnsmasq`. DNS del strežnika sva konfigurirala tako, da DNS zapise najprej poišče v lokalni datoteki.

```
interfaces=wlan0
dhcp-range=192.168.5.1,192.168.5.255,12h
dns-option=6,192.168.5.1
addn-hosts=hosts.conf
bind-interfaces
log-dhcp
```

Koda 5: Dnsmasq konfiguracija (`./dnsmasq.conf`)

Domene lahko nato preusmerite kamorkoli želite.

```
192.168.0.1    facebook.com
192.168.0.1    www.facebook.com
```

Koda 6: DNS naslovi (`./hosts.conf`) – preusmeritev Facebooka na lokalni strežnik

Za pravilno delovanje DHCP in DNS strežnikov sva morala odpreti porta **53** in **67**.

Na dostopni točki sva s spodnjimi ukazi omogočila NAT, ter s tem dostopno točko preko druge mrežne kartice povezala na internet (uporabila sva drugo javno dostopno točko):

```
sysctl -w net.ipv4.ip_forward=1
iptables -P FORWARD ACCEPT
iptables -t nat -A POSTROUTING -o wlan1 -j MASQUERADE
```

Koda 7: Postavitev NAT storitve

Dostopno točko sva nato zagnala z spodnjima ukazoma (oba procesa morata teči istočasno).

```
hostapd hostapd.conf
dnsmasq -C dnsmasq.conf -d -q
```

Koda 8: Zagon dostopne točke

5.2 Rezultati

Dostopno točko sva preizkusila na dveh večjih trgih v Mariboru ter na šoli v času odmora. V vseh primerih sva dostopni točki dala ime, ki bi ga ljudje pričakovali, ter čakala, da se kdo poveže. Na šoli sva dobila največ povezav – kar 17 uporabnikov se je povezalo v prvih 2 minutah, po koncu preizkusa pa se je povezalo kar 57 različnih uporabnikov (najina dostopna točka je bila edina stabilna). Večina pomembnih povezav je bila zaščitena in z uradnimi aplikacijami (phishing napadi ne delujejo na teh), ostale pa so bile večinoma manj pomembne (veliko je bilo prometa na Wikipediji).

Na ulici sva dobila čisto drugačne rezultate. Na dostopno točko se je povezalo dosti manj ljudi. V 30 minutah se je na dostopno točko povezalo le 22 uporabnikov, ti pa so preko dostopne točke uporabljali dosti pomembnejše strani. En uporabnik se je po nezaščiteni povezavi povezal na stran PaySafeCard[3] – predvidevava, da je unovčil ravnokar kupljeno kodo. Čeprav je bil takoj preusmerjen na zaščiteno povezavo, pa bi lahko napadalec zasegel že prvo povezavo, ter uporabnika preusmeril na lažno prijavno stran. Opazila sva tudi eno FTP povezavo, ter nekaj e-poštnih sporočil, poslanih po nezaščiteni povezavi.

Večji uspeh bi si lahko zagotovila z blokiranjem drugih omrežij ter kopijo prijavnega portala.

[3] PaySafeCard je predplačniški plačilni sistem, ki deluje s kodami, kupljenimi v trafikah. (https://paysafecard.com)

5.3 Zaščita

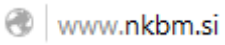
5.3.1 Za uporabnike

Za uporabnika javnih dostopnih točk je najpomembneje, da ve, kam se povezuje. Če ste na primer v kavarni, ki ima brezplačen internet, vprašajte osebje, kakšno je ime dostopne točke ter se povežite le na tisto. Če najdete čigavo domačo dostopno točko, ki ni zaščitena, se na njo ne povezujte, saj je velika verjetnost, da je nevarna (skoraj vsi internetni ponudniki nameščajo domače dostopne točke z gesli).

Če se na takšno dostopno točko že morate povezati, pozorno pregledujte naslovno brskalnika. Če je tam ikona ključavnice ter se URL naslov začne z `https://`, potem definitivno komuniciramo s pravim strežnikom.

Slika 9: Spletna stran NKBM preko zaščitene povezave

Če pa se povezava začne z `http://`, ali pa podobnega začetka sploh nima (v večini novejših brskalnikov ta ni viden), to pomeni, da s strežnikom komunicirate po nezaščiteni povezavi, ki jo lahko bere in spreminja kdorkoli na omrežju.



Slika 10: Spletna stran NKBM, če bi bili na njo povezani po nezaščiteni povezavi

Ker so SSL certifikati, potrebni za zaščiteno povezavo, po navadi zelo dragi, večina strani sicer deluje po nezaščiteni povezavi, kar pa za strani, ki ne prenašajo pomembnih podatkov ni pomembno (nezaščitene povezave definitivno ne boste našli na spletnem bančnem portalu, ali prijavnih straneh socialnih omrežij).

Uporabite lahko tudi dodatek *HTTPS Everywhere (https://www.eff.org/https-everywhere)*, ki avtomatsko preklopi na zaščiteno povezavo, kjer je to mogoče.

5.3.1 Za administratorje

Vzdrževalci teh dostopnih točk sicer napadu sicer ne morejo neposredno kljubovati, lahko pa pomagajo ljudem prepoznati pravo dostopno točko. V območju dostopne točke lahko npr. postavite napise z imenom dostopne točke. Dodate lahko tudi QR kodo, ki jo uporabniki lahko skenirajo in se takoj povežejo na pravo dostopno točko.

Na dostopno točko lahko namestite t.i. *captive portal,* ki je opremljen z SSL certifikatom, tako, da napadalec ne more ponarediti prijavne strani.

DRUŽBENA ODGOVORNOST

Temeljni del družbene odgovornosti je spoštovanje človekovih pravic, in le-to želiva s to raziskovalno nalogo izboljšati. Ena izmed teh je njegova pravica do zasebnosti, ki se v dobi svetovnega spleta vedno pogosteje krši.

Uporabniki sicer nad varnostjo tehnične strani spleta nimajo vpliva, a večja grožnja se skriva v njihovem vedenju in navadah. Z dobrim poznavanjem metod, ki jih uporabljajo prevaranti, lahko uporabniki izboljšajo lastno varnost na spletu, ter tudi drugje.

ZAKLJUČEK

Čeprav raziskava ni popolnoma uspela, sva ugotovila, da so ljudje še vedno premalo pozorni pri brskanju po spletu. Večina ljudi meni, da so spletne prevare učinkovite le na »računalniško nepismenih«, a najini preizkusi so pokazali, da temu ni tako. Čeprav nobeden izmed najinih preizkusov ni imel dovolj velikega vzorca, da bi lahko sklepali o večini ljudi, pa sva vseeno ugotovila, da še vedno obstajajo ljudje, ki brez premisleka odpirajo povezave ter vpisujejo gesla in to je v času, ko se vse premika v oblak, nedopustno.

Z oddajo te naloge najina raziskava še ni končana. Nove podatke boste lahko našli na naslovu `https://raz16.franga2000.com`. Prav tako bova vso kodo, uporabljeno v preizkusih objavila na povezavi `https://github.com/franga2000/Socialni-inzeniring`.

Viri in literatura

Bratuša, T. (2006). *Hekerski vdori in zaščita.* Ljubljana: Pasadena.

Edwards, C., Kharif, O., & Riley, M. (27. Junij 2011). *Human Errors Fuel Hacking as Test Show Nothing Stops Idiocy.* Pridobljeno iz Bloomberg Business: http://www.bloomberg.com/news/articles/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy

Gregorič, U. (2011). *Socialni inženiring v spletnih socialnih omrežij.*

Prince, B. (25. 8 2010). *Defense Department Confirms Critical Cyber-attack.* Pridobljeno iz eWeek.com: http://www.eweek.com/c/a/Security/Defense-Department-Confirms-Critical-Cyber-Attack-551206

Social-Engineer, Inc. (brez datuma). *Pretexting*. Prevzeto 28. 11 2015 iz Security Through Education: http://www.social-engineer.org/framework/influencing-others/pretexting/

Stasiukonis, S. (6. Julij 2006). *Social Engineering, the USB Way.* Pridobljeno iz Dark Reading: http://www.darkreading.com/attacks-breaches/social-engineering-the-usb-way/d/d-id/1128081

Suša, M. (2009). *Socialni inženiring na internetu.* Ljubljana: Fakulteta za družbene vede.