HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Phishing napadi

CCERT-PUBDOC-2005-01-106

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.
Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, **www.lss.hr**- laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

Sustav elektroničke pošte (eng. e-mail) oduvijek je bio vrlo privlačna meta za neovlaštene korisnike. Iznimno velik broj korisnika koji se koriste elektroničkom poštom te popularnost i jednostavnost SMTP protokola, elementi su koji e-mail servis čine idealnim izborom kada se radi o planiranju i provođenju neovlaštenih aktivnosti. U prilog tomu idu i statistički podaci koji jasno pokazuju da se najveći broj malicioznih aktivnosti provodi upravo putem e-mail servisa. Nakon virusa, crva, neželjene elektroničke pošte (SPAM-a), hoax poruka i različitih kombinacija ovih prijetnji, u posljednje vrijeme na Internetu je uočen izniman porast tzv. *phishing* napada, koji se u većini slučajeva također baziraju na korištenju e-mail servisa. Kod *phishing* napada neovlašteni korisnici nastoje doći do povjerljivih korisničkih podataka, koji će im omogućiti izravno ili neizravno ostvarivanje financijske koristi. Najčešće je riječ o korisničkim zaporkama, PIN brojevima, brojevima kreditnih kartica te drugim sličnim povjerljivim podacima koji neovlaštenom korisniku omogućuju pristup informacijskom sustavu financijske ustanove (najčešće banke), u kojoj korisnik posjeduje svoje račune i putem koje obavlja financijske transakcije.

U vrijeme kada popularnost Internet bankarstva i obavljanja transakcija korištenjem Interneta raste iz dana u dan, ovakvi napadi su posebno učinkoviti i opasni. Zlonamjernim korisnicima dodatno u prilog ide i nedovoljna edukacija korisnika te slabo poznavanje Internet tehnologija i opasnosti koje s njima dolaze. Problem je dodatno naglašen činjenicom da se svakim danom javljaju nove i sve naprednije tehnike provođenja *phishing* napada. E-mail više nije jedini medij koji se koristi u ovu svrhu. Sve su češći primjeri koji koriste *instant messaging* aplikacije, lažirane *banner* poruke na Web poslužiteljima, specijalno razvijene *trojan horse* programe te brojne druge tehnike kojima se pokušava povećati učinkovitost napada.

U dokumentu su opisane osnovne karakteristike i način provođenja *phishing* napada, tehnike koje neovlašteni korisnici najčešće koriste te sigurnosne mjere kojima je moguće spriječiti ili ublažiti posljedice napada. Također su izneseni i relevantni statistički podaci koji ukazuju na ozbiljnost ovog problema i važnost njegovog suzbijanja.

2. Phishing

Iako postoji nekoliko različitih definicija *phishing* napada, u osnovi one se mnogo ne razlikuju. *Phishing* napadi podrazumijevaju aktivnosti kojima neovlašteni korisnici korištenjem lažiranih poruka elektroničke pošte i lažiranih Web stranica financijskih organizacija pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka. Pritom se prvenstveno misli na podatke kao što brojevi kreditnih kartica, korisnička imena i zaporke, PIN kodovi i sl., iako postoje i druge alternative.

Termin *phishing* dolazi od engleske riječi "*fishing*" kojom se metaforički opisuje postupak kojim neovlašteni korisnici mame korisnike Interneta kako bi dobrovoljno otkrili svoje povjerljive podatke. Pretpostavlja se da prefiks **ph** dolazi od termina *phreaking,* danas već prilično zaboravljene tehnike kojom su neovlašteni korisnici kompromitirali telefonske sustave. Spajanjem ove dvije fraze (*fishing* + *phreaking*) dobivena je nova kovanica pod nazivom ***phishing***.

Iako se termin *phishing* prvi puta pojavio još 1996. godine na `alt.2600` hakerskoj newsgrupi, tek se posljednjih godina isti proširio u široj javnosti i to ponajviše zbog iznimnog porasta neovlaštenih aktivnosti ovog tipa. Iako u Republici Hrvatskoj još nisu zabilježeni primjeri *phishing* napada, u razvijenijim zemljama ovaj je problem postao prilično aktualan i sve se više pažnje posvećuje edukaciji korisnika i ostalim sigurnosnim kontrolama koje mogu pomoći u sprječavanju takvih napada.

Najveći problem u prevenciji *phishing* napada je taj što se isti ne bazira isključivo na tehničkim elementima, već se koriste sve složenije i naprednije tehnike socijalnog inženjeringa (engl. *social engineering*), koje iskorištavaju neiskustvo i neznanje korisnika Interneta. Kreiranjem specijalno osmišljenih i lažiranih poruka elektroničke pošte, korisnika se pokušava navesti na dobrovoljno i nesvjesno odavanje vlastitih povjerljivih informacija neovlaštenom korisniku.

Provođenje napada dodatno olakšavaju brojne napredne tehnologije za izradu Web stranica (JavaScript, DHTML, ActiveX, Flash itd.), koje osim svojih legitimnih primjena sve više mjesta pronalaze u neovlaštenim aktivnostima kao što je npr. *phishing*. Korištenjem navedenih tehnologija moguće je osmisliti vrlo složene napade koji će zavarati i najiskusnije korisnike. Dodatni problem predstavljaju i

brojne ranjivosti unutar različitih Web preglednika i e-mail klijenata, koje u kombinaciji sa nekim od navedenih tehnologija predstavljaju vrlo moćno oružje u rukama neovlaštenih korisnika. Kao najbolji dokaz tomu su statistički podaci koji pokazuju broj korisnika koji su prevareni ovim putem. Nešto više informacija o statističkim podacima vezanim uz *phishing* napade dano je u poglavlju (Poglavlje 6).

3. Tijek napada

Tijek provođenja *phishing* napada moguće je podijeliti u nekoliko faza:

1. osmišljavanje i pripremanje napada,
2. provođenje napada,
3. prikupljanje povjerljivih informacija i njihovo iskorištavanje.

Slijedi kratki opis pojedinih faza.

3.1. Osmišljavanje i pripremanje napada

U fazi pripreme napada, napadač prikuplja informacije o organizaciji koja se želi kompromitirati te korisnicima koji su potencijalne mete napada. Budući da učinkovitost napada u velikoj mjeri ovisi o tome koliko je napad pažljivo i detaljno planiran, iskusniji neovlašteni korisnici ovoj fazi posvećuju dosta vremena i resursa.

Prvi korak osmišljavanja, odnosno pripreme napada podrazumijeva identifikaciju ciljne organizacije, detaljnu analizu sadržaja i uočavanje sigurnosnih propusta unutar Web stranica, identifikaciju ranjivosti na strani klijenta te druge slične postupke. Na temelju prikupljenih informacija napadač kreira lažiranu kopiju Web stranica ciljne organizacije te osmišljava sadržaj *phishing* poruka koje će prosljeđivati potencijalnim metama napada. Načini kreiranja lažiranih Web stranica ovise prvenstveno o iskustvu i vještini neovlaštenih korisnika, a slično vrijedi i za lažiranje poruka elektroničke pošte. Dosadašnja iskustva pokazuju da se *phishing* napadi mogu prilično razlikovati u složenosti i sofisticiranosti, što kasnije utječe i na njihovu učinkovitost. Poruke elektroničke pošte nastoje se oblikovati tako da djeluju službeno, pri čemu se sadržajem poruke kod korisnika pokušavaju izazvati osjećaji koji će smanjiti mogućnost realne procjene situacije (strah, nesigurnost i sl.).

U fazu osmišljavanja i pripreme također spada i postupak identifikacije ranjivih e-mail poslužitelja koji će se iskoristiti za prosljeđivanje poruka elektroničke pošte. U tu svrhu najčešće se koriste nezaštićeni e-mail ili *proxy* poslužitelji (eng. *open relay*), a sve češće se koriste i kompromitirana osobna računala na kojima su instalirani specijalni programi koji omogućuju slanje e-mail poruka. Nakon što su pripremljeni svi upravo opisani elementi napadač može nastaviti sa sljedećim fazama provođenja napada.

3.2. Provođenje napada

U fazi provođenja napada, napadač šalje pripremljene poruke elektroničke pošte na adrese korisnika koji su odabrani kao potencijalne mete napada. Osim sustava elektroničke pošte, poruke je moguće distribuirati i putem *newsgrupa*, ICQ-a i drugih sličnih *instant messaging* servisa, oglašavanjem putem *bannera* na Web stranicama i sl.

Osim korisnika koji su ciljane mete napada, napadači vrlo često koriste i dodatne kanale kojima bi mogli privući veći broj korisnika. Tako na primjer, napadači lažirane Web stranice vrlo često prijavljuju na Internet tražilice, kako bi se na taj način privukli oni korisnici koji za dolazak do adresa Web stranica koriste alate kao što je npr. Google pretraživač. Nakon što su poruke poslane na pripremljene adrese napadač se prikriva i očekuje prve žrtve napada.

3.3. Prikupljanje povjerljivih informacija

U finalnoj fazi napada, napadač putem lažiranih Web stranica prikuplja povjerljive informacije od krajnjih korisnika i pohranjuje ih za kasnije korištenje. Prikupljeni podaci mogu se iskoristiti za izravno ostvarivanje financijske koristi ili ih je moguće dalje prodavati zainteresiranim osobama. Krajnji cilj ove faze je svakako financijska korist.

4. Tehnike provođenje napada

Nakon osnovnih pojmova i pojašnjenja samog termina *phishing-a*, u nastavku će ukratko biti opisan tipičan primjer provođenja *phishing* napada. Slično kao i kod drugih malicioznih aktivnosti, metode provođenja napada svakodnevno napreduju kako bi se povećala njihova učinkovitost. U slučaju *phishing* napada, zabilježeno je nekoliko različitih tehnika koje će ukratko biti opisane u ovom dokumentu.

4.1. Maskiranje URL adresa

Jedna od najčešćih tehnika koju *phiseri* koriste prilikom lažiranja poruka elektroničke pošte je maskiranje URL adresa (engl. *URL obfuscation*). Korištenjem specijalnih tehnika, URL adrese navedene unutar poruka elektroničke pošte korisnika preusmjeravaju na maliciozne Web stranice, koje su svojim izgledom vrlo slične, najčešće gotovo identične Web stranicama financijske ustanove koja se želi lažno prikazati. Vjerujući da se radi o službenim Web stranicama ustanove, korisnik u predviđenu Web formu unosi povjerljive podatke, a da pritom nije svjestan da se radi o prijevari. Tehnike maskiranja URL adresa najčešće ovise o iskustvu i vještini neovlaštenog korisnika, no u većini slučajeva dovoljno su složene da mogu zavarati i one iskusnije korisnike. Većina tehnika maskiranja URL adresa bazira se na korištenju naprednih svojstava HTML jezika i drugih srodnih tehnologija (Java Script, ActiveX, DHTML i sl.), što znači da korištenje ovakvih tehnika nije moguće kod poruka u čistom tekstualnom obliku (engl. *plain tex)*.

U nastavku poglavlja ukratko su opisane neke od najpopularnijih tehnika maskiranja URL adresa.

- **Korištenje domena sličnog imena**

Najčešći i najjednostavniji primjer URL maskiranja zasigurno je korištenje imena domene koje se na prvi pogled ne razlikuje od legitimnog imena domene organizacije koja se impersonira. Npr. ukoliko se želo kompromitirati banka čije se legitimne stranice nalaze na adresi http://www.banka.hr, korištenje naziva domena kao što su www.banka.city.hr, banka.private.hr, www.banka.biz zavarati će iznenađujuće velik broj korisnika.

Naravno, poznati su i slučajevi gdje su korištene znatno složenije metode koje su dodatno otežavale mogućnost detekcije napada. Npr. registracija domena korištenjem specijalnih znakova iz određenog jezičnog područja, zatim zamjena slova O sa brojem 0, ili velikog slova I sa malim slovom l i sl. Iskustva pokazuju da ovakve jednostavne tehnike maskiranja mogu biti vrlo učinkovite i vrlo efikasne u smislu zavaravanja korisnika.

- **Korištenje URL adresa s uključenim korisničkim imenom i zaporkom**

Poznato je da većina modernih Web preglednika sadrži mogućnost da se kao dio URL adrese navede korisničko ime i zaporka korisničkog računa pod čijim se ovlastima pristupa Web sadržajima. Format URL adrese u tom slučaju je http://username:password@www.example.com.

Slično kao i u brojnim drugim slučajevima, vješti napadač ovakvu konstrukciju URL adrese može iskoristiti za preusmjeravanje korisnika na adresu na kojoj se nalaze maliciozne Web stranice postavljenje u svrhu prikupljanja povjerljivih korisničkih informacija.

Npr. URL adresa http://banka:internet_bankarstvo@malicious.com/login.php neiskusnog će korisnika preusmjeriti na Web poslužitelj na adresi malicious.com, iako je on uvjeren da se radi o službenim Web stranicama banke.

S obzirom na mogućnosti primjene ovakve strukture URL adresa u maliciozne svrhe, Microsoft je u novijim inačicama Internet Explorera uklonio ovu funkcionalnost.

- **Skraćene URL adrese**

Budući da Web aplikacije vrlo često koriste složene i prilično dugačke URL adrese, pojavile su se organizacije koje nude besplatnu uslugu kojom se takve dugačke adrese skraćuju na prihvatljivije duljine. Jedna od takvih usluga je i ona koja se može naći na adresi http://www.tinyurl.com.

Koristeći tehnike socijalnog inženjeringa i svojstava pojedinih klijenata za pregledavanje elektroničke pošte, koji dugačke URL adrese razlome u više redaka, *phiseri* vrlo često upravo ovakve servise koriste za preusmjeravanje prometa na svoje poslužitelje. Umjesto da se od korisnika zahtjeva da dijelove dugačke, izlomljene adrese nekoliko puta kopiraju u **Adress Bar** polje Web preglednika, lažirane poruke korisnicima nude mogućnost da koriste skraćeni oblik koji će korisnika preusmjeriti na maliciozni poslužitelj.

U tom slučaju *phishing* poruka elektroničke pošte sadrži informacije koje korisnika navode da posjeti skraćeni oblik URL adrese, kako bi se izbjegli problemi sa razlomljenim URL adresama. Neiskusniji korisnici vrlo često prihvaćaju takvu mogućnost, što napadačima dodatno olakšava provođenje napada.

- **Kodiranje URL adresa**

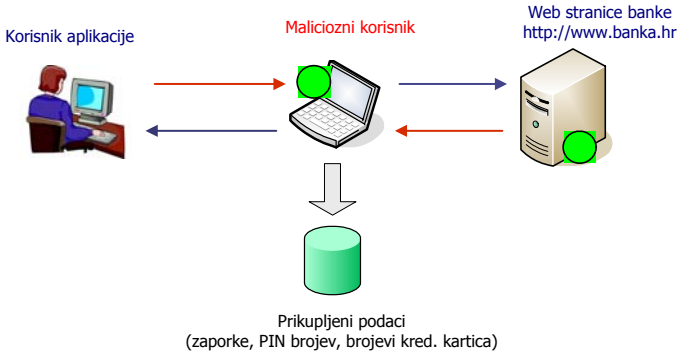
Kako bi se osigurala podrška za različite jezične skupine, većina novijih programskih paketa podržava različite tipove kodiranja kojima je moguće prikazati specifične dijakritičke znakove. Takav je slučaj i sa većinom modernih Web preglednika, što neovlašteni korisnici često koriste za provođenje neovlaštenih aktivnosti. Osim *phishing* napada, gdje je ovo svojstvo iznimno praktično za zavaravanje korisnika, slične tehnike koristile su se i za provođenje brojnih drugih napada.
Neke od osnovnih tehnika kodiranja URL adrese opisane su u nastavku:

- *URL kodiranje (escaped encoding)* – klasičan oblik kodiranja URL adresa specifičan po znaku % koji se stavlja ispred heksadecimalnog zapisa znaka koji se kodira. Npr. znak / prikazuje se u obliku niza %2F.
- *Unicode kodiranje* – Unicode je internacionalni standard za kodiranje znakova, koji korištenjem 16-bitnog zapisa omogućuje prikaz gotovo 50000 znakova iz različitih jezičnih skupina. Standard je razvijen zbog ograničenog broja znakova koje je bilo moguće prikazati u ASCII formatu, zbog čega su različita jezična područja koristila različite implementacije ASCII kodiranja. S obzirom na probleme kompatibilnosti sa starijim sustavima s vremenom su razvijene modificirane inačice ovog standarda od kojih je svakako najpoznatiji UTF-8 standard opisan u nastavku.
- *UTF*-8 – kodiranje UTF-8 standardom podržava kodiranje znakova korištenjem jednog do šest bajtova. To znači da se isti znak može prikazati na nekoliko različitih načina, a dodatna pogodnost je ta što je ovaj standard u potpunosti kompatibilan sa tradicionalnim ASCII kodiranjem.
  Primjer korištenja UTF-8 standarda prikazan je na kodiranju znaka točka ("."). 8-bitni prikaz 2E, 16-bitni prikaz C0 AE, 24-bitni prikaz E0 80 AE, 32-bitni prikaz F0 80 80 AE itd.
- *Heksadecimalni, oktalni i decimalni prikaz* – kod prikaza URL adrese moguće je uvijek koristiti i drugačiji format zapisa IP adrese kako bi se zavaralo korisnika. Npr. decimalni prikaz adrese http://192.168.1.1 moguće je prikazati na sljedeće načine:
  - heksadecimalni prikaz – http://0xC0.0xA8.0x1.0x1
  - oktalni prikaz – http://0300.0250. 0001

  Na sličan način moguće je koristiti i prikaz bez korištenja znaka točke kojim se odvajaju pojedini dijelovi adrese (engl. *dotless*). Npr. http:// 3232235777 u decimalnom obliku ili http:// C0A80101 u heksadecimalnom obliku.

4.2. Man in the Middle napadi

Presretanje komunikacije između klijenta i poslužitelja jedna je od najčešćih tehnika dolaska do povjerljivih korisničkih informacija. Ubacivanjem u komunikacijski kanal uspostavljen između klijenta i poslužitelja napadač je u mogućnosti analizirati kompletni promet koji se razmjenjuje između ove dvije točke, čak i onda kada se koristi kriptirana komunikacija. Samim time, primjena Man in the Middle (MITM) napada gotovo je idealna za provođenje *phishing* napada.
Za uspješnu realizaciju napada, klijenta je potrebno preusmjeriti na malicioznu adresu putem koje će se promet dalje preusmjerivati na legitimne Web poslužitelje financijske ustanove koja se želi lažno prikazati. Napadačevo računalo u tom slučaju obavlja funkciju *proxy* poslužitelja, pri čemu bilježi sve podatke koji su neophodni za daljnje provođenje napada. Na sljedećoj slici prikazan je osnovni koncept MITM napada.

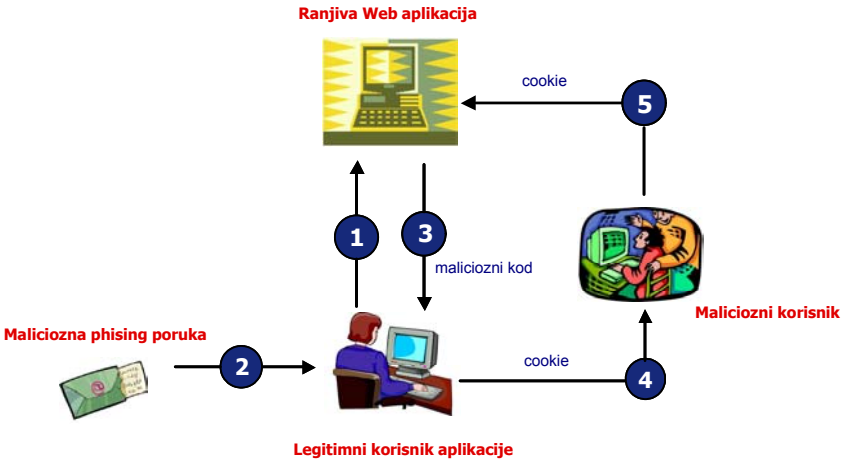


Slika 1: Presretanje komunikacije između klijenta i poslužitelja

Tehnike kojima se korisnici navode na maliciozne *proxy* poslužitelje variraju. Osim tehnika maskiranja URL adresa opisanih u prethodnom poglavlju, moguće je koristiti i znatno složenije napade koji će dodatno otežati detekciju napada.
Jedna od mogućnosti je korištenje DNS *cache poisoning* napada. U tom slučaju napadač u DNS bazu banke ili neke druge financijske ustanove ubacuje maliciozne DNS zapise koji će korisnike, umjesto na legitimne Web poslužitelje ustanove, preusmjeriti na malicioznu adresu koja je pod kontrolom neovlaštenog korisnika. Osnovni problem ove metode je taj da neovlašteni korisnik mora biti u mogućnosti kompromitirati DNS poslužitelj ciljane ustanove, što vrlo često zahtjeva dodatna znanja i iskustva.

4.3. Cross Site Scripting

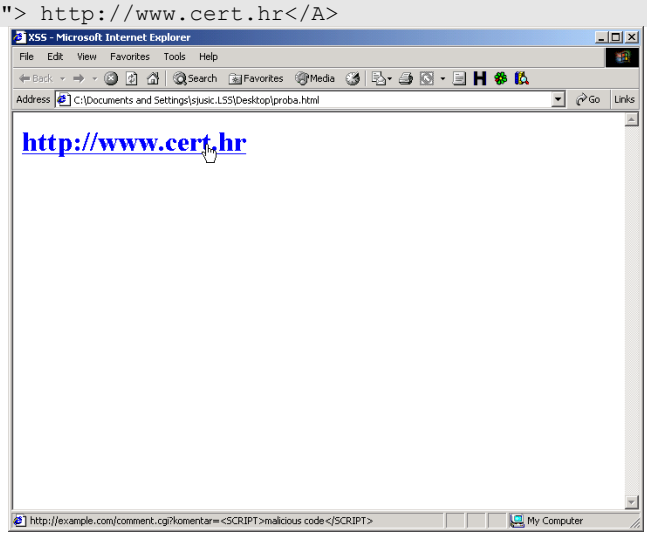
Za dolazak do povjerljivih korisničkih podataka napadač može iskoristiti i sigurnosne propuste unutar Web aplikacije ustanove čiji se korisnici žele kompromitirati. Ukoliko je aplikacija ranjiva na *Cross Site Scripting* (XSS) napade, napadaču se otvaraju dodatne mogućnosti za provođenje napada.
Za one čitatelje koji nisu upoznati sa *Cross Site Scripting* napadima, potrebno je reći da je to vrsta napada kojom se unutar Web preglednika korisnika pokušava izvršiti maliciozni skriptni kod (najčešće Java Script ili VBS Script), koji će napadaču omogućiti realizaciju zlonamjernih postupaka. XSS ranjivost najčešće se javlja kao posljedica nedovoljnog filtriranja sadržaja koje aplikacija ispisuje na Web stranice. Ukoliko aplikacija bez ikakve provjere na stranicu ispisuje podatke koje korisnik može proizvoljno uređivati, vrlo je velika vjerojatnost da je aplikacija ranjiva na XSS napad. Ukoliko korisnik aplikaciji, umjesto legitimnih podataka prenese maliciozni skriptni kod koji će aplikacija bez provjere ispisati unutar stranice, taj će se kod izvršiti unutar Web preglednika krajnjeg korisnika.
Na sljedećoj slici prikazan je osnovni koncept XSS napada (Slika 2).



Slika 2: Cross Site Scripting

U prvom koraku legitimni se korisnik prijavljuje u sustav korištenjem odgovarajućeg Web sučelja i nastavlja sa radom unutar aplikacije. U tom trenutku napadač istom korisniku prosljeđuje malicioznu poruku elektroničke pošte u kojoj je sadržana URL adresa s ugrađenim malicioznim skriptnim kodom, koji se želi izvršiti na korisnikovom računalu. Maliciozni kod izvršava se unutar korisničkog Web preglednika (korak 3) te izvršava maliciozne radnje određene učitanim kodom (u ovom slučaju krađa Web kolačića u kojem je sadržan identifikator sjednice za pristup sustavu). U koracima 4 i 5 napadač pomoću prikupljenih podataka ostvaruje pristup sustavu.
Primjer XSS napada opisan je u nastavku:

```
<A HREF="http://example.com/comment.cgi? komentar=<SCRIPT>malicious
code</SCRIPT>"> http://www.cert.hr</A>
```



Slika 3: Maliciozna URL adresa

Pritiskom na navedenu URL adresu korisnik se usmjerava na poslužitelj `example.com`, gdje se ujedno nalazi i ranjiva Web aplikacija koja izravno na stranicu ispisuje sadržaj parametra `komentar`. Ukoliko parametar `komentar` sadrži maliciozni skriptni kod, taj će se kod izvršiti unutar korisnikovog Web preglednika, ponekad i s prilično visokom razinom ovlasti budući da dolazi sa stranice kojoj korisnik inicijalno vjeruje. Maliciozni kod koji će se izvršiti na strani klijenta ovisi o vještini napadača i tipu napada koji se provodi, a najčešće se koristi programski kod kojim se prikupljaju *cookie* datoteke koje sadrže identifikatore sjednice za pristup Web aplikaciji. Prikupljene podatke neovlašteni korisnik kasnije može iskoristiti za daljnje provođenje malicioznih aktivnosti.
Također treba napomenuti da postoje različite varijante XSS napada, ovisno o načinu na koji se klijentu prosljeđuje maliciozni kod. U upravo opisanom primjeru u tu je svrhu iskorištena lažirana poruke elektroničke pošte sa malicioznom URL adresom u koju je ugrađen skriptni kod koji se želi izvršiti.
Jedna od varijanti XSS napada, koja je posebno zanimljiva sa stanovišta provođenja *phishing* napada, je ona koja iskorištava svojstva pojedinih aplikacija da unutar određene stranice učita sadržaj druge, vanjske, Web stranice.
Npr., zamislimo Web aplikaciju koja putem parametra unutar URL adrese omogućuje učitavanje vanjskih Web sadržaja. URL adresa u tom slučaju imala bi oblik sličan ovome http://www.banka.com/index.php?URL=http://www.malicious.com. Posjećivanjem navedene adrese unutar index.php stranice, automatski se učitava sadržaj koji se nalazi na adresi www.malicious.com. Ukoliko se radi o malicioznom sadržaju isti će biti izvršen unutar Web preglednika klijenta koji pristupa stranici.
Za potrebe *phisnig* napada, napadač može kreirati lažiranu Web stranicu koja će biti identična Web stranicama banke ili neke druge financijske organizacije čiji su korisnici meta napada. Ukoliko se takva, maliciozna Web stranica učita u Web preglednik korisnika, on neće biti svjestan da se radi o lažiranoj Web stranici kojoj je jedini cilj prikupljanje povjerljivih korisničkih informacija. Naravno, za

uspješno provođenje napada ciljna Web aplikacija organizacije mora omogućavati učitavanje proizvoljnih vanjskih Web sadržaja.
Tijek napada u tom je slučaju vrlo jednostavan. Napadač korisniku prosljeđuje lažiranu poruku elektroničke pošte koja sadržava sljedeću URL adresu http://www.banka.com/index.php?http://www.malicious.com/fakepage.html (naravno, pritom se vrlo često koriste tehnike maskiranja URL adresa kako bi se otežala mogućnost detekcije napada te dodatne tehnike koje su specifične za *phishing* napade). Unutar legitimnih Web stranica organizacije www.bank.com u tom se slučaju učitavaju maliciozne Web stranice kreirane od strane malicioznog korisnika.

4.4. Upravljanje sjednicama

Upravljanje sjednicama (engl. *session management*) dobro je poznat problem kod Web aplikacija. Budući da je HTTP bezkonekcijski protokol (engl. *conectionless*), problematiku upravljanja i praćenja sjednica potrebno je rješavati na razini samih aplikacija. U tu svrhu najčešće se koriste identifikatori sjednica (engl. *session ID*), jedinstveni nizovi putem kojih se prati stanje pojedinih sjednica. Načini na koji se ovi identifikatori razmjenjuju između klijenta i poslužitelja variraju, a najčešće metode podrazumijevaju Web kolačiće, skrivene forme, parametri GET zahtjeva i sl.
Nakon uspješne autentikacije, poslužitelj jednom od upravo navedenih metoda, klijentu prosljeđuje jedinstveni identifikator sjednice kojeg klijent za vrijeme cijelog trajanja sjednice koristi za pristup aplikaciji. Kao dio svakog HTTP upita, klijent aplikaciji prosljeđuje dobiveni identifikator na temelju kojeg aplikacija prati aktivnost korisnika.
Ukoliko je upravljanje sjednicama loše riješeno unutar Web aplikacije, *phiseri* to mogu vješto iskoristiti za dolazak do povjerljivih korisničkih informacija. Tako su na primjer poznate Web aplikacije koje su korisnicima omogućavale da sami definiraju inicijalnu vrijednost identifikatora sjednice prilikom prijavljivanja u sustav. Nakon inicijalne autentikacije korisnika, predefinirana se vrijednost identifikatora sjednice za vrijeme cijelog trajanja sjednice koristi za pristup sustavu.
U ovom slučaju tijek napada je sljedeći (Slika 4). Napadač korisniku prosljeđuje lažiranu poruku elektroničke pošte koja sadrži URL adresu s uključenim identifikatorom sjednice koja će se kasnije koristiti za pristup aplikaciji (korak 1). Budući da je predefinirana vrijednost identifikatora sjednice u ovom slučaju napadaču poznata, on može ostvariti pristup aplikaciji bez ikakvih ograničenja nakon što se korisnik prijavi u sustav. Najveći problem u ovom slučaju je upravo određivanje trenutka kada se korisnik prijavio u sustav pritiskom na vezu koja se nalazi u lažiranoj poruci elektroničke pošte. Ovaj problem neovlašteni korisnici najčešće rješavaju tako da kontinuirano pokušavaju pristupiti ciljnoj aplikaciji s identifikatorom sjednice koji je navedena u lažiranoj poruci. Za vrijeme dok korisnik nije prijavljen u sustav, napadačevi pokušaji biti će odbijeni, budući da aplikacija nema podatke o iniciranoj sjednici (korak 2). U trenutku kada se korisnik prijavi u sustav (korak 3), napadač bez ograničenja moći pristupiti aplikaciji korištenjem poznatog identifikatiora sjednice (korak 4).

Slika 4: Sigurnosni propust upravljanja sjednicama

Kako bi ovaj napad u potpunosti uspio potrebno je zadovoljiti nekoliko uvjeta. Prvo, ciljna Web aplikacija mora sadržavati propuste u načinu implementacije upravljanja sjednicama. Nakon toga klijenta je potrebno navesti da posjeti URL adresu ranjive Web aplikacije, te u zadnjem koraku naknadno predvidjeti trenutak kada će se klijent prijaviti u sustav. Tak nakon što su zadovoljeni svi

navedeni uvjeti, napadač može pristupiti sustavu pod ovlastima korisničkog računa koji je kompromitiran.

4.5. Napredne HTML funkcionalnosti

Budući da je socijalni inženjering jedan od temeljnih načela na kojima počivaju *phishing* napadi, *phiseri* svakodnevno razvijaju sve naprednije tehnike kojima će zavarati krajnje korisnike i navesti ih na postupke koji idu u prilog napadaču. Većina ovih tehnika bazira se na korištenju naprednih funkcionalnosti HTML jezika te brojnih drugih tehnologija vezanih uz razvoj Web stranica. Korištenjem specijalnih tehnika kreiraju se lažirane poruke elektroničke pošte koje svojim izgledom vrlo vjerno oponašaju stranice financijskih ustanova koje se žele kompromitirati. U nastavku su opisane neke od najčešćih tehnika koje se primjenjuju u ovu svrhu.

- **Web okviri (eng. *frames*)**

Web okviri posebno su zanimljivi sa stanovišta provođenja *phishing* napada, budući da napadačima otvaraju brojne mogućnosti prikazivanja malicioznih sadržaja unutar legitimnih Web stranica. Korištenjem specijalno kreiranih Web stranica, baziranih na okvirima, korisniku je moguće prikazati maliciozni Web sadržaj, a da on pritom ne primijeti da se radi o pokušaju napada.

U sljedećem primjeru koristi se tzv. skriveni okvir (engl. *hidden frame*) koji će se iskoristiti za učitavanje i prikrivanje malicioznog HTML koda.

Hidden_frame.html

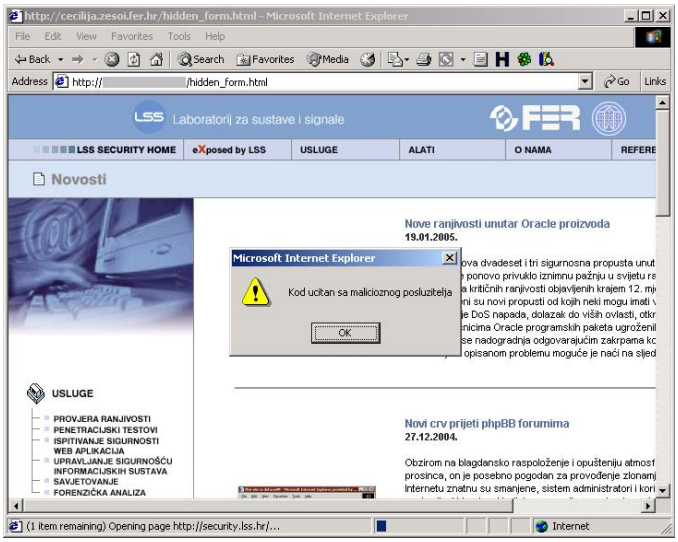
```
<html>
<FRAMESET ROWS="*,1" FRAMEBORDER="0" BORDER=0 BORDER="0">
    <FRAME SRC="http://www.cert.hr" NAME="main" SCROLLING=AUTO>
    <FRAME   SRC="http://malicious.lss.hr/frame.html"   NAME="hidden"
SCROLLING=NO >
</FRAMESET>
</html>
```

Navedena stranica rezultirati će učitavanjem sadržaja sa Web poslužitelja http://security.lss.hr unutar glavnog okvira (main), dok će se unutar skrivenog okvira učitati stranica `frame.html` sa poslužitelja http://malicious.lss.hr (sadržaj stranice `frame.html` korištene u sklopu ovog primjera prikazana je u nastavku).

frame.html

```
<html>
<script>alert("Kod ucitan sa malicioznog posluzitelja")</script>
</html>
```

Učitavanje stranice `hidden_frame.html` u ovom će slučaju rezultirati sljedećim prikazom.



Slika 5: Učitavanje malicioznog koda korištenjem okvira

Kao što je moguće primijetiti, osim glavne stranice učitan je (i izvršen) maliciozni kod sa adrese http://malicious.lss.hr. Iako je u ovom slučaju iskorišten jednostavni Java Script kod, stvarni primjeri napada mnogo su složeniji i koriste mnogo destruktivniji programski kod.
Ovakav tip napada neovlašteni korisnici mogu iskoristiti u različite svrhe:

- prikrivanje izvora s kojeg se učitava maliciozan kod. Adresu malicioznog poslužitelja u ovom je slučaju moguće vidjeti jedino pregledavanjem izvornog koda `hidden_form.html` datoteke. **Address** polje Web preglednika sadrži adresu HTML datoteke sa definiranim `frameset` elementima, iz čega nije moguće naslutiti da se radi o pokušaju napada.
- prikrivanje izvornog koda učitane Web stranice. U slučaju Web stranice koja koristi Web okvire, odabir opcije **View source** neće rezultirati prikazom izvornog koda stranica koje su učitane u Web preglednik. Kao što je ranije pokazano, izvorni kod `hidden_form.html` datoteke sadrži samo definiciju `frameset` elemenata sa vezama na odgovarajuće stranice koje će se učitati u pojedini okvir.
- umetanje malicioznog koda koji će se izvršavati u pozadini i prikupljati podatke o aktivnostima korisnika unutra glavnog prozora Web preglednika. Ovakva upotreba može se usporediti sa *spyware*, *adaware* i drugim sličnim malicioznim programima.
- koristeći napredna svojstva skriptnih jezika, koji se izvršavaju na strani klijenta (JavaScript, Visual Basic i sl.), moguće je skrivene okvire iskoristiti i za modifikaciju prikaza pojedinih polja Web preglednika (*Address* polje, *Status* polje s pripadajućim ikonama, *Toolbar* polja i sl.). Ove tehnike napadači mogu upotrijebiti u sklopu složenijih napada s ciljem zavaravanja iskusnijih korisnika.

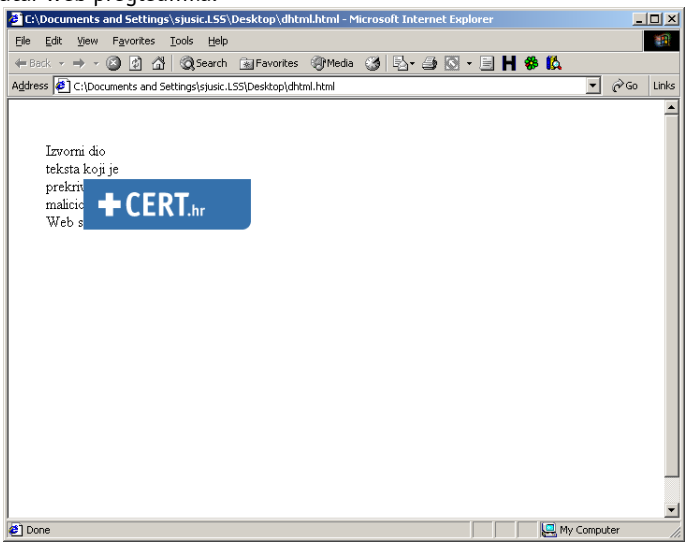
- **Prepisivanje sadržaja Web stranica**

Prepisivanje sadržaja Web stranica (eng. *page content overriding*) također je jedna od tehnika koju maliciozni korisnici vrlo često koriste za prikaz proizvoljnog Web sadržaja. U tu svrhu najčešće se koriste svojstva DIV direktive koja dolazi u sklopu Dynamic HTML jezika (DHTML). DIV direktiva Web programerima omogućuje grupiranje Web sadržaja u tzv. virtualne kontejnere, koje je kasnije moguće proizvoljno pozicionirati unutar prozora Web preglednika i na taj način prepisati postojeće sadržaje. Ukoliko vješto osmišljeni, ovakvi napadi mogu biti iznimno opasni i vrlo teški za otkrivanje.
Primjer korištenja DHTML DIV funkcije prikazan je u nastavku.

```
<html>
<DIV
STYLE="position:relative;left:30px;top:30px;height:100px;width:100px">
Izvorni dio teksta koji je prekriven malicioznim Web sadrzajem.
<IMG SRC="cert.gif" STYLE="position:absolute; left:40px; top:40px">
</DIV>
```

```
</html>
```

U navedenom primjeru dio teksta Web stranice (označen žutom bojom) djelomično je prekriven slikom pod nazivom cert.gif. Na sljedećoj slici moguće je vidjeti kako će navedena stranica izgledati nakon što je učitana unutar Web preglednika.



Slika 6: Prepisivanje sadržaja korištenjem DHTML DIV direktive

Iako je ovdje prikazan prilično jednostavan, i sam po sebi neupotrebljiv primjer korištenja DHTML DIV direktive, vrlo je lako uočiti mogućnosti primjene ove tehnologije i u maliciozne svrhe. Mogućnost proizvoljnog pozicionirana HTML sadržaja unutar Web stranica vrlo je moćno oružje neovlaštenih korisnika ukoliko se pažljivo upotrebi.

- **Zamjena grafičkih elemenata unutar Web stranice**

No, bez obzira na brojne tehnike koje neovlaštenim korisnicima omogućuju prikazivanje malicioznih Web sadržaja unutar Web preglednika korisnika, postoje i neki dodatni elementi na koje je potrebno utjecati ukoliko se napad želi učiniti potpuno realnim. Pritom se prvenstveno misli na elemente Web preglednika koji nisu vezani uz sam sadržaj Web stranice kao što su npr. *Address Bar* i *Status Bar* polja, zatim ikone kojima se označava kriptirana komunikacija (maleni lokot u donjem desnom kutu prozora) i sl. Za razliku od manje iskusnih korisnika, koje će u većini slučajeva zavarati neki od ranije opisanih trikova, iskusniji korisnici mogu prepoznati da se radi o malicioznim stranicama ukoliko se ne vodi računa o svim detaljima koji su vezani uz izgled aplikacije koja se kompromitira.
Kako bi riješili ovaj problem i povećali učinkovitost svojih napada, neovlašteni korisnici osmislili su specijalne metode koje omogućuju manipulaciju nekim od navedenih objekata. U tu svrhu najčešće se koriste svojstva skriptnih jezika kao što su Java Script, VBS Script i dr.

4.6. Prikupljanje podataka praćenjem aktivnosti korisnika

Pored korištenja dosad opisanih metoda, koje se prvenstveno baziraju na socijalnom inženjeringu, lažiranju Web stranica i preusmjeravanju korisnika na maliciozne poslužitelje, napadači sve češće koriste i neke alternativne, ponekad mnogo jednostavnije, ali i učinkovitije metode dolaska do povjerljivih informacija. Kao primjer se mogu navesti *key-logger* i *screen-capture* programi koji bilježe aktivnosti korisnika na osobnom računalu te ih prosljeđuju na adresu malicioznog korisnika.
Za razliku od ranije spomenutih tehnika, koje zahtijevaju mnogo truda i vremena kako bi se napad realizirao u potpunosti, ponekad je mnogo jednostavnije na osobno računalo korisnika postaviti maliciozni program koji će bilježiti povjerljive podatke i prosljeđivati na adresu malicioznog korisnika. Naravno, za provođenje ovakvog tipa napada potrebno je prethodno ostvariti pristup korisničkom računalu kako bi se omogućilo postavljanje malicioznog programa. U tu svrhu moguće je iskoristiti neki od sigurnosnih propusta unutar operacijskog sustava ili programa kojeg korisnik koristi, a u posljednje vrijeme iznimno su popularni i tzv. *spyware*, *adware* i drugi slični programi.

Danas je na Internetu moguće pronaći velik broj programa koji nude mogućnost bilježenja znakova unesenih putem tipkovnice ili hvatanje slike prikazane na zaslonu računala. Neki od tih alata potpuno su legalni i moguće ih je bez većih problema naći na Internetu, iako postoje i oni maliciozni koji su puno manje poznati i najčešće razvijeni za specifične namjene. U smislu zaštite od ovakvog tipa napada korisnicima se preporučuje redovita instalacija sigurnosnih zakrpi, te korištenje osobnih vatrozida i redovito ažuriranih antivirusnih programa.

4.7. Ranjivosti unutar Web preglednika

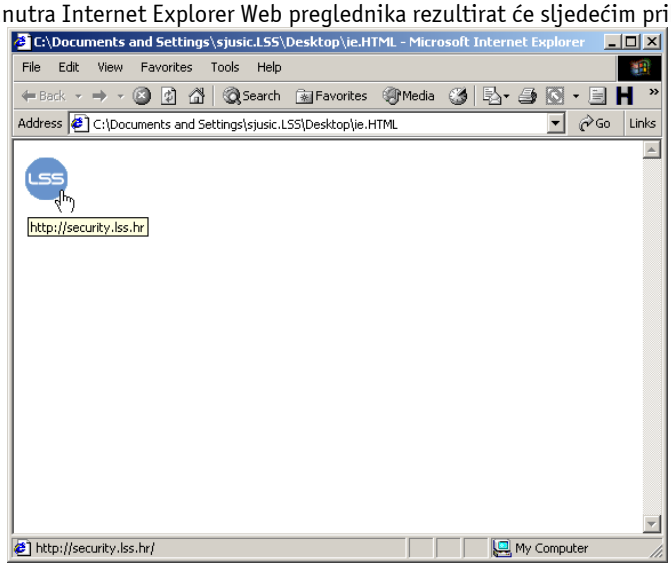
Kao što je već ranije spomenuto, socijalni inženjering igra vrlo važnu ulogu u procesu provođenja *phishing* napada. Budući da zavaravanje korisnika i njihovo navođenje na otkrivanje povjerljivih osobnih informacija predstavlja jedan od temelja za uspješno provođenje napada, napadači posebnu pažnju posvećuju načinu na koji kreiraju lažirane poruke elektroničke pošte. Poruke se nastoje učiniti što vjerodostojnijima i službenijima, kako bi se napad učinio što uvjerljivijim. Kako bi se umanjila mogućnost prepoznavanja maliciozne aktivnosti, vrlo često se koriste sigurnosni propusti i slabosti unutar popularnih programskih paketa za pristup Internetu (Web preglednici, klijenti za pregledavanje poruka elektroničke pošte i sl.),. Internet Explorer Web preglednik posebno je poznat po brojnim sigurnosnim propustima, iako se sigurnosni propusti sve češće otkrivaju i kod alternativnih Web preglednika kao što su Mozzila Fireworks, Opera i sl.
U nastavku će biti opisane neke od poznatijih ranjivosti koje je moguće iskoristiti u ovu svrhu kao i način njihove primjene. Složenost napada ovisi naravno i o iskustvu i vještini osobe koja provodi napad.

4.7.1. Microsoft Internet Explorer Embedded Image URI Obfuscation Weakness

U 5. mjesecu 2004. godine otkrivena je ranjivost unutar Microsoft Internet Explorer Web preglednika koja omogućuje prikrivanje stvarne URL adrese na koju je Web preglednik usmjeren. Propust je moguće iskoristiti korištenjem specijalno kreirane IMG HTML oznake smještena unutar HREF direktive. Primjer programskog koda koji iskorištava opisani sigurnosni propust prikazan je u nastavku:

```
<html>
<A HREF=http://security.lss.hr alt="http://security.lss.hr"> <IMG
SRC="lss.gif" USEMAP="#cert" border=0
alt="http://security.lss.hr"></A> <map NAME="cert"
alt="http://security.lss.hr"> <area SHAPE=RECT COORDS="224,21"
HREF="http://www.cert.hr"alt="http://security.lss.hr"> </MAP>
</html>
```

Učitavanje koda unutra Internet Explorer Web preglednika rezultirat će sljedećim prikazom.



Slika 7: Iskorištavanje sigurnosnog propusta unutar IE Web preglednika

Iako *Status Bar* polje i kursor miša prikazuju da veza pokazuje na adresu http://security.lss.hr, korisnik će pritiskom na gornju adresu biti preusmjeren na adresu http://www.cert.hr. Ovakve i brojne druge slične ranjivosti korisnik može iskoristiti za preusmjeravanje korisnika na maliciozne adrese, a da pritom vrlo vješto prikrije stvarnu URL adresu poslužitelja. Za provođenje ovog napada vrlo je važno korištenje MAP funkcije, koja će u ovom slučaju nadjačati HREF direktivu i prikazati proizvoljan tekst koji napadaču omogućuje provođenje napada.

4.7.2. Microsoft Internet Explorer URL Vulnerability

Internet Explorer URL ranjivost IE Web preglednika također je vrlo pogodna za provođenje *phishing* napada. Propust je vezan uz način na koji Internet Explorer Web preglednik procesira URL adrese koje u sebi sadrže korisničko ime i zaporku za pristup sustavu, tzv. *Friendly Login* URL adrese (npr. http://username:password@security.lss.hr).
Primijećeno je da ukoliko login dio URL adrese prije znaka @ sadrži znak %01, Web preglednik u *Address bar* polju neće prikazati niti jedan znak koji se nalazi iza umetnutog znaka %01. Npr.

```
http://www.banka.com%01@www.malicious.com
```

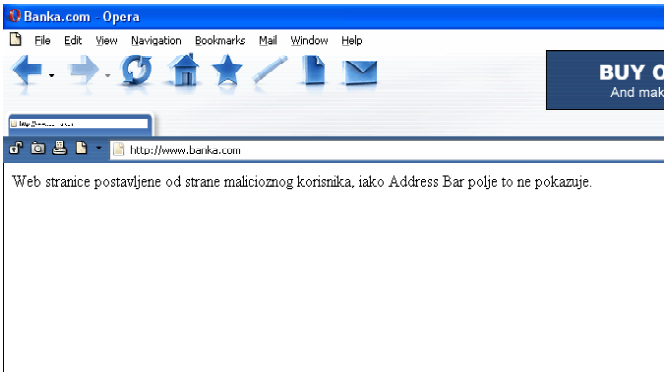
Prikazanu adresu ranjivi će Web preglednik prikazati bez dijela adrese koji se nalazi iza znaka %01, što neovlaštenom korisniku omogućuje prikrivanje stvarne adrese na koju je preglednik usmjeren. Kako je već ranije spomenuto, ova funkcionalnost je uklonjena kod novijih inačica IE Web preglednika.

4.7.3. Sigurnosni propusti Opera Web preglednika

Većina modernih Web preglednika implementira "*Shortcut Icon*" svojstvo, koje omogućuje prikaz odgovarajuće ikone unutar *Address Bar* polja. Iako i Opera Web preglednik podržava spomenuto svojstvo, primijećeno je da za razliku od ostalih Web preglednika, Opera podržava korištenje iznimno dugačkih ikona. Iako na prvi pogled nije očito kako bi se ovakva funkcionalnost mogla iskoristiti u maliciozne svrhe, neovlašteni korisnici su vrlo brzo uočili takvu mogućnost.
Opisano svojstvo moguće je iskoristiti tako da se kreira specijalno osmišljena ikona koja će osim sličice sadržavati i URL adresu koja se želi prikazati u Web pregledniku korisnika. Budući da se ikona pozicionira ispred URL adrese, ovim je putem moguće prikazati proizvoljnu adresu unutar *Address Bar* polja koja će zavarati krajnjeg korisnika.
U nastavku je prikazan primjer iskorištavanja upravo opisanog problema.

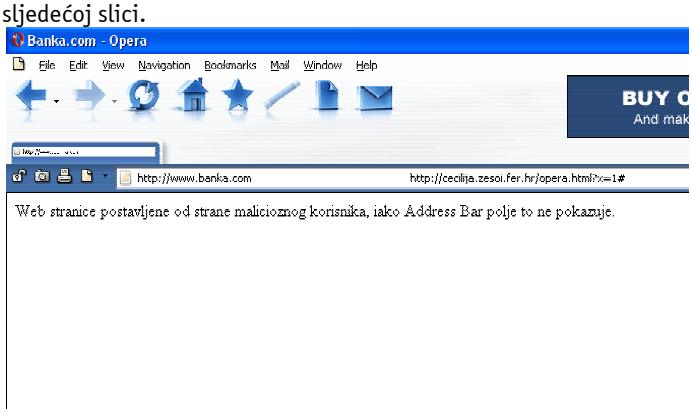
```
<html>
<head>
<title>Banka.com</title>
<link rel="shortcut icon" href="banka4.gif">
<script>
onload=function () {
        if (!location.search) {
                        location.href=location.href+"

&#8207;"
        } else if (window.name!="rDone") {
                        window.name="rDone";
                                        setTimeout(function () {
location.reload(true); },350);
        }
        }
        </script>
        </head>
        <body>
        Web stranice postavljene od strane malicioznog korisnika, iako
Address Bar polje to ne pokazuje.
        </body>
</html>
```

Učitavanje prikazanog koda u Opera Web preglednik rezultirati će sljedećim prikazom.



Slika 8: Lažiranje URL adrese unutra Opera Web preglednika

Adresa http://www.banka.com dio je ikone postavljene unutra *Address Bar* polja Web preglednika. Stvarna adresa na koju je klijent usmjeren moguće je vidjeti pomicanjem kursora unutar *Address* polja i prikazana je na sljedećoj slici.



Slika 9: Stvarna adresa na koju je klijent preusmjeren

Iz priloženog primjera moguće je uočiti da lažirana adresa djeluje vrlo uvjerljivo i da većina korisnika neće posumnjati da se radi o malicioznoj adresi.

5. Zaštita od phishing napada

Zaštitu od *phishing* napada potrebno je implementirati na više razina. Budući da se radi o napadu koji kombinira tehničke elemenata sa socijalnim inženjeringom, zaštitu je potrebno usmjeriti u oba smjera. Tehničke aspekte potrebno je riješiti odgovarajućim sigurnosnim kontrolama koje će onemogućiti provođenje napada (certifikati, sigurno programiranje, redovita instalacija sigurnosnih zakrpi i sl.), dok je probleme socijalnog inženjeringa moguće riješiti prvenstveno edukacijom i podizanjem svijesti krajnjih korisnika.

Slično kao i u ostalim sferama računalne sigurnosti kontrole je moguće podijeliti u detekcijske i preventivne. Detekcijske kontrole vezane su uz mogućnost pravovremenog otkrivanja i sprječavanja napada nakon što se isti pojavi, dok su preventivne kontrole vezane uz aktivnosti koje sprječavaju samu pojavu napada. Naravno, najbolji rezultati dobivaju se kombiniranjem oba pristupa.

5.1. Preventivne mjere

5.1.1. Zaštita na strani poslužitelja i aplikacija davatelja usluga

Implementacijom odgovarajućih *anti-phishing* sigurnosnih kontrola davatelji usluga mogu znatno podići razinu sigurnosti koju nude svojim korisnicima. Preventivni pristup rješavanju problema znatno će umanjiti mogućnost provođenja *phishing* napada, a korisnici će imati više povjerenja u usluge koje koriste.

- **Edukacija korisnika**

Budući da socijalni inženjering predstavlja temelj za provođenje *phishing* napada, jedan od najvažnijih koraka u njihovom sprječavanju je upravo edukacija korisnika. Korisnike je potrebo pravovremeno i redovito informirati o potencijalnim sigurnosnim problemima i načinima njihovog sprječavanja. Korisnike je potrebno jasno upoznati sa načinima komunikacije koje ustanova koristi i naglasiti da je bilo koji drugi oblik komunikacije nevažeći.
Neke od metoda koje mogu pomoći u podizanju svijesti i edukaciji korisnika su:

- Redovito obavještavanje korisnika o aktualnim promjenama i novostima unutar ustanove. Uvijek je moguće navesti i primjere neovlaštenih aktivnosti kako bi se korisnike upoznalo sa osnovnim tehnikama zavaravanja koje neovlašteni korisnici koriste.
- Omogućavanje prijave *phishinga* napada. Pravovremena detekcija *phishing* napada znatno će umanjiti broj njenih žrtava. Naravno, ustanova mora uložiti dovoljno sredstava u obradu takvih upozorenja i suradnju sa zakonodavnim tijelima kako bi se omogućilo istraživanje takvih slučajeva.
- Isticanje elemenata provjeravanjem kojih je moguće provjeriti legitimnost službenih Web stranica organizacije (HTTPS konekcija, ikona lokota, valjanost certifikata, provjera URL adrese i sl.).
- Kreiranje sigurnosnih politika i pravilnika vezanih uz poslovanje ustanove i odnosne s korisnicima. Kreiranjem i uvođenjem ovakvih dokumenata korisnicima se olakšava detekcija svih postupaka koji odstupaju od definiranih pravila.

- **Snažna autentikacija korisnika**

Svim bankama i drugim sličnim organizacijama preporučuje se korištenje snažnih mehanizama koji će onemogućiti provođenje *phishing* napada, čak ukoliko i napadač dođe do povjerljivih korisničkih informacija. U tom smislu preporučuje se korištenje token i smart card autentikacijskih mehanizama u kombinaciji sa PIN brojem ili zaporkom. Dvostruka autentikacija od korisnika zahtjeva da dva puta dokaže svoj identitet, čime se dodatno podiže razina sigurnosti. Osim poznavanja PIN broja koji je potreban za pristup sustavu, korisnik mora i fizički posjedovati sam token uređaj kako bi ostvario pristup. Dodatna prednost ovakvih uređaja je činjenica da koriste jednokratne zaporke čija je valjanost ograničena određenim vremenskim periodom.
Ovakav oblik autentikacije davatelju usluge, ali i krajnjem korisniku, daje veći osjećaj sigurnosti, što je vrlo važno kod kritičnih sustava koji procesiraju osjetljive informacije. Osnovni nedostatak ovakvih rješenja su nešto veći troškovi davatelja usluge po korisniku, veće potrebe za edukacijom i podrškom i sl.

- **Siguran razvoj Web aplikacija**

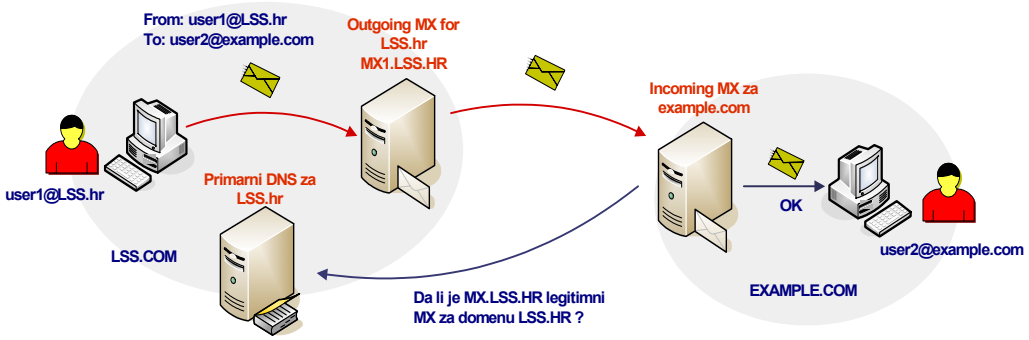
Siguran razvoj programskog koda jedan je od temeljnih uvjeta za uspostavu sigurnog i pouzdanog informacijskog sustava. Budući da su *phishing* napadi usmjereni prema ustanovama koje nude financijske usluge, ovaj je problem dodatno naglašen.
Osnovno pravilo koje vrijedi prilikom razvoja informacijskih sustava visoke razine sigurnosti je da se sigurnosni aspekti moraju uključiti u što ranijoj fazi projekta. Naknadno rješavanje sigurnosnih problema, nakon što je aplikacija već dovršena, najčešće će rezultirati velikim brojem pogrešaka i slabosti koje predstavljaju potencijalnu opasnost. Obzirom da je sigurnost Web aplikacija iznimno široko područje ovdje će biti navedene neke osnovne preporuke kojih bi se programeri trebali držati:

- restriktivno filtrirati korisnički unos,
- restriktivno filtrirati sve podatake koji se ispisuju na stranicu,
- koristiti snažne i provjerene kriptografske algoritame,
- koristiti provjerene sustave za upravljanje sjednicama,
- prilikom ispisivanja pogrešaka ne otkrivati podatke o radu aplikacije,
- provesti detaljno testiranje aplikacija prije uvođenja u produkcijsko okruženje,
- koristiti sigurne autentikacijske mehanizme i kontrolu pristupa.

- **Sigurnost mail poslužitelja**

Budući da se u sklopu provođenja *phishing* napada za zavaravanje korisnika najčešće koriste lažirane poruke elektroničke pošte, sigurnost mail poslužitelja također igra vrlo važnu ulogu u zaštiti od ovakvih napada. Obzirom da SMTP protokol, na kojem se bazira e-mail servis, ne podržava sigurnosne kontrole koje bi osigurale integritet, povjerljivost i autentičnost poruka elektroničke pošte, upravo je to jedan od osnovnih razloga zašto se e-mail servis najčešće koristi za provođenje malicioznih

aktivnosti. Dodatno, poruke elektroničke pošte vrlo je lako lažirati, što *spammeri* i *phiseri* vrlo često koriste kako bi zavarali korisnike i povećali učinkovitost svojih napada.
Kako bi se riješio problem lažiranja poruka elektroničke pošte dosad je predloženo nekoliko rješenja, no niti jedno od njih nije u potpunosti zaživjelo.
Jedno je od rješenja je ono od Microsofta pod nazivom Caller ID, odnosno Sender ID. Osnovna ideja ovog koncepta je da organizacije u svoje DNS poslužitelje, osim dolaznih MX poslužitelja zaduženih za primanje poruka elektroničke pošte, navedu i one odlazne, koji se koriste za slanje poruka elektroničke pošte. Primatelj poruke bi na temelju From: polja dolazne poruke mogao provjeriti da li je ista poslana sa legitimnog e-mail poslužitelja koji je registriran kao odlazni MX poslužitelj domene čije je ime navedeno u poruci. Na ovaj način bi za svaku poruku bilo moguće provjeriti da li zaista dolazi sa domene koja je navedena u samoj poruci. Opisani koncept prikazan je na sljedećoj slici (Slika 10).



Slika 10: Koncept zaštite od lažiranja email poruka

Detaljnije informacije o Sender ID konceptu moguće je pronaći na stranicama Microsfta (http://www.microsoft.com/mscorp/twc/privacy/spam/senderid/default.mspx) te u CARNet CERT dokumentu pod nazivom "Identifikacija pošiljatelja poruke elektroničke pošte" (http://www.cert.hr/filehandler.php?did=168). Sličan koncept predložen je i pod nazivom RMX (engl. *Remote Mail Exchanger*) zapisi (http://www.mikerubel.org/computers/rmx_records/).

- **Digitalno potpisivanje poruka elektroničke pošte**

Digitalnim potpisivanjem poruka moguće je znatno podići razinu sigurnosti e-mail sustava. Korištenjem asimetrične kriptografije i certifikata osigurava se autentičnost, integritet i povjerljivost poruke što je temeljni sigurnosni zahtjev kod modernih informacijskih sustava. Kao primjer standarda koji se može koristiti za digitalno potpisivanje poruka elektroničke pošte mogu se navesti S/MIME i PGP, odnosno OpenPGP. Važno je napomenuti da iako ova dva standarda korisnicima nude gotovo identične funkcionalnosti, postoje određene razlike koje ove dvije tehnologije čini međusobno nekompatibilnima. S/MIME originalno je zamišljen od strane tvrtke RSA Data Security. Zapis poruka baziran je na PKCS #7 formatu, dok se za certifikate koristi X.509v3 standard. Za razliku od S/MIME servisa, PGP koristi svoje vlastite formate što ova dva servisa čini međusobno nekompatibilnima.
Također, digitalno potpisivanje i provjeru poruka elektroničke pošte moguće je implementirati ili na razini klijenta elektroničke pošte ili na razini mail poslužitelja putem kojeg se poruke šalju ili primaju. Danas na tržištu postoji velik broj alata koji nude ove funkcionalnosti i tvrtke koje se bave financijskim poslovanjem svakako bi trebale ozbiljno razmotriti mogućnosti njihovog korištenja.

5.1.2. Zaštita na strani klijenta

Osim zaštite poslužitelja i aplikacija na strani davatelja usluga, potrebno je voditi računa i o zaštiti osobnih računala koje korisnici koriste za pristup Internetu. Sigurnosne propuste unutar operacijskih sustava i različitih programskih paketa što su MS Office, Internet Explorer i sl., neovlašteni korisnici vrlo često koriste za provođenje neovlaštenih aktivnosti. Ukoliko se ne vodi računa o sigurnosnim postavkama i redovitoj nadogradnji sustava, korisnici osobnih računala postaju vrlo lake mete za neovlaštene korisnike. Na Internetu je danas moguće pronaći velik broj malicioznih programa putem kojih je vrlo lako ostvariti pristup osobnom računalu ukoliko isto nije redovito održavano. Problem je postao dodatno naglašen pojavom tehnologija koje omogućuju stalnu vezu na Internet (*cable modem*,

xDSL i sl.) budući da su računala 24h dnevno izložena prijetnjama s Interneta. Slično vrijedi i za *phishing* napade koji vrlo često koriste sigurnosne propuste unutar programa kao što su Internet Explorer, MS Outlook, Opera, Mozzila Firefox i sl.
U nastavku će biti spomenute neke od mjera koje će podići razinu sigurnosti osobnih računala.

- **Antivirusna zaštita, antispam, osobni vatrozidi**

U prvu liniju obrane kada se govori o osobnim računalima zasigurno spadaju alati kao što su antivirusna zaštita i osobni vatrozidi, a sve češće se u tu kategoriju svrstavaju antispam i antispyware alati te sustavi za detekciju neovlaštenih aktivnosti (engl. *Intrusion detection Sysetm, IDS)*. Ispravno korištenje i redovito ažuriranje ovih alata temelj je za održavanje zadovoljavajuće razine sigurnosti na osobnim računalima.
Njihova upotreba u većini će slučajeva spriječiti pojavu malicioznih programa kao što su virusi, crvi, trojanski konji i sl., blokirati maliciozne konekcije s Interneta, detektirati pokušaje nelegitimnog pristupa sustavu te brojne druge slične maliciozne aktivnosti. Također, kombiniranjem navedenih alata automatski se postiže i razina zaštite sustava,.

- **Instalacija sigurnosnih zakrpi**

Slično kao i na razini poslužiteljskoj razini, redovita instalacija sigurnosnih zakrpi igra važnu ulogu kod održavanja klijentskih računala. Korištenje alata koji automatiziraju postupke dohvaćanja i instalacije sigurnosnih zakrpi sve je popularnije te se svakako preporučuje njihovo korištenje, pogotovo kod većih sustava sa velikim brojem klijentskih i poslužiteljskih računala.

- **Sigurnost klijenata elektroničke pošte**

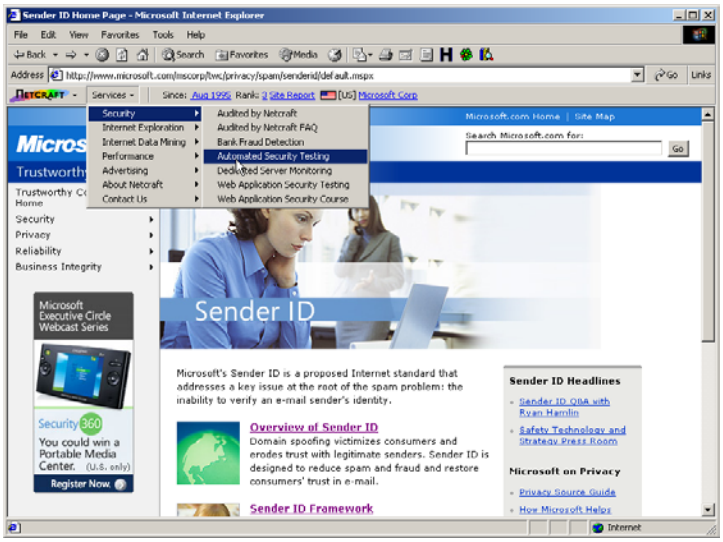
S obzirom na sve naprednije funkcionalnosti koje dolaze sa klijentima za pregledavanje elektroničke pošte, povećao se i broj mogućnosti koje napadači mogu iskoristiti za provođenje neovlaštenih aktivnosti. S ciljem podizanja sigurnosti klijenata za pregledavanje poruka elektroničke pošte preporučuje se onemogućavanje prikaza poruka u HTML formatu, izvršavanje skriptnih jezika kao što su VBS, Java Script i sl., blokiranje potencijalno malicioznih privitaka (engl. *attachment*), korištenje alata za detekciju SPAM poruka i sl. Onemogućavanjem HTML prikaza spriječiti će se većina *phishing* napada koji koriste maskiranje URL adresa.

- **Sigurnost Web preglednika**

Slično kao i kod klijenata za pregledavanje poruka elektroničke pošte, uvođenje naprednih funkcionalnosti i kod Web preglednika donose nove sigurnosne propuste koje neovlašteni korisnici mogu iskoristiti za provođenje malicioznih aktivnosti. S ciljem podizanja razine sigurnosti osobnog računala i prevencije *phishing* napada preporučuju se sljedeći koraci:

- onemogućavanje pop-up funkcionalnosti,
- onemogućavanje podrške za Java aplikacije,
- onemogućavanje ActiveX podrške,
- zabrana automatskog izvršavanja svih datoteka dohvaćenih sa Interneta,
- minimalna podrška za multimedijalne formate,
- redovita instalacija sigurnosnih zakrpi,
- korištenje alternativnih Web preglednika (Opera, Mozzila i sl.).

Dok će neke od navedenih postavki možda biti prestroge za kućne korisnike, u poslovnim okruženjima one bi trebale biti standard kojeg će se pridržavati svi korisnici.
Obzirom na iznimno velik broj sigurnosnih problema koji su se u posljednje vrijeme pojavili unutra IE Web preglednika, sve veći broj korisnika prelazi na alternativna rješenja kao što su Mozzila Firefox, Opera i sl. Analize pokazuju da je IE Web preglednik trenutno najsofisticiraniji Web preglednik na Internetu, iako većina korisnika koristi svega 5% njegovih funkcionalnosti. Problem je dodatno naglašen činjenicom da su komponente IE Web preglednika integrirane u sam operacijski sustav, što znači da iskorištavanje sigurnosnih propusta automatski može omogućiti potpuno preuzimanje kontrole nad sustavom.
U smislu zaštite od *phishing* napada sve su popularniji i specijalni dodaci za Web preglednike koji uključuju specijalne sigurnosne kontrole namijenjene detekciji i sprječavanju *phishing* napada. U većini implementacija ovi alati provjeravaju da li je određena adresa poznata kao izvor *phishing* napada. Jedan od takvih alata je i Netcraft Toolbar koji je moguće dohvatiti sa sljedeće adrese http://toolbar.netcraft.com/install. Alat se nakon uspješne instalacije integrira unutar Web preglednika, nakon čega je moguće koristiti njegove funkcionalnosti (Slika 11).



Slika 11: Netcraft toolbar

Ugrađeni dodatak korisniku omogućuje jednostavan i brz dolazak do brojnih informacija o Web stranicama koje posjećuje, na temelju čega je moguće kvalitetnije prosuditi o njihovom integritetu i legitimnosti. Detaljnije informacije o načinu rada Netcraft Toolbar dodatka moguće je pronaći na Web stranicama proizvođača (http://news.netcraft.com/).

- **Opreznost korisnika**

U većini slučajeva korisnici svojom opreznošću i promišljenim postupcima mogu umanjiti mogućnost da postanu žrtve *phishing* napada. U nastavku su navedene neke od preporuka na temelju korisnik može prepoznati *phishing* napad ili neku drugu sličnu malicioznu aktivnost:

- Na sve službene obavijesti koje korisnika putem elektroničke pošte obavještavaju o osjetljivim pitanjima kao što je zatvaranje računa, potreba za promjenom korisničkih podataka i sl., preporučuje se reagirati telefonski ili usmeno. Nikako ne odgovarati na primljenu poruku ili koristiti adrese navedene u tijelu poruke.
- Sve službene poruke financijskih ustanova trebale bi biti digitalno potpisane. Ukoliko to nije slučaj, preporučuju se dodatne mjere opreznosti.
- Strogo izbjegavati odavanje povjerljivih financijskih informacija putem poruka elektroničke pošte. SMTP protokol podatke mrežom šalje u čistom tekstualnom obliku što ga čini ranjivim na napade praćenjem mrežnog prometa (engl. *sniffing*).
- Ukoliko se povjerljive informacije unose putem Web sučelja, preporučuje se poseban oprez i dodatne provjere kojima će se utvrditi legitimnost i integritet poslužitelja. Potrebno je provjeriti da li se koristi kriptirana komunikacija (https:// oznaka u *Address Bar* polju ili mali lokot u donjem desnom kutu Web preglednika).
- Detaljno analizirati SSL certifikat ponuđen od strane davatelja usluge. Provjeriti da li je certifikat valjan i da li je izdan od odgovarajuće ustanove. Informacije o certifikatu moguće je dobiti u bilo kojem trenutku dvostrukim klikom miša na ikonu u obliku lokota u donjem dijelu prozora.
- Ukoliko se na Web stranicama organizacije primijete "čudne" promjene u odnosu na ranije poznati izgled, preporučuje se dodatni oprez. *Phiseri* vrlo često prilikom lažiranja stranica naprave sitne pogreške, kojima se lažirane stranice mogu razlikovati od originalnih.

5.2. Detekcijske kontrole

Vrlo važan aspekt zaštite od *phishing* napada zasigurno je i njihova pravovremena detekcija, na temelju koje je moguće poduzeti odgovarajuće sigurnosne mjere koje će minimizirati posljedice napada. Nakon detektiranog napada organizacije mogu svojim korisnicima poslati obavijest koja će ih

upozoriti na potencijalnu opasnost, a moguće su i puno strože mjere kao što je privremeno onemogućavanje usluge za sve korisnike sustava.

5.2.1. Registracija domena sličnog imena

U svrhu detekcije *phishing* napada financijske ustanove bi trebale redovito pratiti registraciju domena čije je ime slično imenu domene organizacije. U sklopu provođenja *phishing* napada, napadači vrlo često registriraju imena domene koja su slična imenima domene organizacije koja se želi iskoristiti za *phishing* napad. Npr., ukoliko se Web stranice organizacije nalaze na adresi http://www.gradskabanka.com, poželjno je pratiti registraciju svih domena čiji je naziv u određenoj mjeri sličan ovome. Npr.

- dodavanje crtice: gradska-banka.com,
- korištenje domena: drugih država: gradskabanka.ch,
- izbacivanje znakova: gradska-bank.com,
- slična imena: grad-banka.com
- itd...

Iako uvijek postoji mogućnost da se radi o legitimnoj domeni, ovakve registracije domena svakako je poželjno imati pod kontrolom.
Na sličan način potrebno je voditi računa i o isteku registriranih domena kako bi se pravovremeno produžila njihova valjanost. Danas na Internetu postoje organizacije koje vode računa o isteku registracije domena i nude ih drugim korisnicima koji su zainteresirani za njihovu kupnju. Organizacije koje imaju registrirano nekoliko različitih domena posebno trebaju voditi računa o ovome problemu, budući da se nepažnjom neko od tih imena može zaboraviti.

5.2.2. Korištenje antispam servisa i alata

Postoje komercijalni alati i servisi koji omogućuju prepoznavanje poruka elektroničke pošte koje u sebi sadrže karakteristike *phishing* napada. Korištenjem ovakvih alata moguće je prepoznati pokušaje napada te prijaviti problem odgovornim osobama organizacije uz koju je napad vezan. Na temelju detektiranih poruka također je moguće kreirati odgovarajuće potpise koji će se distribuirati ostalim proizvođačima antispam alata u svrhu detekcije novih pokušaja napada.

5.2.3. Prijave od strane korisnika

Detekciju *phishing* napada moguće je učiniti učinkovitijom ukoliko se korisnicima omogući jednostavan i brz mehanizam za prijavu uočenih incidenata. Na temelju poruke elektroničke pošte za koju korisnik smatra da je vezana uz provođenje *phishing* napada, moguće je obavijestiti odgovorne osobe ukoliko za to postoji odgovarajući mehanizam. U ovom slučaju odgovornost je na strani banaka i ostalih sličnih ustanova da korisnike obavijeste o mogućnostima prijave napada i načinima na koje je to moguće provesti.

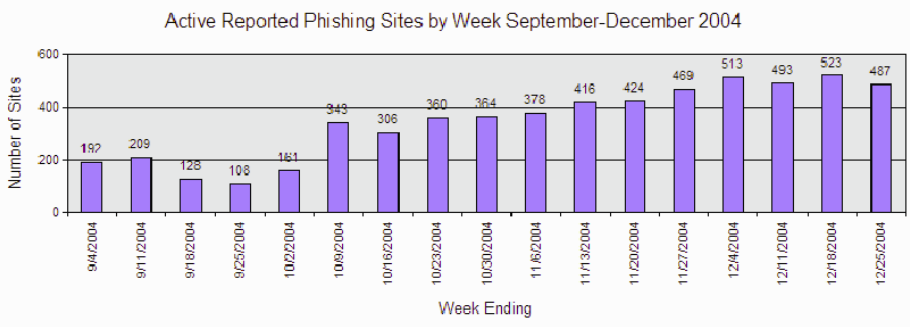
6. Statistički podaci

Kako bi se čitateljima ukazalo na ozbiljnost *phishing* napada, u ovom će poglavlju biti prikazani neki općeniti statistički podaci vezani uz ovaj tip neovlaštenih aktivnosti. Podaci su preuzeti sa Web stranica Anti-Phishing working Group grupe (http://www.antiphishing.org), čije su aktivnosti vezane isključivo uz *phishing* napade. Izneseni podaci vrijede za 12. mjesec 2004. godine.
Općenite informacije:

Broj aktivnih *phishing* Web stranica u 12. mjesecu	1707
Prosječni mjesečni porast u broju *phishing* napada između 7. i 12. mjeseca 2004. godine	24%
Broj ustanova koje su bile pogođene *phishing* napadima	55
Država u kojoj je postavljeno najviše lažiranih *phishing* Web stranica	United States
Broj lažiranih URL adresa koje u sebi sadrže ime organizacije koja se želi iskoristiti za napad	24%

Broj *phishing* poslužitelja bez registriranog imena (samo IP adresa)	63%
Broj *phishing* poslužitelja koji ne koriste TCP port 80	13.1%
Prosječni vijek trajanja *phishing* poslužitelja	5,9 dana
Najduži vijek trajanja *phishing* poslužitelja	30 dana

Iz priloženih podataka jasno se može zaključiti da se radi o alarmantnom broju *phishing* napada, a dodatno zabrinjava da je ovaj broj u konstantnom porastu. Prosječni porast *phishing* napada između 7. i 12. mjeseca 2004. godine je 24%, a treba uzeti da su u tim brojkama uzeti u obzir samo prijavljeni napadi. Također je zabrinjavajući podatak da su neki od malicioznih poslužitelja bili aktivni skoro mjesec dana, što je iznimno dugačak period.
Grafički prikaz na sljedećoj slici (Slika 12) prikazuje broj *phishing* poslužitelja u 12. mjesecu 2004. godine po tjednima.

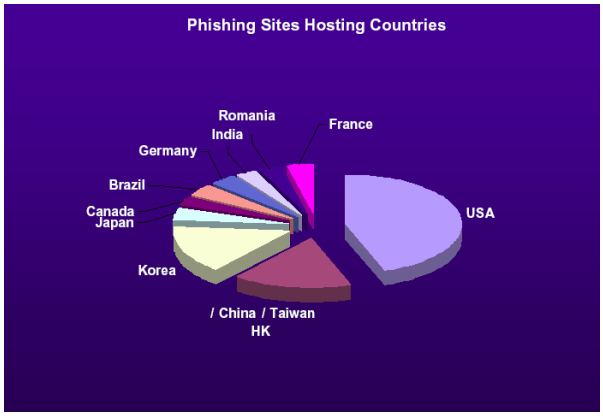


Slika 12: Broj *phishing* napada po tjednima u 12. mjesecu 2004. godine.

Podaci također pokazuju da 13% poslužitelja ne koristi TCP portove 80 i 443 za pokretanje Web poslužitelja. U ovu skupinu najvećim dijelom spadaju kompromitirana osobna računala na kojima su podignuti maliciozni Web poslužitelji na neuobičajenim portovima, kako bi se izbjegla detekcija od strane korisnika sustava. Sljedeća tablica prikazuje najčešće korištene TCP portove za uspostavu malicioznih *phishing* Web poslužitelja.

TCP port	Postotak
80/TCP	86%
87/TCP	3,6%
85/TCP	1,88%
5180/TCP	1,5%
2333/TCP	1%

Broj prijavljenih *phishing* poruka elektroničke pošte također je u porastu u odnosu na ranije mjesece (ukupno 9,019 prijavljenih poruka), iako ovaj porast iznosi svega 6% u odnosu na mjesec studeni. Prosječni porast *phishing* poruka u odnosu na 7. mjesec, što je puno mjerodavniji podatak, iznosi puno većih 38%.
Najveći broj malicioznih Web poslužitelja zasada je identificiran u Sjedinjenim Američkim Državama (oko 32%), iza koje slijede prvenstveno Azijske zemlje; Kina (12%), Koreja (11.8), Japan (2.8).



Slika 13: Lokacije malicioznih *phishing* poslužitelja

7. Zaključak

Phishing napadi nova su prijetnja korisnicima Interneta. Kombiniranjem tehnika socijalnog inženjeringa te lažiranja Web stranica i poruka elektroničke pošte neovlašteni korisnici pokušavaju doći do povjerljivih korisničkih informacija koje će im omogućiti ostvarivanje financijske koristi. Kako je detaljno objašnjeno u dokumentu, tehnike koje neovlašteni korisnici koriste u ovu svrhu vrlo su složene što rezultira iznimno velikim brojem žrtava *phishing* napada. Iako u Hrvatskoj još nisu zabilježeni pokušaji *phishing* napada, korisnike se ovim putem želi upozoriti na njihove osnovne karakteristike i načine provođenja te mogućnosti zaštite.

8. Reference

[1] Anti-Phishing Workgroup (APWG), http://www.antiphishing.org
[2] The Phishing Guide, Next Generation Security Software
[3] APWG, Proposed Solution to Address the threat of email spoofing scams