CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Limbo malware

CCERT-PUBDOC-2008-11-247

+CERT.hr u suradnji s LSS

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

Rezultat toga rada je i ovaj 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

Zloćudni softver, baš kao i sve druge tehnologije, svakim danom razvija se sve brže. Nastaju nove vrste zloćudnih programa koje je sve teže otkriti i ukloniti. Oni ne samo da su sve brojniji, već raste i njihova složenost.

Posebna opasnost vreba od jedne relativno nove vrste zloćudnih programa – bankarskih trojanskih konja. Riječ je o zloćudnim programima koji su specijalizirani za napade na bankarske institucije i njihove korisnike. Oni ne napadaju veliki broj žrtava, a koriste najnovije tehnike za izbjegavanje detekcije antivirusnim alatima. Predstavnik ove kategorije zloćudnog softvera je trojanski konj „Limbo“. Radi se o jednom od najprofinjenijih zloćudnih programa današnjice. Iako se podaci o njemu teško nalaze i izvori informacija su poprilično mutni, činjenica je da je riječ o opasnom programu koji može prouzročiti milijunske štete svojim žrtvama.

U ovom dokumentu obrađena je ova nova kategorija zloćudnog softvera – bankarski trojanski konji, te Limbo kao njezin glavni predstavnik.

2. Razvoj zloćudnih programa

Za pojam zloćudni program (eng. *malware*), prema organizaciji NIST (eng. *National Institute of Standards & Technology*), vrijedi slijedeća definicija:

> *"Pojam malware se odnosi na program koji je, najčešće tajno, ubačen u sustav sa namjerom kompromitiranja povjerljivosti, integriteta ili dostupnosti žrtvinih podataka, aplikacija ili operacijskog sustava, ili na neki drugi način pokušava ometati žrtvu."*

Općenito se pojam zloćudni program odnosi na sve aplikacije čija je svrha, po prirodi, zloćudna. Postoji puno različitih vrsta zloćudnih programa. Neki od njih su virusi, crvi, logičke bombe, špijunski programi te trojanski konji. Vrste zloćudnih programa detaljnije su opisane u idućem poglavlju.

2.1. Vrste zloćudnih programa

2.1.1. Virusi

Virusi su najpoznatija vrsta zloćudnih programa i upravo zbog toga nestručnjaci i druge vrste zloćudnih programa najčešće poistovjećuju s virusima, iako je to pogrešno. Riječ je o zloćudnim programima koji za svoju egzistenciju i širenje koriste druge programe i datoteke. Oni se šire kopiranjem svojeg vlastitog koda u drugi program koji se tada naziva program "domaćin" (eng. host). Sam proces kopiranja koda naziva se „infekcija“.

Današnji virusi najčešće posjeduju mogućnost izmjene svog oblika te se takvi virusi nazivaju metamorfni. Time izbjegavaju mogućnost detekcije antivirusnim alatima koji koriste uzorke virusa (eng. *virus signature*) kako bi ih prepoznali. Virusi koji su u opticaju tj. neželjeno se šire računalnim sustavima nazivaju se "virusima u bijegu" (eng. "*in the wild*"), dok se virusi čuvani u laboratorijskim uvjetima nazivaju "zoo virusi". Viruse čuvane u laboratorijskim uvjetima koriste stručnjaci iz antivirusne industrije za razvoj tehnika obrane od ovih zloćudnih programa.

2.1.2. Crvi

Crvi (eng. *worms*) su samo-replicirajući zloćudni programi koji se šire putem računalnih mreža. Oni su, za razliku od virusa, najčešće zasebni programi te ne koriste druge programe kao svoje domaćine. Za svoje širenje obično koriste sigurnosne propuste u mrežnim aplikacijama i protokolima, i to bez znanja i interakcije korisnika sustava. Teret (eng. *payload*) koji nose može imati razne učinke, no njihova glavna karakteristika je da zagušuju mrežu i smanjuju propusnost, za razliku od virusa koji narušavaju integritet datoteka koje inficiraju.

Jedna od najpoznatijih podvrsta su tzv. *Mass-mailer* crvi, koji se šire putem poruka elektroničke pošte koje u privitku sadrže zloćudni program. Obično se za širenje koriste adrese pohranjene u *e-mail* klijentima na zaraženim računalima.

2.1.3. Logičke bombe

Logičke bombe su vrsta zloćudnih programa koji se ubacuju u inače legitiman softver i izvršavaju samo pod određenim uvjetima tj. kada se ispuni neka "logika" (npr. na određeni datum) koju je autor odredio. Vrijeme ili neki događaj (eng. *event*) obično se koriste kao okidači za ovu posebnu vrstu zloćudnih programa.

Kada su uvjeti zadovoljeni, izvršava se određeni skup instrukcija koje predstavljaju stvarni sadržaj zloćudnog programa. Važno je napomenuti da ovaj sadržaj nije u svim slučajevima zloćudan. Tu se može raditi i o brisanju komercijalnih programa nakon isteka probnog perioda. No, u kontekstu

zloćudnih programa, oni se češće koriste u kriminalne svrhe. Primjer takve uporabe je ubacivanje logičke bombe u softver kao znak osvete nezadovoljnih ili otpuštenih zaposlenika.

2.1.4. Backdoor programi

Backdoor programi su alati koje zlonamjerni napadači koriste kako bi dobili tajni pristup udaljenom računalu. Oni obično dolaze u paketu s nekim drugim zloćudnim programom (trojancem, virusom…) i omogućavaju napadaču slanje daljnjih naredbi zaraženim računalima. Oni su ponekad posljedica pogrešaka u dizajnu programa i protokola koje omogućavaju napadačima neželjeni pristup. Primjer takve vrste backdoor programa je rana primjena SMTP (eng. *Simple Mail Transfer Protocol*) protokola koja je omogućavala udaljeno izvršavanje naredbi.

2.1.5. Trojanski konji

Trojanski konji jedni su od najjednostavnijih, no u posljednje vrijeme vrlo raširenih, oblika zloćudnih programa. Ti programi sadrže neku korisnu funkcionalnost te time privlače korisnika da ih pokrene i time omogući izvršavanje i zloćudnog tereta. Postoje dvije vrste trojanskih konja: oni koji su u potpunosti izradili zlonamjerni napadači, te postojeći korisni programi koje su napadači izmijenili.

Posebno opasna vrsta trojanskih konja, koje danas najviše koriste zlonamjerni napadači, su bankarski trojanski konji. Njihov osnovni cilj je krađa osobnih podataka žrtve, poput brojeva kreditnih kartica i PIN-ova, koji napadaču omogućuju stjecanje izravne financijske koristi. U ovu kategoriju zloćudnih programa spada i Limbo, koji je detaljnije opisan u nastavku ovog dokumenta.

2.1.6. Špijunski programi

Osnovna svrha špijunskih programa (eng. *spyware*) je nadgledanje aktivnosti korisnika računala, te često krađa osjetljivih informacija. Korisnikove aktivnosti obično se nadgledaju kako bi se utvrdile njegove navike i potrošački profil. Te informacije ponekad se koriste za ciljano reklamiranje, no često je cilj njihove uporabe krađa identiteta korisnika.

2.1.7. Rootkit programi

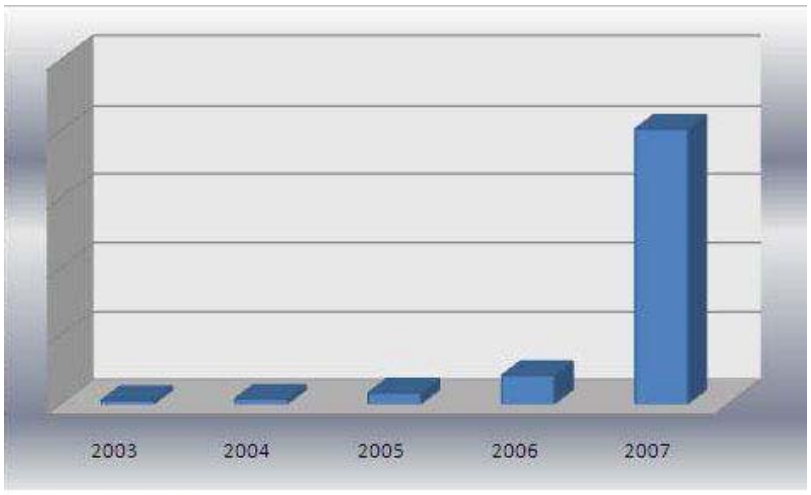
Rootkit programi koriste se za mijenjanje osnovnih funkcionalnosti operacijskog sustava u svrhu sakrivanja drugih zloćudnih aktivnosti. Naziv *rootkit* su dobili po tome što napadač, koji ih koristi, ima tzv. "*root*" , odnosno najveće (administratorske) ovlasti na sustavu. Posebno su opasni upravo zato jer ih je jako teško otkriti.

2.1.8. Bot/Botnet programi

Bot program je aplikacija koja izvršava sve naredbe koje primi od tzv. "*master*" aplikacije. Mreža računala na koje su instalirani *Bot* programi čini *Botnet* mrežu. Ovi programi obično se koriste za izvođenje distribuiranih DoS (eng. *Denial of Service*) napada, no, obzirom da se radi o potpuno autonomnim programima, mogu se koristiti i za niz drugih zlonamjernih aktivnosti u ovisnosti o naredbama koje im se šalju. Komunikacija između *Bot* programa i "*master*" aplikacije najčešće se odvija putem IRC (eng. *Internet Relay Chat*) kanala.

2.2. Statistike

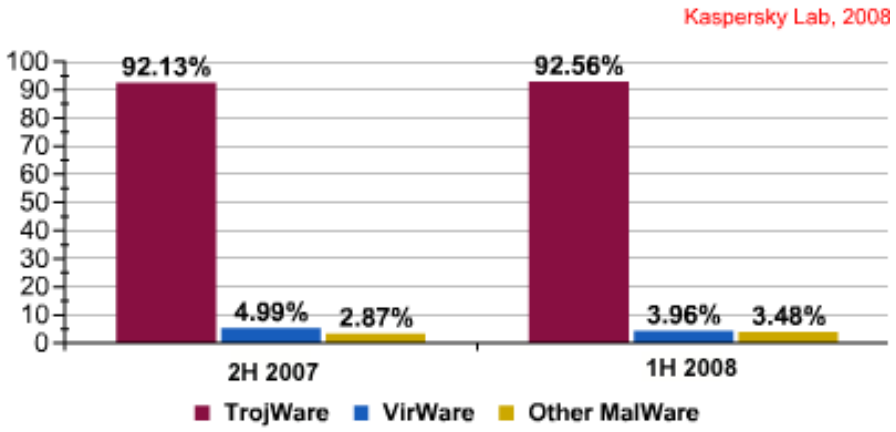
Broj zloćudnih programa već godinama raste gotovo eksponencijalnom brzinom. Zabrinjavajući faktor je taj što osim njihovog broja, gotovo istom brzinom raste i njihova složenost. Razloge ovoga trenda treba prvenstveno tražiti u sve profinjenijim metodama kojima se autori zloćudnih programa koriste u njihovoj izradi, kao i u brojnim mutacijama već odavno poznatih primjeraka. Slika 2.1 prikazuje ovaj trend kroz prikaz odnosa broja novih zloćudnih programa u posljednjih pet godina.



Slika 2.1. Porast broja zloćudnih programa kroz godine

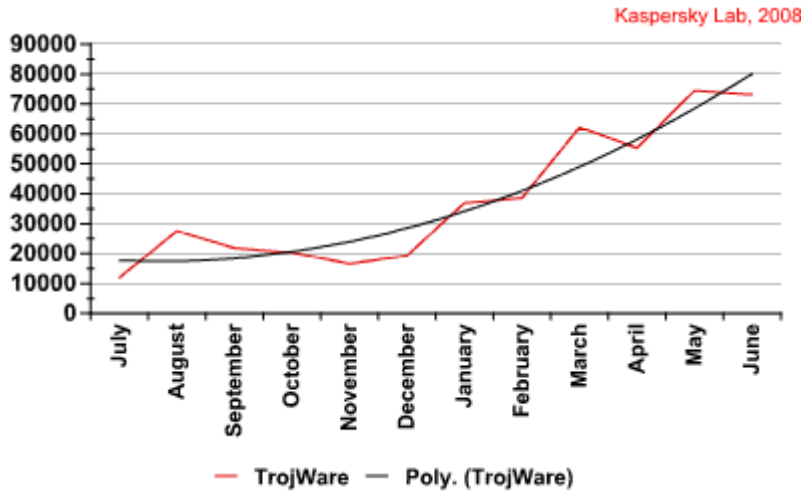
Sukladno porastu broja zloćudnih programa, antivirusna industrija sve teže se nosi sa brojnim inačicama koje svakodnevno obrađuju. Stručnjaci iz tvrtke Avert Labs tako su objavili da su tijekom 2007. godine zaprimali dnevno u prosjeku 372 nove vrste zloćudnih programa što ukupno daje 135,885 novih inačica zloćudnog softvera godišnje. To čini 38% svih zloćudnih programa koje su otkrili stručnjaci iz ove tvrtke[1].

Što se tiče zastupljenosti pojedinih vrsta zloćudnih programa u njihovom ukupnom broju, na slici 2.2 može se vidjeti da trojanski konji s preko 90% zastupljenosti u posljednja dva polugodišta prevladavaju sektorom zloćudnog softvera.



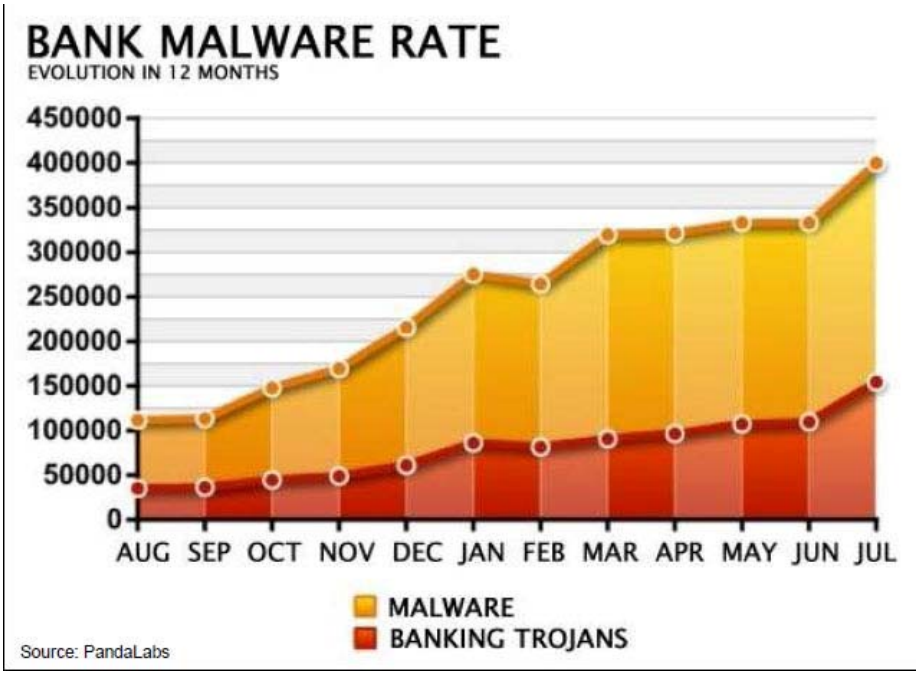
Slika 2.2. Zastupljenost pojedinih vrsta zloćudnog softvera

Na slici 2.3 može se, u konkretnim brojkama, vidjeti izniman porast broja novih inačica trojanskih konja od gotovo 900% u samo 12 mjeseci.



Slika 2.3. Porast broja novih inačica trojanskih konja

Razlog ovom trendu povećanja broja različitih inačica trojanskih konja može se pronaći u pojavi relativno nove podvrste – bankarskih trojanaca. Riječ je o vrsti trojanaca koji postoje odavno, no njihov razvoj i napredak, pa time i povećan intenzitet pojavljivanja, posebno je uočljiv u posljednjih 12 mjeseci. Riječ je o specijaliziranima programima koji napadaju razne financijske institucije i njihove korisnike. Limbo trojanac ubraja se upravo u ovu vrstu zloćudnog softvera. Njihov udio u ukupnom broju zloćudnih programa u posljednjih 12. mjeseci, prema podacima tvrtke Panda Security, može se vidjeti na slici 2.4.

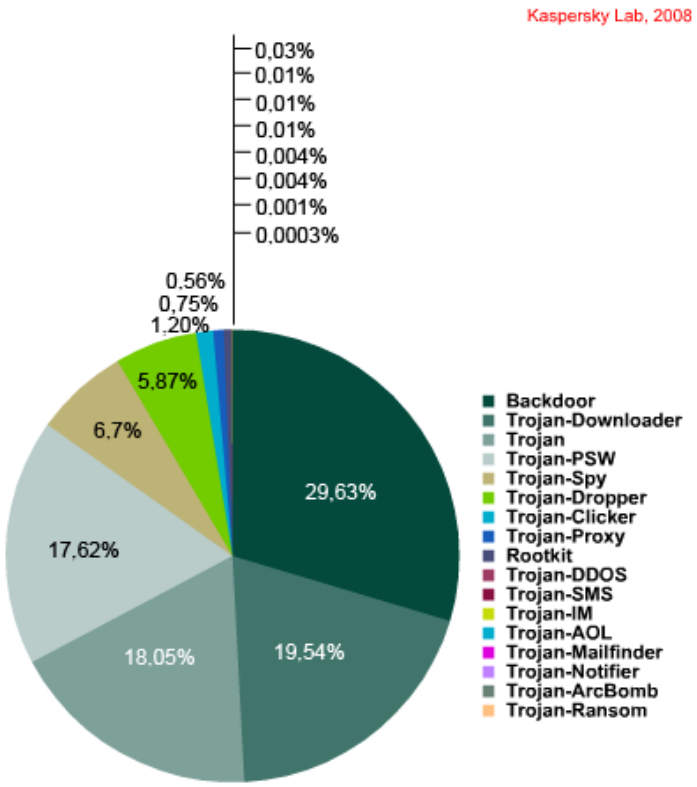


Slika 2.4. Udio bankarskih trojanaca

Opasnost koja vreba od ove nove vrste zloćudnog softvera može se naslutiti i prema podatku koji je objavila analitička tvrtka Gartner. Naime, prema njihovom istraživanju, 3.6 milijuna državljana Sjedinjenih Američkih Država je u 2007. godini bilo žrtva financijske prijevare[2].

2.3. Trojanski konji

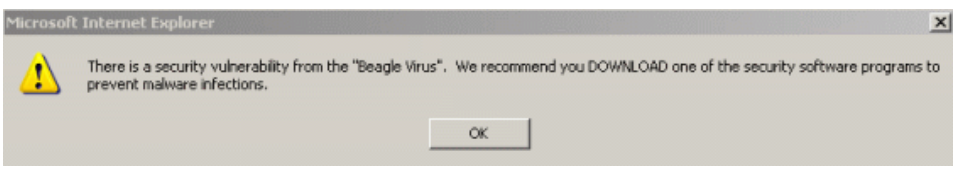
Kao što je prikazano u prethodnom poglavlju, trojanski konji danas su najraširenija vrsta zloćudnih programa. Oni, u pravilu, uvijek nanose štetu zaraženim korisnicima. Kroz povijest se pojavljivalo nekoliko značajnijih trojanskih konja koji su detaljnije opisani u ovom poglavlju. Prema svojoj namjeni i ponašanju, trojanci se mogu podijeliti u više klasa. Na slici 2.5 prikazane su pojedine klase trojanaca s odgovarajućim udjelima u ukupnom broju trojanaca, prema aktualnim podacima tvrtke Kaspersky. Trojanci su podijeljeni u klase prema svojem ponašanju. Prema ovim podacima najrasprostranjeniji trojanski konji su oni koji imaju *backdoor* funkciju. Računala koja su zaražena ovom podvrstom trojanskih konja najčešće se koriste u *Botnet* mrežama, pa je logična njihova visoka zastupljenost.



Slika 2.5. Klase trojanaca sa udjelima ukupnom broju

2.3.1. Vundo

Trojanski konj Vundo (također poznat i kao VirtuoMondo i MS Juan) poznat je po tome što uzrokuje iskakanje reklamnih prozora i degradaciju performansi kod korištenja određenih web stranica. Obično reklamira lažne antispyware proizvode čijom se instalacijom korisnik može zaraziti još ponekim zloćudnim programom. Ovaj trojanac nastanjuje se na sustav koristeći propust programskog paketa Sun Java inačice 1.5.0_7. Na sustavu se pojavljuje kao BHO (eng. *Browser Helper Object*) objekt, odnosno dodatak za Internet Explorer, te u obliku DLL (eng. Dynamic Link Library) datoteka dodanih procesima WinLogon.exe i Explorer.exe.



Slika 2.6. Primjer poruke Vundo trojanca

Vundo napada web preglednik Internet Explorer i starije inačice preglednika Mozilla Firefox i Opera. Iznimno ga je teško ukloniti jer onemogućava rad nekih osnovnih Windows aplikacija kao što su Task Manager i Registry Editor. Većina antivirusnih rješenja nema mogućnost njegovog automatskog uklanjanja pa se zato preporuča slijediti upute za ručno uklanjanje (koje se mogu pronaći na web adresi http://www.vundo.org).

2.3.2. Haxdoor

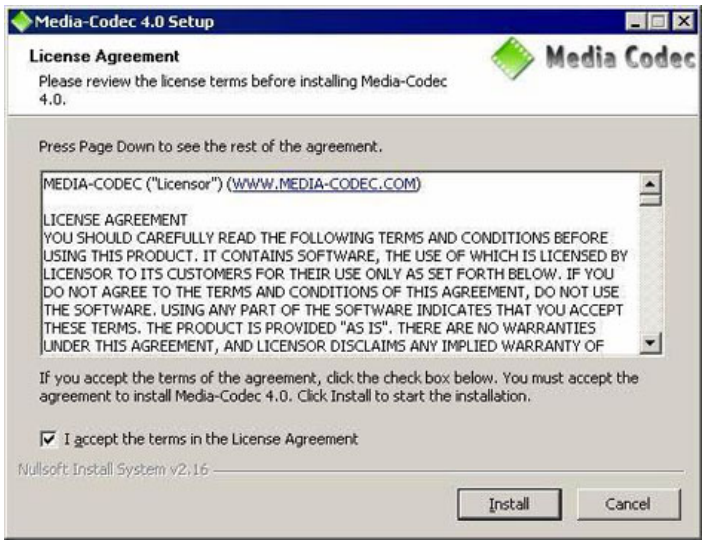
Haxdoor trojanac je u svojoj suštini backdoor program s *rootkit* mogućnostima. On, poput *rootkit* programa, sakriva svoju prisutnost na sustavu i može ga se otkriti jedino antivirusnim alatima koji koriste *rootkit* detektore (npr. Panda Antivirus). Sadrži mogućnost špijuniranja korisnika, a koristi se za krađu podataka vezanih uz bankarske transakcije (lozinke, korisnička imena, sigurnosni kodovi…) i drugih osjetljivih informacija.

Ovaj napredni trojanac sakuplja lozinke kada zaraženi korisnik pristupi web stranicama neke od najpoznatijih svjetskih banaka (CitiBank, Nordea, Barclays…). Također sadrži mogućnost sakupljanja lozinki iz nekih messenger klijenata te mijenjanja postavke Internet Explorera. Svi sakupljeni podaci šalju se na e-mail adresu corpse@mailserver.ru. Autor također može upravljati ponašanjem trojanca, slanjem nekih jednostavnih naredbi putem IRC kanala.

U medijima je zabilježen napad ovog trojanca na jednu od većih švedskih banaka - Nordea Bank[3]. Tom prilikom prouzročena je šteta od oko 500,000 britanskih funti. Također je objavljeno da su razne inačice ovog trojanca oštetile tisuće stanovnika Ujedinjenog Kraljevstva u nepoznatom iznosu[4].

2.3.3. Zlob

Zlob je trojanac koji dolazi u obliku lažnog DirectX kodeka za reprodukciju video zapisa. Prvi put je otkriven krajem 2005. godine, ali tek sredinom 2006. je privukao veću pažnju antivirusne industrije. Jednom kada je instaliran, uzrokuje iskakanje raznih reklamnih prozora upozoravajući korisnika da je zaražen virusom. Također, poput Vundo trojanca, savjetuje instalaciju lažnih antivirusnih rješenja čime korisnik može još više kompromitirati svoj sustav. Zlob se najčešće prenosi putem nekih messenger servisa (Meebo, AOL, Windows Live) ili putem nekih Internet igara (World of Warcraft, Counter-Strike i dr.). Prema podacima tvrtke F-Secure do sada su otkrivene 32 različite inačice ovog trojanca.



Slika 2.7. Instalacija Zlob trojanca

2.4. Trendovi

Glavna razlika između nekadašnjih kompjuterskih virusa i današnjih zloćudnih programa je njihov skraćeni životni ciklus i orijentacija na nove ciljeve – krađa identiteta, *Botnet* mreže, krađa brojeva kreditnih kartica i drugih osobnih informacija žrtava. U ovom poglavlju prikazani su neki noviji trendovi u izradi zloćudnih programa kao što su ciljani napadi, razvoj crnog tržišta zloćudnog softvera i slično.

2.4.1. Ciljani napadi

Današnji zloćudni programi dizajnirani su tako da, uvjetno rečeno, ne dižu previše buke. Za razliku od prošlosti, kada su virusi i crvi dizajnirani tako da zaraze što je više moguće računala i općenito su bili prilično uočljivi – današnji zloćudni programi stvoreni su tako da budu što manje sumnjivi.

Autori zloćudnih programa danas koriste napredne tehnike kako bi zaobišli zaštitu koju koriste antivirusni programi i ostali neotkriveni. Jedna od glavnih strategija za postizanje ovog cilja je distribucija relativno malog broja kopija sa više različitih inačica istog zloćudnog programa. Nekada je jedan virus ili crv bio odgovoran za inficiranje stotina, tisuća pa čak i milijuna različitih računala. Vidljivost ovakvih situacija bila je očita za stručnjake iz antivirusnih kompanija. Danas je situacija drugačija, i stručnjaci sve teže otkrivaju nove inačice zloćudnih programa, jer zaraženi korisnici najčešće ni sami nisu svjesni da su žrtve zloćudnog softvera.

Novi zloćudni programi obično inficiraju samo nekoliko stotina računala prije nego se nadograde na neku novu inačicu, kako ih antivirusi ne bi mogli otkriti. Autori antivirusnih rješenja tako su stavljeni pred novi izazov – kako otkriti zloćudni softver koji je zarazio samo nekoliko stotina računala?

2.4.2. Ispitivanje pomoću antivirusa

Iako je ova tehnika stara i već otprije poznata, trend njenog korištenja je u porastu. Svaka nova inačica zloćudnog softvera ispituje se pomoću antivirusnih rješenja kako bi se izbjegla detekcija. Ovaj postupak autorima je znatno pojednostavljen postojanjem automatiziranih servisa na Internetu, poput stranica Jotti i VirusTotal, koji na jednostavan način omogućuju ispitivanje programa pomoću više antivirusnih rješenja odjednom.

Slika 2.8. Primjer korištenja stranice VirusTotal

Današnji autori zloćudnog softvera također koriste i posebne alate za ispitivanje svojih programa na heurističku analizu i analizu ponašanja, koje predstavljaju najnaprednije tehnologije kojima se danas koriste tvorci antivirusnih rješenja. Na ovaj način mogu se osigurati da njihov program neće, slanjem na besplatnu provjeru primjerice VirusTotal alatom, biti poslan stručnjacima iz antivirusnih tvrtki.

Cilj ovog ispitivanja nije toliko u izbjegavanju detekcija od strane svih antivirusnih rješenja, već barem od većine njih. S obzirom da se napada mali broj računala, nije isplativo raditi napredne zloćudne programe ukoliko će oni biti otkriveni nakon nekoliko dana ili sati.

2.4.3. Alati za sažimanje

Jedna od najviše korištenih tehnika za izbjegavanje detekcije je sažimanje (eng. *packing*) izvršnih datoteka zloćudnih programa pomoću posebno oblikovanih alata (eng. runtime packers). Ovi alati mogu mijenjati i sažimati izvorne datoteke pomoću posebnih algoritama za komprimiranje, te time promijeniti izvorni oblik programa. Konačni rezultat je izmijenjena izvršna datoteka koja i dalje obavlja istu funkciju kao i original. Time autori izbjegavaju antivirusnu zaštitu koja koristi uzorke (eng. *signature*), ukoliko antivirus ne koristi algoritme za dekomprimiranje (eng. *unpacking*). Autori zloćudnih programa uhvatili su se u koštac s problemom dekomprimiranja tako da koriste izmijenjene inačice poznatih alata za sažimanje izvršnih datoteka ili stvaraju vlastite alate.

2.4.4. Crno tržište

Najnoviji trend na području proizvodnje zloćudnih programa je stvaranje tzv. crnog tržišta. Današnji kriminalci više ne trebaju posjedovati veliko tehnološko znanje i sami stvarati zloćudne programe, već jednostavno mogu na raznim forumima kupiti posebno oblikovani zloćudni program koji je podešen za njihove potrebe. Autori zloćudnog softvera sve se više okreću ovoj novoj koncepciji – prodaji zloćudnog softvera kao usluge (eng. *malware-as-a-service*). Ovaj trend posebno je velik u posljednje dvije godine, a najaktivnije tržište je na području Rusije.

Na crnom tržištu mogu se nabaviti *Botnet* mreže za izvršavanje DoS (eng. *Denial of Service*) napada, personalizirani trojanski konji, poslužitelji za slanje neželjene pošte (eng. spam), posebni alati za sažimanje i drugi zloćudni programi. Limbo trojanac također se može kupiti, i to po cijeni od 350 USD, dok je prije samo dvije godine njegova cijena bila 1.500 USD. U ovom trendu pada cijena trojanskih konja na crnom tržištu može se tražiti razlog njihove sve veće zastupljenosti u ukupnom broju zloćudnih programa. U tablici 2.1 prikazane su cijene nekih poznatijih zloćudnih programa.

Keylogger Teller 2.0	400 USD
MPACK	700 USD
Limbo	350 USD
WebMoney Trojan	500 USD
FTP Checker	15 USD

izvor: PandaLabs

Tablica 2.1. Cijene zloćudnih programa

Zabilježen je čak i slučaj pokušaja prodaje zloćudnog programa s licencnim ugovorom. Slučaj su otkrili stručnjaci iz tvrtke Symantec, a u ugovoru se prijetilo prijavom korisnika antivirusnim tvrtkama ukoliko pokuša preprodati program[5].

I understand that the restriction on the domain or IP is somewhat inconvenient. But unfortunately, this is the only way to avoid resale script. You must understand that this is necessary, otherwise the link will be able to use every student. This script was written for serious people with special knowledge and expertise in this business. It's written on the basis of three years' experience in this regard. This version is fully consistent with PERSONALLY my requirements.

Price :

- **Bundle :** $ 590 for a single domain and / or IP address (the IP address can be multiple domains). Of course you can make code expansion and connectivity to other domains! If you do, for example, spam-suggest making a separate domain under the bridge, then he was never zabanit.
- **Additional IP / domain :** $ 490
- **Apdeyty :**
  - Smaller apdeyty-$ 15 (or free)
  - Major (new ekspy) - $ 50
  - fix bug-free (in the version 1.x)
- **Help in installing it on your own server :** $ 15
- **Consultations :** free

Probiv ~ 13% adalte (~ 20% ifreym), 25-30% (exUSSR) to a suitable traffe.

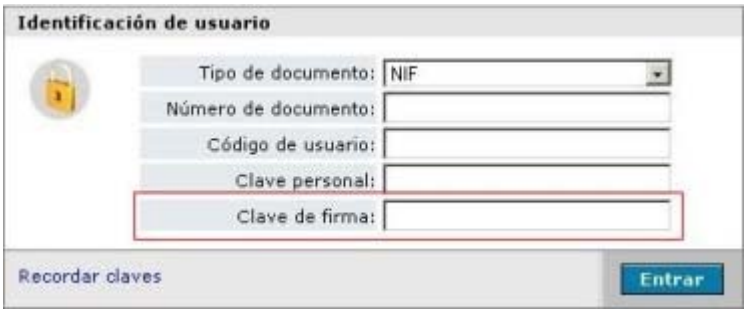
Slika 2.9. Prodaja zloćudnog programa na "*underground*" forumu

3. Limbo

3.1. Bankarski trojanski konji

Bankarski trojanci jedna su od najopasnijih vrsta zloćudnih programa danas. Ovi zloćudni programi specijalizirani su za krađu podataka koji se koriste za bankarske transakcije na Internetu. Oni koriste napredne tehnike za prijevaru korisnika, kao što je HTML injekcija, kako bi izvukli iz korisnika podatke kao što su PIN (eng. Personal Identification Number) brojevi, lozinke, brojevi kreditnih kartica i drugi osjetljivi podaci. Trenutno ne postoji efikasna zaštita protiv njih, pa se niti jedan korisnik Internet bankarstva danas ne može osjećati potpuno sigurnim.

Izrađuju ih profesionalni kiber (eng. cyber) kriminalci kao što su ruska skupina RBN (eng. *Russian Business Network*), a koriste sve napredne tehnike za izbjegavanje detekcije antivirusnim alatima. Antivirusne kompanije razvijaju posebne heurističke algoritme kako bi se nosili sa ovim naprednim programima. Primjeri ove vrste trojanaca su već spominjani: Haxdoor, zatim Sinowal, Bancos te Limbo trojanac o kojem će biti više riječi u idućem poglavlju.



Slika 3.1. Primjer HTML injekcije koda u web stranicu

Slijedi lista poznatih obitelji bankarskih trojanaca i njihovih karakteristika. Oni se razlikuju prema bankarskim institucijama koje napadaju, alatima za sažimanje koje koriste te prema svojem ponašanju na sustavu zaraženog korisnika.

- Banbra, Dadobra, Nabload, Banload
  - napisani su u programskom jeziku Visual Basic
  - koriste Yoda Protector alat za sažimanje
  - napadaju banke u Portugalu i Brazilu
  - ukradene podatke šalju elektroničkom poštom i ftp (eng. File Transfer Protocol) protokolom na udaljeni poslužitelj
- Bancos
  - programirani u Visual Basicu
  - napadaju Banke u Portugalu i Brazilu
- Sinowal, Wspoem, Anserin, AudioVideo
  - koriste ručno napravljen alat za sažimanje
- Goldun, Haxdoor, Nuclear Grabber
  - registriraju DLL i SYS datoteke u Windows Registry-u
- Bankolimb, Nethell, Limbo
  - sastoje se od dva modula – DLL i XML datoteke
  - integriraju se u web preglednik kao programski dodatak (Browser Helper Object)

3.2. Značajke Limbo trojanca

Trojanski konj Limbo prvi puta je otkriven još u siječnju 2007. godine. Do danas je otkriveno više različitih inačica ovog trojanca pa je također poznat i pod imenima Nethell, Bankolimb, PWS-Banker i dr. Antivirusni uzorci izdani su za neke inačice ovog trojanca, no obzirom na brzinu njegovog mutiranja i broj različitih inačica postoji mogućnost da nisu sve obuhvaćene. U tablici 3.1 možemo vidjeti imena pod kojima se vodi u raznim bazama podataka proizvođača antivirusnog softvera.

Kaspersky	Trojan-Downloader.Win32.Small.hbo
Sunbelt	Trojan.Nethell.B
BitDefender	Trojan.Spy.Banker.ZVO
F-Secure	Trojan-Spy.Win32.Banker.evz
F-Prot	W32/Banker.BABN
Panda	Trj/Bankolimb.A

Tablica 3.1. Imena u bazama zloćudnih programa

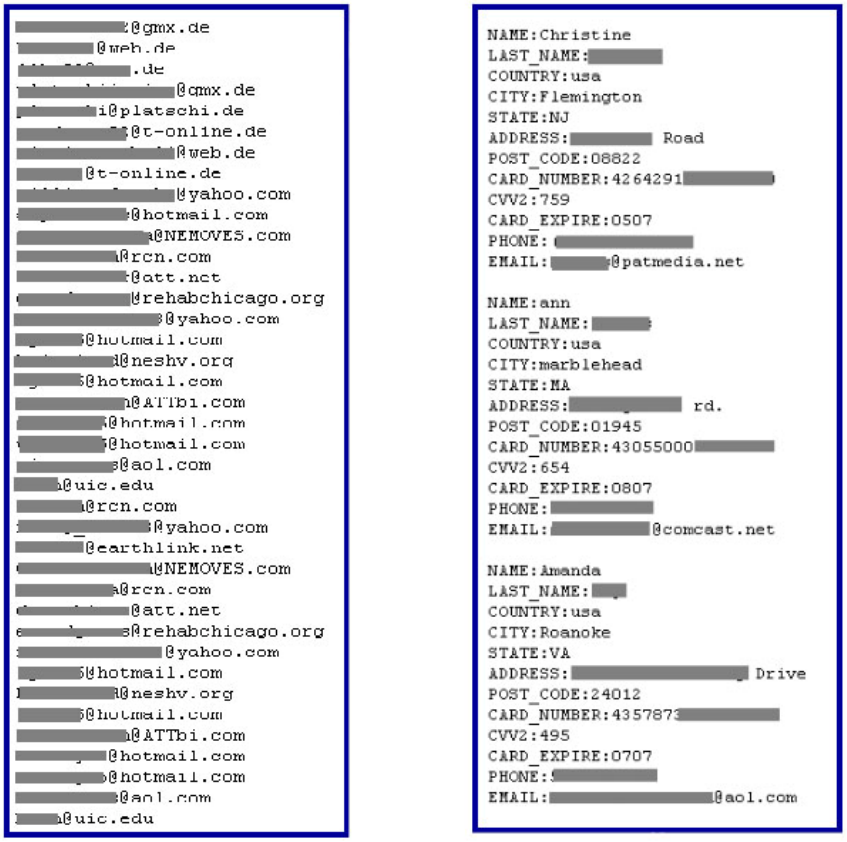
Glavni cilj napada ovim trojancem su bankarski sustavi. On se integrira u web preglednik žrtve koristeći tehniku ubacivanja HTML (eng. Hypertext Markup Language). Formularima koje na webu prikazuje bankarska institucija, u stvarnom vremenu, dodaju se nova polja koja od korisnika traže osjetljive podatke. Tehnika HTML injekcije je upravo ono što razlikuje napad Limbo trojancem od drugih *phishing* napada. Kod drugih *phishing* prijevara korisnik se obično preusmjerava na potpuno drugu web adresu gdje se nalazi stranica slična ili jednaka kao stranica banke koja se napada. Obzirom da Limbo mijenja stranicu banke u stvarnom vremenu (na računalu korisnika) ovakav napad može prevariti i iskusnije korisnike i baš zato je učinkovit. Za ulazak na sustav žrtve ovaj trojanac se koristi standardnim metodama poput instalacije naizgled korisnih programskih dodataka za web preglednik (npr. instalacija kodeka za gledanje video datoteka unutar preglednika) kao i drugim, za korisnika nevidljivim, metodama.

Baš kao i mnogi drugi zloćudni programi, Limbo se prodaje na crnim tržištima po cijenama koje variraju od 350 do 1000 USD. Njegova cijena ima tendenciju pada, pa se i frekvencija njegovog pojavljivanja povećala. Prodaje se uglavnom na ruskim forumima, pa se pretpostavlja da je njegov autor jedan od brojnih pripadnika ruske *underground* scene. Iako se pretpostavlja da je već nanio znatnu štetu raznim financijskim institucijama koje napada, u medijima još nije objavljen nijedan takav slučaj. To je razumljivo obzirom da bankarske institucije često sakrivaju takve događaje od medija zbog straha od narušavanja ugleda.

Limbo se sastoji od tri modula koji su detaljnije opisani u nastavku poglavlja. To su:

- Helper.dll – jezgra trojanskog konja
- Helper.xml – konfiguracijska datoteka i
- Control Panel – aplikacija na poslužitelju koja sakuplja ukradene podatke i šalje naredbe pojedinim inačicama trojanaca na zaraženim računalima

Podaci koje Limbo krade sa korisničkih računala variraju od PIN-ova i lozinki do brojeva kreditnih kartica i socijalnog osiguranja, te e-mail adresa koje se mogu koristiti za slanje neželjene pošte (eng. *spam*). Primjer *log* datoteke koju je stvorio Limbo prikazan slici 3.2.



Slika 3.2. Log datoteka Limbo trojanca

3.2.1. XML modul

XML modul obično se zove helper.xml iako, baš kao i kod DLL modula, nazivi variraju kod raznih inačica trojanca. XML modul je svojevrsna konfiguracijska datoteka ovog trojanca i u njoj se nalaze svi podaci važni za izvedbu napada. Primjerice, u njoj se pohranjeni HTML kodovi za ubacivanje u web stranice raznih financijskih institucija. U posljednjim inačicama koje su otkrivene, ova datoteka je bila kriptirana. Na slici 3.3 možemo vidjeti podatke koji se nalaze u ovoj datoteci. Za svaku bankarsku instituciju pohranjeni su podaci koji se ubacuju u web stranicu kako bi ona izgledala što realnije.

Slika 3.3. Sadržaj datoteke helper.xml

3.2.2. DLL modul

DLL modul je središnji dio ovog trojanskog konja. Prilikom instalacije, Limbo ovu datoteku (helper.dll) ubacuje u Windows Registry kao BHO (eng. Browser Helper Object) objekt. BHO objekt je programski dodatak koji web pregledniku Internet Explorer dodaje novu funkcionalnost. Datoteka se nalazi u direktoriju c:\Windows\System32.

Kao programski dodatak web pregledniku, ovaj trojanac ima mogućnost pristupa korisničkim lozinkama sačuvanim unutar preglednika te brisanja tzv. kolačića (eng. cookies). Također trojanac sadrži i funkcionalnost hvatanja korisničkog unosa na tipkovnici (eng. keylogger). Sve podatke koje prikupi, Limbo pohrani u svoju log datoteku i šalje na središnji poslužitelj.

Upravo DLL datoteka je dio trojanca koji najviše varira kod različitih inačica ovog trojanca. Nove inačice stvaraju se na dnevnoj osnovi kako bi se izbjegla detekcija antivirusnim alatima. Zabilježeni su slučajevi od čak šest različitih varijacija trojanca u samo jednom danu. Korisnici Limba imaju na raspolaganju jednostavnu aplikaciju za izradu novih varijacija samo jednim klikom miša. Aplikacija namijenjena stvaranju novih DLL modula prikazana je na slici 3.4. Nakon što je nova inačica izrađena ona se lako distribuira na zaražena računala.

Slika 3.4. Aplikacija za izradu novih inačica Limba

DDL modul stvara jedinstveni identifikacijski broj za svako zaraženo računalo. Taj se broj koristi za komunikaciju sa središnjim poslužiteljem. Limbo može slati log datoteke na središnji poslužitelj te primati naredbe od njega. Poslužitelj sa Limbom komunicira preko PHP (eng. Hypertext Preprocessor) skripti. Naredbe koje poslužitelj može slati Limbu su slljedeće:

- DOWNLOAD – dohvaćanje proizvoljne datoteke s Interneta
- UPDATE – nadogradnja DLL datoteke
- DELETECOOKIES – brisanje kolačića
- DELETESELF – brisanje trojanca
- RUN – pokretanje proizvoljnog programa na sustavu
- LOADXML – učitavanje konfiguracijske datoteke
- REBOOT – ponovno pokretanje sustava

- KILLWIN – gašenje Windowsa

3.2.3. Control Panel

Control Panel je aplikacija koja se nalazi na središnjem poslužitelju kojim upravlja napadač. Pomoću ove aplikacije napadač prima ukradene podatke poslane sa zaraženih računala i upravlja trojancima slanjem naredbi. Ukoliko neko zaraženo računalo nije trenutno upaljeno, naredbe se pamte i šalju prvom slijedećom prilikom.

Slika 3.5. Forma za slanje naredbi

Pomoću Control Panela napadač može pregledavati podatke o zaraženim računalima, filtrirati ih po zemljama, pa čak i računati statistike. Control Panel također ima mogućnost pregledavanja i pretraživanja primljenih log datoteka. Na slici 3.6. možemo vidjeti sučelje koje Control Panel nudi za pretraživanje log datoteka.

Slika 3.6. Sučelje za pretraživanje log datoteka

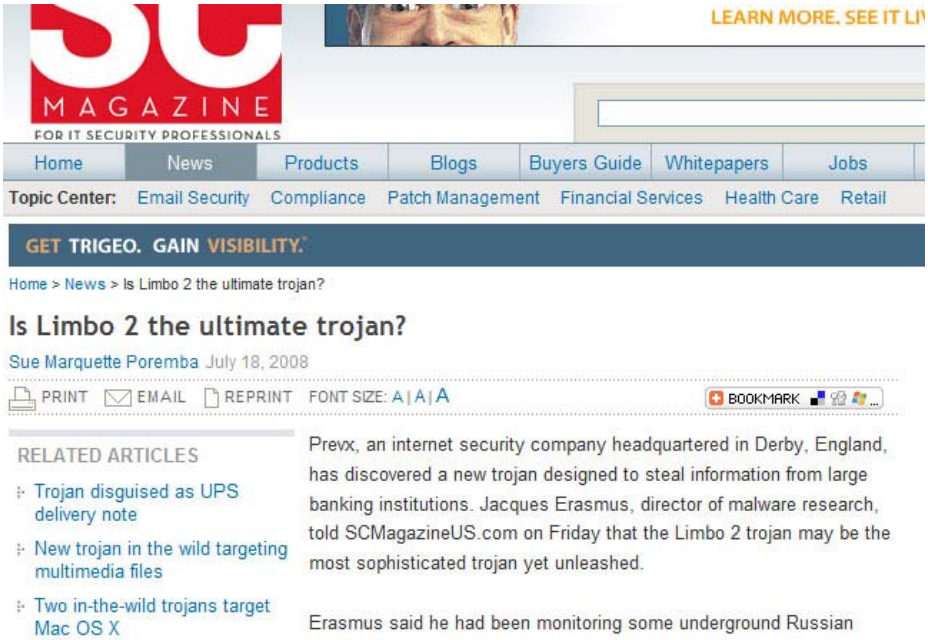
3.3. Limbo u medijima

Iako se relevantni podaci o njemu pronalaze „na kapaljku“, Limbo je posljednjih mjeseci izazvao prilično veliku medijsku pažnju. Razlog je neupitno velika opasnost koja vreba od strane ovog i sličnih trojanaca, no s druge strane i strah, jer čak ni najbolji antivirusni programi ne mogu pružiti odgovarajuću zaštitu. Tijekom ove godine objavljene su dvije medijske priče s Limbom u centru pažnje, a razvile su se i razne polemike u krugovima stručnjaka koji se bave zloćudnim programima.

Prva priča potekla je iz tvrtke Prevx. Riječ je o tvrtki koja se bavi sigurnošću, a i sama proizvodi antivirusno rješenje. Stručnjaci iz ove tvrtke tvrdili su da su pronašli trojanskog konja sa dosad neviđenim mogućnostima. Kako su rekli, ovaj trojanac, kojeg nazivaju Limbo 2, može izbjeći sve danas popularne antivirusne proizvode. Naravno vrlo brzo je stigao demanti. Allysa Myers iz tvrtke McAfee objavila je na svojem blogu da Limbo nije ništa drugo nego generički PWS-Banker trojanac te da ga gotovo svaki bolji antivirus može otkriti. Što je prava istina teško je reći. Limbo je svakako jedan od najprofinjenijih zloćudnih programa koji kolaju Internetom danas i koristi sve napredne tehnologije za izbjegavanje detekcije. No, s druge strane, metode koje koristi za sakrivanje nisu novost proizvođačima antivirusnih rješenja. Oni također svakodnevno rade na novim rješenjima i tehnologijama kako bi uspjeli otkriti i najnaprednije zloćudne programe.

Druga priča objavljena je od strane Uri Rivnera, direktora sektora novih tehnologija u tvrtki RSA. U svom medijskom priopćenju Rivner je naglašavao opasnost od nove tehnike koju Limbo koristi – HTML injekcije. Prema njegovim riječima, čak ni najiskusniji korisnici ne mogu primijetiti da su žrtva prijevare, jer izmjenom web stranice banke u stvarnom vremenu Limbo kod korisnika ne pobuđuje nikakvu sumnju. Rivner je također iznio podatke o padajućim cijenama Limbo trojanca na crnom tržištu zloćudnih programa te posebno istakao opasnost koja je posljedica dostupnosti ovih naprednih zloćudnih programa.

Iako obje tvrtke koje su objavile priče i same razvijaju proizvode koji na neki način rješavaju istaknute probleme, pa se njihova medijska istupanja mogu shvatiti kao promidžba, činjenica je da napredni zloćudni programi postoje te da javnost mora biti svjesna posljedica koje mogu nastati ukoliko se ne podigne svijest o važnosti podučavanja korisnika i primjene dobrih sigurnosnih praksi u zaštiti korisničkih računala.

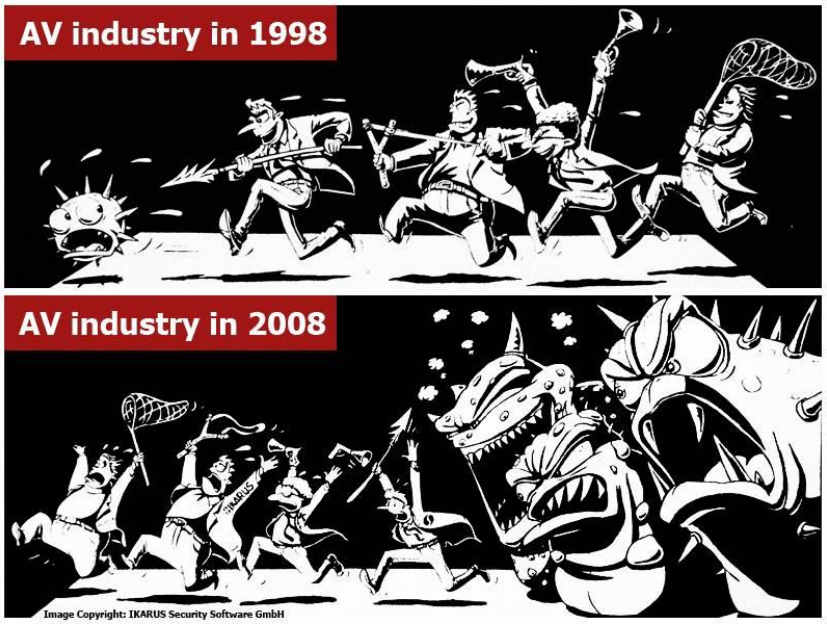


Slika 3.7. Limbo u medijima

4. Zaštita

4.1. Tehnike otkrivanja zloćudnih programa

Antivirusne kompanije se svakim danom sve teže nose s povećanjem broja i složenosti zloćudnih programa. Kako bi što kvalitetnije zaštitile svoje korisnike, razvijaju nove proaktivne tehnologije koje mogu otkriti zloćudni program bez korištenja klasičnog sustava s uzorcima programa (eng. signature). Slika 4.1. na šaljiv način prikazuje odnos snaga između zloćudnih programa i antivirusne industrije nekad i danas.



Slika 4.1. Antivirusna industrija nekad i danas

Prema podacima koje je objavio australski CERT (eng. Computer Emergency Response Team) osamdeset posto novih zloćudnih programa prolazi nezamijećeno pored svih danas cijenjenih antivirusnih rješenja. Ovaj zabrinjavajući podatak dobro ilustrira situaciju u kojoj se antivirusne kompanije danas nalaze i probleme s kojima se suočavaju[6].

Prva generacija antivirusnih proizvoda potpuno se zasnivala na sustavu detekcije pomoću uzoraka zloćudnih programa. Ova generacija obilježila je veći dio devedesetih godina prošlog stoljeća. U tom periodu tek se kretalo s uvođenjem detekcije pomoću heurističkih tehnika. Ovo razdoblje također je obilježilo pojavljivanje prvih masovnih trojanskih konja, poput NetBus i BackOrifice trojanaca.

S 2000. godinom počele su se pojavljivati nove vrste zloćudnih programa, prvenstveno mrežni crvi i špijunski programi koji su imali epidemijske razmjere. Osnovnim antivirusnim tehnikama tada je pridodan i osobni vatrozid za zaštitu od mrežnih crva, kao i alati za čišćenje sustava koji su pomagali u oporavku od posljedica infekcije zloćudnim programima.

Danas se razvija tzv. treća generacija antivirusnih proizvoda koji se zasnivaju na naprednim heurističkim tehnikama te na analizama ponašanja (eng. behavioral analysis) programa na sustavu. Iako su neke od ovih tehnologija tek u začetku, napredak je u nekim slučajevima vidljiv. Veliki problem ovih novih tehnologija je velik broj tzv. lažno pozitivnih (eng. false positive) detekcija. Sve se više ističe važnost više-razinske sigurnosti. Ona podrazumijeva korištenje više sigurnosnih tehnologija odnosno slojeva u zaštiti računala i mreža.

4.2. Načini zaštite

Opasnosti koje vrebaju na Internetu danas ima više nego ikada. Milijuni ljudi svakodnevno su žrtve krađa identiteta i financijskih prijevara. Upravo zato je važno dobro se zaštiti, jer time ne povećavamo samo svoju sigurnost već i globalnu sigurnost svih korisnika Interneta.

Organizacija Fraudwatch International nudi sljedeće savjete za zaštitu od zloćudnih programa i prijevara:

1. **Ne otvarajte linkove unutar e-mail poruka**

   Hiperlinkovi koji se pojavljuju unutar poruka elektroničke pošte često su lažni ili sakriveni. Tekst koji opisuje link ne mora odgovarati sadržaju na koji link vodi. Savjet je svakako ne otvarati linkove koje se nalaze u e-mail porukama iz nepoznatih izvora.

2. **Koristite filtre za neželjenu poštu**

   Istraživanja su pokazala da je 85% svih poslanih poruka elektroničke pošte neželjeno, dok su većina sredstvo nekakve prijevare. Filtri neželjene pošte mogu spriječiti dio lažnih i zloćudnih poruka koje dolaze do krajnjih korisnika. Više informacija o ovom i drugim filtrima na aplikacijskoj razini TCP/IP stoga može se pronaći u sigurnosnom dokumentu "Zaštita od upada korištenjem L7-filtara" objavljenom na stranicama CERT-a.

3. **Koristite antivirusni softver**

   Antivirusi su najučinkovitiji način zaštite od virusa, trojanaca i drugih oblika zloćudnih programa. Oni sadrže mogućnost detekcije i uklanjanja takvih programa, pa se njihovo korištenje iznimno preporuča.

4. **Koristite osobni vatrozid**

   Vatrozidi mogu analizirati ulazni i izlazni promet koji prolazi kroz računalo. Oni tako mogu spriječiti upad hakera na računalo kao i instalaciju virusa, trojanaca i drugih zloćudnih programa. Kao zadnja linija obrane oni, čak i u slučaju instalacije trojanskog konja, mogu spriječiti slanje osjetljivih podataka na središnji poslužitelj.

5. **Instalirajte sve zakrpe za programe koje koristite**

   Zlonamjerni napadači koriste sigurnosne pogreške i ranjivosti u programima i operacijskim sustavima za upade i distribuciju zloćudnog softvera. Proizvođači softvera svakodnevno izdaju zakrpe za svoje programe kako bi uklonili te pogreške i ranjivosti. Upravo zato je važno instalirati sve dostupne zakrpe i time povećati otpornost svog sustava.

6. **Koristite antispyware programe**

   Špijunski programi (eng. spyware) najčešće se nastanjuju na sustav bez znanja korisnika. Iako njihova aktivnost može biti bezopasna, oni sakupljaju privatne podatke korisnika i time narušavanju njegovu privatnost. Na tržištu postoji cijeli niz besplatnih *antispyware* proizvoda (Ad-Aware, Spybot Search&Destroy i dr.), pa se savjetuje njihova upotreba.

7. **Provjerite svoje bankovne račune**

   Ukoliko ste odgovorili na sumnjivi e-mail ili ostavili svoje podatke na sumnjivim web stranicama, što prije provjerite svoj bankovni račun. Ukoliko uočite nepravilnosti prijavite slučaj nadležnoj banci i institucijama.

8. **Educirajte se o sigurnosti**

   Ovaj zadnji savjet možda je i najvažniji. Kako broj Internet prijevara svakodnevno znatno raste, korisnici moraju biti svjesni opasnosti koje vrebaju kao i načina na koji se mogu zaštiti. Baš kao zloćudni softver i načini zaštite napreduju svakim danom, pa je važno stalno se educirati i informirati o njima.

5. Zaključak

Obzirom na značajan korak u razvoju zloćudnih programa, teško je reći da li će stručnjaci koji se bave njima uspjeti iznjedriti nove tehnologije za zaštitu. Iako se u statistikama vidi njihov značaj porast, pitanje je koliko još vrsta i različitih inačica ovog softvera postoji na računalima diljem svijeta, a da se za njih uopće ne zna.

Cilj autora današnjih zloćudnih programa nije više samo-dokazivanje i eksperimentiranje, već krađa osjetljivih informacija i stjecanje izravne financijske koristi. Današnji kiber kriminalci opasniji su u svojim postupcima nego ikad dosad. Jedan od razloga ove situacije je i neusklađenost zakonskih regulativa u raznim zemljama svijeta, pa se kriminalci rijetko uspješno procesuiraju.

Stručnjaci iz antivirusne industrije rade na razvoju novih proaktivnih tehnologija kako bi se što uspješnije borili protiv novih izazova koje pred njih stavljaju autori zloćudnih programa. No veliku važnost u toj borbi svakako ima edukacija krajnjih korisnika. Naime, upravo korisnici i njihova svijest o opasnostima koje ih okružuju na Internetu najvažnija su karika u lancu sigurnosti. Antivirusi, vatrozidi i druga sigurnosna rješenja nikada neće omogućiti stopostotnu sigurnost, no pravilnom edukacijom korisnika u uporabi sredstava i praksi koje sigurnosna industrija predlaže može se znatno povećati njihova sigurnost, kao i globalna sigurnost svih korisnika Interneta.

6. Reference

[1] A banner year for malware, digital threats and the security industry , http://www.avertlabs.com/research/blog/index.php/2008/01/07/a-banner-year-for-malware-digital-threats-and-the-security-industry, siječanj 2008.

[2] Identity theft and fraud in Limbo,

http://www.mxlogic.com/securitynews/viruses-worms/identity-theft-and-fraud-in-limbo139.cfm, listopad 2008.

[3] Phishers haul in money from Nordic bank,

http://www.theregister.co.uk/2007/01/19/phishers_attack_nordea, siječanj 2007

[4] Haxdoor Trojan claims thousands of UK victims,

http://news.zdnet.co.uk/security/0,1000000189,39284024,00.htm, listopad 2006.

[5] Criminals try to 'copyright' malware,

http://www.msnbc.msn.com/id/24394270, travanj 2008.

[6] Eighty percent of new malware defeats antivirus,

http://www.zdnet.com.au/news/security/soa/Eighty-percent-of-new-malware-defeats-antivirus/0,130061744,139263949,00.htm, srpanj 2006.

[7] Kaspersky Security Bulletin 2008: Malware Evolution January - June 2008,

http://www.viruslist.com/analysis?pubid=204792034, rujan 2008.

[8] Vundo, http://en.wikipedia.org/wiki/Vundo,

[9] Cybercrime for sale,

http://pandalabs.pandasecurity.com/archive/Cybercrime_2E002E002E00_-for-sale-_2800_I_2900_.aspx, travanj 2007.

[10] Combating Malware: Leveraging the Power of a Planet, Panda Security, 2007.

[11] Malware 101 – Viruses, Aman Hardikar, 2008.

[12] From Traditional Antivirus To Collective Intelligence, Panda Security, 2007.

[13] The Business of Cybercrime, Luis Corrons, Panda Security, 2007.