

# **ZLONAMERNO UMREŽAVANJE KAO OBLIK ZLOUPOTREBE INFORMACIONIH TEHNOLOGIJA**

Radule Šoškić, dipl.inž, CISSP  
„Telekom Srbija” a.d.  
[rms@telekom.yu](mailto:rms@telekom.yu)

**Apstrakt:** Ovaj tekst izlaže neka važna pitanja koja se odnose na problematiku malicioznog umrežavanja. Učinjen je pokušaj da se ukratko izloži razvojni put ovakvih mreža, kao i trenutno stanje u ovoj oblasti, kako po pitanju ciljeva i motiva tako i po pitanju alata, tehnologije i tehnika koje se danas koriste. Takođe, ukazuje se i na pretnje i rizike koji se odnose na potencijalne mete i žrtve napada.

## **BOTNETS – MALICIOUS NETWORKS AS A FORM OF INFORMATION TECHNOLOGY ABUSE**

**Abstract:** This paper is aimed at bots and botnets related issues. It is an attempt to present a timeline of botnet evolution, today's state-of-the art botnet technology, attackers' actual motives, goals and tools of trade, as well as the accompanying threats and risks for potential targets and victims.

# 1. UVOD – KONCEPTI I DEFINICIJE

Zlonamerno umrežavanje je izraz koji je za potrebe ovog teksta odabran kao uslovno najpogodniji prevod čitavog niza engleskih izraza: *Zombie Networks*, *Robot Nets*, *Botnets*, *Zombie Armies* itd. Ovi izrazi označavaju uglavnom jedan isti pojam – grupu umreženih računara koji su kompromitovani od strane istog napadača i koji se nalaze pod njegovom kontrolom i upravljanjem. Ovakve mreže danas predstavljaju veliku i stalno rastuću opasnost za sve računare prisutne na Internetu, posebno tamo gde je nivo informatičke sigurnosti nizak. Logička i fizička organizacija ovakvih mreža, protokoli za upravljanje i kontrolu, skup komandi, ciljevi i efekti, kao i druge karakteristike ovakvih mreža mogu značajno da variraju. Cilj ovog teksta je da se na sveobuhvatan ali ne preterano opširan način pruži pregled problematike koja je vezana za ovaj vid zloupotreba.

Pre svega, potrebno je nabrojati neke pojmove koji su ključni za razumevanje ove problematike.

**a) *Zombie*, *Robot*, *Bot*** – ovi nazivi označavaju računar čiji je sistem informatičke sigurnosti kompromitovan tako da je on, nakon uspešnog napada, priključen zlonamerno formiranoj mreži i postao njen deo. Da bi jedan računar postao „bot”, neophodno je najpre da poseduje jednu ili više eksploataibilnih slabosti, zatim da napadač poseduje napadački alat kojim se ta slabost može iskoristiti (*Exploit*) i da se tokom napada na žrtvu uspešno i neprimetno instalira maliciozni kod u kojem je implementirana sama funkcionalnost „bota” (*Servant Code*).

**b) *Zombie Net(work)*, *Robot Net(work)*, *Botnet*, *Zombie Army*** – nazivi za mreže formirane od „botova” odnosno od „zombija”.

**v) *Command & Control (C&C)*** – označava način i sredstva kojima vlasnik upravlja i kontroliše svoju mrežu „botova”. Ovo uključuje niz specifičnosti: odgovarajuću topologiju i organizaciju mreže, mrežne i aplikativne protokole (standardne ili privatne), skup raspoloživih komandi (naredbi) i sl.

**g) *Herding*, *Botherding*** - „uzgajanje” ili „održavanje stada”. Ovaj izraz označava skup postupaka i metoda kojima se jedna zlonamerno formirana mreža inicijalno uspostavlja (*Deployment*) i kasnije proširuje novim članovima; to se takođe odnosi i na postupke i metode za očuvanje postojećeg članstva kao i za isključenje postojećih članova iz mreže. Tu spadaju i tehnike za skrivanje i očuvanje tajnosti identiteta „komandnog centra” iz kojeg se upravlja mrežom.

**d) *Attack Traffic*** – saobraćaj koji mreža zombija proizvodi sa ciljem napada na krajnju žrtvu. Srodan je termin *Attack Payload* kojim se označava sadržaj paketa koji se šalju u toku napada.

## 2. ISTORIJAT I RAZVOJ

### 2.1. Prvi primeri

Pojava malicioznog umrežavanja nije nova. Prvi primeri datiraju iz perioda 1999. - 2001. U to vreme publikovane su i prve analize konkretnih primera ovakvih mreža registrovanih na Internetu.

Prve mreže čiji je način rada dokumentovan i objavljen bile su *Trinoo* i *Tribal Flood Network* [1][2]. One se pojavljuju u julu 1999. Njihovo širenje se baziralo na slabostima i nizu manjkavosti u *RPC* protokolu koje su tada bile vrlo aktuelne. Za ove mreže je bilo karakteristično to da su se uspostavljale manuelno, bez prisustva ikakvog

automatskog mehanizma. Pronalaženje žrtava, napadi, zauzimanje i instalacija malicioznog koda vršeni su ručno – neposrednim angažovanjem ljudskog faktora. Bilo je uočljivo da su napadači vrlo pažljivo birali žrtve među onima čije su veze prema Internetu imale najširi propusni opseg.

Topologija je bila vrlo jednostavna – dvoslojna *Handler/Agent* struktura u kojoj je komandni centar direktno komunicirao sa svakim pojedinačnim zombijem u mreži (topologija zvezde). Dizajn je takođe dozvoljavao istovremeno prisustvo većeg broja komandnih centara – hendlera. Za komandovanje i kontrolu korišćeni su nestandardni, privatni protokoli koji su razvijeni na bazi *TCP*, *UDP* i *ICMP* protokola.

Funkcionalnost ovih mreža je bila veoma limitirana. One su bile dizajnirane isključivo kao sredstvo za realizaciju distribuiranih napada tipa *Denial of Service (DDoS)*. Praktično sve što su „zombiji” radili svodilo se najpre na čekanje komande a zatim na zasipanje jedne jedine izabrane žrtve velikom količinom paketa. Paketi koji su se koristili za napad bili su *UDP Flood*, *TCP SYN Flood* i *ICMP Echo Request*.

Ove mreže su bile povezane tako što su agenti posedovali fiksne (*hard-coded*) liste hendlera, dok su sami hendleri čuvali IP adrese agenata u lokalnim fajlovima.

Ima mnogo indikacija da su ove prve mreže nastale sa ciljem da se jedan teorijski i istraživački rad proveru u realnom okruženju (takozvani *Proof of Concept*) a ne u ozbiljnoj nameri da se njihovom primenom pribavi neka korist ili načini šteta. Već na prvi pogled se zapaža da su ove mreže dizajnirane tako da ne poseduju nikakve mehanizme za zaštitu tajnosti. Protokoli za komunikaciju imali su statičke i jasno prepoznatljive signature, koje su se mogle lako detektovati na *IDS* sistemima, dok su na agentima postojale fiksne liste hendlera, tako da je svaki komandni centar mogao biti jednostavno lokalizovan. Softver se mogao lako pronaći na Internetu, tako da je bio podložan detaljnoj analizi. Čak su i autori softvera bili brzo identifikovani i, premda pod pseudonimom, dobili prilično veliki publicitet i prostor u medijima. [3]

## 2.2. Upotreba enkripcije

Već u avgustu 1999. pojavljuje se novi tip malicioznih mreža, poznat pod imenom *Stacheldraht* (bodljikava žica, na nemačkom)[4]. U osnovi, ova mreža je predstavljala kombinaciju mreža *Trinoo* i *TFN*, ali je sobom donela dve velike novosti u dizajnu. Kao prvo, komandno-kontrolna komunikacija između hendlera i agenata sada je bila enkriptovana. Drugo, uvedena je mogućnost automatskog ažuriranja agenata. U pogledu uspostavljanja i širenja same mreže, i dalje se koristi ručna metoda – selekcija potencijalnih agenata vršena je prema raspoloživom propusnom opsegu, a instalacija malicioznog koda i dalje nije bila automatska.

## 2.3. Skrivanje i ometanje detekcije

Krajem 1999. (u decembru) pojavljuje se *TFN2K*. [5] Ova mreža je unela dodatna poboljšanja u odnosu na sve prethodne. Komandno-kontrolni protokol je usavršen tako da maksimalno otežava detekciju i otkrivanje hendlera. Takođe, napadački saobraćaj je dizajniran tako da je bilo veoma teško identifikovati same agente – u paketima se koriste lažne izvorne adrese (*IP Spoofing*), paketi su često i na različite načine malformirani, itd.

Uprkos značajnim poboljšanjima, ostaje karakteristično to da je za uspostavljanje ovakve mreže bio neophodan veliki manuelni rad. Uspešno otkrivanje, napadanje i zauzimanje novih zombija još uvek je zavisilo od hakerskog „ručnog rada”. Stoga je razumljiv napor da se dizajn unapredi pre svega u pravcu zaštite same mreže od lakog otkrivanja. Bilo je neophodno ne samo izbeći kaznu zbog nelegalnog i

kriminalnog delovanja, već pre svega sprečiti preotimanje teško izgrađene napadačke infrastrukture od strane „podzemne“ konkurencije.

Početak 2000. godine beleži se porast registrovanih *DDoS* napada, od kojih su neki bili usmereni na veb sajtove visokog profila. Može se zaključiti da je eskalacija *DDoS* napada uzela maha tek nakon što su prethodno usavršene tehnike za „zametanje tragova“. Haker poznat po pseudonimu *Mafiaboy* u to vreme izvršio je niz uspešnih *DDoS* napada na *Yahoo!*, *eBay*, *Amazon* i *CNN*.

U aprilu 2000. pojavljuje se novi alat za *DDoS* napade, poznat pod imenom *mstream*. [6] Mreža *mstream* je za napad koristila *TCP ACK* pakete sa randomizovanim podacima o izvoru i nasumično odabranim portom na destinaciji. Iako je sam kod bio vrlo primitivan u odnosu na svoje prethodnike, registrovano je više mreža realizovanih pomoću ovog alata. Jedina novost je da su svi priključeni korisnici dobijali informacije o svim novim konekcijama – uspešnim ili neuspešnim. Analizom otkrivenih mreža i poređenjem sa nizom prethodnika dolazi se do zaključka da se arhitektura *attacker+handler/agent* učvrstila i održala kao neka vrsta standarda u ovoj oblasti.

## 2.4. Daljinska kontrola i višeslojna topologija

Svi pomenuti primeri posedovali su neku vrstu mogućnosti za daljinsko upravljanje. Vlasnik mreža je mogao nekom vrstom *TCP* protokola (slično *telnet* protokolu) da pristupi handleru iz različitih tačaka u mreži, uz korišćenje lozinke. Time je topologija mreže dobila još jedan sloj i dodatno iskomplikovala otkrivanje i eventualno hvatanje osoba odgovornih za napad. To znači da je ne samo agent već i handler mogao biti postavljen na tuđu, kompromitovanu mašinu. Time je pravi komandni centar postajao mobilan i praktično neuhvatljiv.

## 2.5. Chatting Zombies

U avgustu 2000. godine pojavio se *Trinity DDoS Tool* [7] koji je doneo sa sobom jednu zaista revolucionarnu novost, novost koja će izvršiti veliki uticaj na usmerenje budućeg razvoja malicioznih mreža, sve do danas. Naime, *Trinity* koristi *IRC* kao komandno-kontrolni protokol. *IRC* (*Internet Relay Chat*) je najstariji i najpopularniji protokol za direktnu komunikaciju tipa klijent-klijent, koji je utro put nizu drugih sličnih rešenja kao što su *ICQ*, *AOL IM*, *Yahoo! IM*, *MS Messenger* i drugi. *IRC* je opisan u *RFC 1459* još 1993. godine, veoma dobro je dokumentovan i što je najvažnije dobro pokriven serverskom infrastrukturom, budući da je ovaj oblik komunikacije veoma popularan i široko rasprostranjen.

Dakle, umesto da se iscrpljuju u razvoju, testiranju i implementaciji zasebnih komunikacionih protokola, autori malicioznog softvera kreću sasvim drugim putem: počinju da koriste standardne protokole i već postojeću mrežu servera. Pokazalo se da je malicioznu komunikaciju mnogo lakše prikriti među bezbrojnim kanalima *IRC* komunikacije, iako je ona javna i svima dostupna, nego u opskurnim i komplikovanim privatnim rešenjima. Stvari se nekad najbolje skrivaju kada se drže naočigled svih.

## 2.6 Automatizacija i prelazak na Windows

Dalji razvoj malicioznih mreža išao je u pravcu razvoja automatskih rešenja za njihovo uspostavljanje i širenje (*deployment*). Prvi rezultati oslanjali su se na socijalni

inženjering, odnosno na eksploataciju slabosti u ljudskom faktoru. Tokom 2000. godine zabeleženo je nekoliko značajnih novih virusa – trojanaca čija je propagacija išla preko fajlova priključenih uz poruke elektronske pošte (*e-mail attachments*). Najpoznatiji predstavnik ove klase virusa u ovom periodu bio je *VBS/LoveLetter*, [8] dok je najpopularniji alat za automatsko uspostavljanje i širenje bio *t0rnkit*. [9]

Nešto kasnije (januar 2001.) pojavljuju se novi alati koji su posedovali mehanizme za automatsko otkrivanje novih „kandidata za zombije” i za automatsku propagaciju. Pre svega to je bio tzv. *Ramen*, [10] koji je eksploatisao slabosti u nekim *Unix/Linux* programskim paketima, ali i niz drugih, koji su se raširili tokom 2001. godine: *VBS/OnTheFly* (*Anna Kournikova*) [11] i *W32/sircam*, koji su se širili kroz socijalni inženjering, *erkms* i *li0n*, koji su instalirali *DDoS* agente koristeći slabosti u *BIND* sistemima itd.

Druga polovina 2001. bila je obeležena rastućom kompleksnošću i sofistiranošću tehnika za propagaciju malicioznog koda. „Crvi” kao što su *W32/Leaves* i *Code Red* demonstrirali su do tada neviđene sposobnosti: *W32/Leaves* je eksploatisao prethodno postavljene „trojance” tipa *SubSeven* [12] i imao sposobnost samostalnog obnavljanja i ažuriranja kao i menjanja sopstvene funkcionalnosti tokom propagacije; *Code Red* [13] je bio sposoban da izvršava *TCP SYN DoS* napade usmerene na izabranu metu. Mogao je da skenira opsege mrežnih adresa u potrazi za pogodnom žrtvom, što je često dovodilo i do lokalnih *DoS* stanja usled ekstremno visokog skenirnog saobraćaja. Nešto kasnije pojavio se i *Code Red II*, koji je takođe eksploatisao slabosti u *IIS Indexing Service DLL*-u.

Nakon toga, razvoj je išao u smeru pojačavanja napadačke snage; agregacijom većeg broja tehnika koje su do tada karakterisale razne pojedinačne viruse, crve i agente, nastao je „supercrv” pod nazivom *Nimda* (*Admin*, napisano unazad). [14] Ovaj crv je imao mogućnost propagacije preko čitavog niza vektora: priključci uz poštu, *SMB* protokol, trojanci iz prethodnih napada (*backdoors*), eksploatacija jedne slabosti programa *Internet Explorer* i eksploatacija jedne slabosti u *IIS* (*Internet Information Server*).

Ovde se može uočiti evolucija propagacionih mehanizama: u početku je propagacija išla iz jednog centralnog izvora i obavljala se ručno (*Trinoo*); zatim se prešlo na tzv. lančanu propagaciju kod koje se inicijalni napad dešava ručno a zatim se maliciozni kod dalje automatski raznosi sa sistema na sistem (*Ramen*); krajnji stadijum predstavlja autonomna propagacija (virusi/crvi, na pr. *Code Red*) – kod njih se i napad i raznošenje odvijaju automatski.

Sve do kraja 2000. godine, softver za maliciozno umrežavanje bio je razvijan isključivo za *Unix/Linux* platforme. Onda je nastupio preokret i naglo kreće razvoj agenata za Windows. To su bili prvi ozbiljni znaci sazrevanja malicioznih mreža i otvaranje puteva za njihovu komercijalizaciju.

### 3. TRENUTNO STANJE I TRENDovi

#### 3.1 Pet godina kasnije – ima li promena?

Nakon intenzivnog razvoja u toku prve tri godine, tehnologije i tehnike demonstrirane u nizu parcijalnih *Proof of Concept* produkata razvile su se do nivoa koji je omogućavao prelazak u novu, ozbiljniju fazu. Iz napred izloženog je vidljivo da su još krajem 2001. na sceni bili prepoznati vrlo sofisticirani mehanizmi za sve faze u životnom ciklusu jedne univerzalne maliciozne mreže:

- Automatizovan izbor žrtve za ulogu agenta i/ili hendlera. Ručna selekcija ustupa mesto izboru na slepo – uglavnom usmerenom na vulnerabilne *Windows* računare

- Automatizovana propagacija na bazi višestrukih vektora napada (*mail attachments, backdoors, file sharing, exploiting vulnerabilities*, itd)
- Komandno-kontrolni saobraćaj zaštićen simetričnom enkripcijom
- Upotreba standardnog i vrlo pogodnog protokola u komandno-kontrolne svrhe - *IRC*
- Raznovrstan napadački saobraćaj – *TCP SYN, TCP ACK, UDP, ICMP, SMB* itd.

Dakle, već 2001. godine imali smo sve raspoložive elemente za izgradnju pouzdane i bezbedne, uz to potpuno automatizovane zlonamerne mreže koja radi na najpopularnijem i najšire rasprostranjenom operativnom sistemu.

Kako, onda, stvari stoje danas?

Pokret koji je započeo 2001. trajno je napadačima pomerio ciljnu grupu na tzv. obične, male korisnike. Danas je sve češća pojava da čak obična domaćinstva formiraju čitave računarske mreže od dva i više računara, te da se na Internet povezuju širokopojasnim pristupnim mrežama.

Po pravilu, nivo edukacije i svest o problematici informatičke sigurnosti kod ovih korisnika su vrlo niski. Pored domaćinstava, po niskom nivou informatičke zaštite u ovu grupu, nažalost, spadaju i mnoga mala preduzeća, agencije, biro, ambulante i sl. Provajderi internet usluga o njima ne vode posebnu brigu. Ova klasa korisnika najčešće problematiku zaštite percipira kroz magloviti osećaj da ih niko neće ni napasti, pošto njihova informatička imovina – podaci, oprema i drugo – uglavnom nema neku veliku vrednost. Stoga je kod njih informatička sigurnost veoma slabo održavana ili uopšte ne postoji (*Antivirus Updates, Firewall, Patches...*). Činjenica da se kod ovakvih korisnika najčešće sreće takozvana „informatička monokultura“ (*Windows, MS Office Internet Explorer, Outlook Express, Windows Media Player* itd) još više ih čini podložnim velikom broju različitih automatskih napada.

### 3.2. Razmere problema – kolike su i mogu li se sagledati?

Danas je sasvim uobičajeno da se sreću maliciozne mreže sastavljene od više stotina hiljada računara. Danas je, takođe, sasvim uobičajeno da se na „crnom“ tržištu iznajme, uz finansijsku nadoknadu, čitave armije zombija na određeno vreme. Motivi za „uzgajanje i održavanje“ malicioznih mreža više nisu istraživački duh ni intelektualna hakerska radoznalost. Maliciozne mreže danas imaju snagu oružja u elektronskom ratovanju i ogroman komercijalni potencijal. Ciljevi njihovih organizatora i vlasnika sve češće su u stvaranju profita. Sledeći statistički podaci iz 2004. [15][16] najbolje svedoče o razmerama problema:

- Na Internetu postoji preko 1.000.000 zombija
- Broj malicioznih mreža je veći od 30.000
- Procenjuje se da je preko 25% inficiranih računara pod kontrolom hakera
- Širokopojasne mreže su odgovorne za porast broja inficiranih računara od 93% u 2004.
- Na honeynet.org je registrovano 226.585 jedinstvenih IP adresa logovanih samo na jednom od *IRC C&C* kanala
- Prosečna veličina pojedine mreže je oko 2000 zombi kompjutera
- Maksimalna veličina pojedine mreže se može samo naslutiti; Holandska policija je u jednoj akciji 2005. godine razbila mrežu od 100.000 zombi računara [17]

### 3.3 Novi „igrači” na terenu

Danas na „botnet sceni” praktično nema ni jednog igrača iz perioda 1999 – 2001. Svaki pokušaj da se uspostavi maliciozna mreža nekim od alata iz tog vremena danas bi bio krajnje neefikasan ako ne i potpuno nemoguć. Današnji alati svojom funkcionalnošću daleko premašuju sve pretpostavke koje su se na tu temu mogle izneti pre samo par godina. U daljem tekstu dajemo kratak opis nekoliko malicioznih mreža registrovanih u toku 2005.-2006.

- **Agobot/Phatbot/Xtrembot:** Ovo je verovatno do danas najpoznatiji od svih tipova softvera za razvoj malicioznih mreža. [18] Na listama antivirusnih signatura postoji više od 500 različitih verzija ovog softvera, pri čemu taj broj stalno raste. Izvorni kod je pisan u jeziku C++ i stavljen je u javni domen pod *GPL* licencom. Autor je jedan mladi Nemač, poznat pod pseudonimima *Ago* i *Wonk*, koji je uhapšen u maju 2004. godine pod optužbom za kompjuterski kriminal. Kod je, za razliku od drugih hakerskih alata, pisan veoma čisto i pregledno i predstavlja veoma reprezentativan primer apstraktnog dizajna. Ovaj softver je verovatno i najsavršeniji maliciozni kod napisan do današnjeg dana. Njegova struktura je modularna, tako da je dodavanje novih funkcija i komandi lako izvodljivo. S obzirom da je kod objektno orijentisan, većinu izmena je moguće napraviti prostim ekstenzijama na već postojećim klasama. Agobot u sebi ima snifer (*sniffer*) za prisluškivanje i analizu saobraćaja, baziran na *libpcap* biblioteci i *PCRE* (*Perl Compatible Regular Expressions*). Koristi *ADS* (*Alternate Data Streams*), nedovoljno poznato i slabo dokumentovano svojstvo *NTFS* fajl-sistema, kao jedno od sredstava za svoje skrivanje. Takođe, sposoban je za tzv. „sakrivanje procesa” (*Process Hiding*), po čemu je ravan najboljim *rootkit* alatima. Ova dva svojstva ga čine skoro nemogućim za detekciju. Agobot ima sposobnost da detektuje prisustvo tzv. „dibagera” (*debuggers*, na pr. *SoftICE*, *OllyDbg* i sl.), kao i virtuelnih mašina (*VMWare*, *VirtualPC*) tako da je veoma otporan na reverzni inženjering. Jedna od varijanti Agobota koristi *WASTE Chat* kao kanal za komunikaciju. Uz sve to, posebna varijanta Agobota, pisana za *Linux* sposobna je da detektuje *Linux* distribuciju na kojoj trenutno radi i da onda izabere odgovarajuću skriptu za inicijalizaciju.
- **SDBot/RBot/UrXBot:** Ovo takođe nije jedan, već cela familija malicioznih programa. [19] Tokom 2005. godine ovaj softver je bio dugo na „*Top 10*” listi većine proizvođača antivirusnih programa. Kod u programskom jeziku *C* u kojem je *SDBot* pisan prilično je loš, što je lako zaključiti jer je kod otvoren i licenciran pod *GPL* licencom. Dizajn takođe nije u rangu Agobota; iako su mu funkcije dosta slične, skup komandi nije tako širok niti im je implementacija toliko sofisticirana. Bez obzira na to *SDBot* je doživeo veliku popularnost kod napadača i zabeležio veliki broj „naslednika” kao što su *RBot*, *RxBot*, *UrBot*, *UrXBot*, *JrBot* itd.
- **Botovi zasnovani na programu mIRC – tzv. GT-Bots:** *mIRC* je klijentski program za *IRC* koji je veoma popularan kod *Windows* korisnika. *GT* je skraćenica od *Global Threats*, što je opšti naziv za sve botove koji koriste *IRC*. Zbog toga se za celu kategoriju *IRC* botova koristi zajednički naziv *GT-Bots*. [19] Njih ima toliko da bi svaki pokušaj detaljnije enumeracije i kategorizacije bio ne samo izvan obima ovog teksta već možda i sasvim nemoguć. Ovi botovi rade tako što pokrenu jednu skrivenu instancu programa *mIRC*, koju zatim koriste kao kanal za komandu i kontrolu. Tipičan znak njihovog prisustva je postojanje programa/procesa *HideWindow* koji služi za sakrivanje pokrenutog *mIRC* klijenta. Inače, ovakvi botovi u toku instalacije na zombi mašinu postavljaju niz specifičnih *mIRC* skripti (ekstenzija „*mrc*”) i niz biblioteka za dinamičko linkovanje (*DLL*) kojima se osnovnom *mIRC* programu značajno menja postojeća i dodaje nova funkcionalnost. Na taj način, *mIRC* klijentu postaju dostupne funkcije kao što su skeniranje mreže, otkrivanje novih „žrtava” i dalje širenje maliciozne mreže. Ovakvi botovi se zapravo šire eksploatacijom otkrivenih slabosti i prenosom sopstvenog koda dalje na

kompromitovane računare. Pri ovakvoj operaciji količina prenetog koda često prelazi 1Mb, što je takođe jedan od indikatora za prisustvo malicioznog umrežavanja.

- **The Dataspy Network X (DSNX):** Ovaj bot [20] je napisan u jeziku C++ i takođe je u javnom domenu, pod *GPL* licencom. Ima veoma fleksibilan *plug-in* interfejs koji napadaču omogućava jednostavno dodavanje novih skenera i modula za širenje kroz mrežu. Osnovna varijanta se distribuira bez modula za širenje, tako da je bez nekoliko dodatnih *plug-in* modula potpuno neupotrebljiva. Međutim, ovaj nedostatak ozbiljnom napadaču ne predstavlja posebno tešku prepreku. Postoji veliki broj dodatnih modula do kojih se relativno jednostavno može doći, među kojima su i moduli za *DDoS* napade, postavljanje skrivenih *web* servera, skeniranje portova itd...
- **Q8 Bots:** Osnovna varijanta, pod imenom *Q8Bot*, karakteristična je po ekstremno kompaktnom kodu, koji se sastoji od samo 926 linija u jeziku C. Pisan je za *Linux/Unix*, što ga izdvaja među savremenim botovima, koji su praktično svi pisani za *Windows*. Iako je veoma mali, u njemu se nalaze sve najbitnije funkcije jednog modernog bota: dinamičko ažuriranje skidanjem sadržaja sa *HTTP* servera, različiti *DDoS* napadi (*SYN* i *UDP Flood*), niz različitih izvršnih komandi itd. Osnovna verzija takođe ne poseduje instrumente za širenje, tj. prenos sopstvenog koda na druge zombije u mreži, tako da mora biti dopunjena radi pune funkcionalnosti.
- **Kaiten:** Slično prethodnom, i ovaj bot je veoma mali (čitav kod u jednom fajlu) i u osnovnoj varijanti se pojavljuje kao nepotpun – bez mehanizma za širenje. Takođe je pisan za *Linux*, i pošto se sadrži samo od jednog fajla lako ga je preneti na drugi računar i tamo kompajlirati – najčešće se kod „skine” sa udaljenog servera pogodnom komandom (*wget*) i kompajlira direktno na računaru žrtve. Ceo ovaj zadatak se lako kodira u običnom skript-fajlu. Kaiten ima veoma pogodan interfejs za rad sa udaljenosti (*remote shell*), tako da se traganje za daljim žrtvama može sprovoditi kroz *IRC*.

### 3. 4 Novi ciljevi, novi rizici

Kao što je već rečeno, prvi primeri zlonamernog umrežavanja bili su isključivo sposobni za izvođenje *DDoS* napada. Prvih nekoliko godina, razvoj je bio usmeren ka iznalaženju najboljih rešenja za automatsku propagaciju i širenje mreža. Traženi su načini da se hendleri i agenti osposobe za „crvoliko” kretanje od žrtve do žrtve, uz minimum učešća ljudskog faktora. U isto vreme, usavršavani su i načini za skrivanje počinilaca, komunikacioni kanali i drugo. U periodu od 2001.-2004. tehnologija je bila potpuno zrela za ispunjenje ambicioznijih ciljeva. Od tada pa do danas, registrovan je veliki broj potpuno novih primena ovakvih mreža. Ovde ćemo izneti najznačajnije među njima.

1. **Komercijalni DDoS napadi** – Postoje brojni dokumentovani primeri da su mreže bot računara komercijalno korišćene za izvođenje distribuiranih *DoS* napada. Operacija Federalnog istražnog iroa (*FBI*) izvedena pod imenom *Cyberslam* [21] iznosi slučaj dvojice hakera (*Jay R. Echouafni, Joshua Schichtel - EMP*), koji su odgovarali za niz incidenata u kojima je naneta šteta tuđim kompjuterskim sistemima. Njih dvojica su komandovali mrežom od oko 3000 tačaka, koja je korišćena za slanje masovnih e-mail poruka i za *DDoS* napade na *blacklist* servere. Jedan naručilac im je platio da izvedu *DDoS* protiv njegove konkurencije. Tom prilikom, infrastruktura globalno poznatog on-line sistema *Speedera* bila je izbačena iz rada, što je dodatno skrenulo pažnju javnosti na taj slučaj i ubrzalo njihovo hvatanje.
2. **Spamming** – neki botovi imaju sposobnost da na kompromitovanoj mašini podignu generički proksi tipa *SOCKS v4/v5*, za *TCP/IP* aplikacije (*RFC 1928*).

Posle toga, kompromitovana žrtva može da se koristi za posebne namene kao što je otpremanje neželjene pošte – e-mail spam. Takav proksi može da prosledi ogromne količine pošte koja se generiše od strane ogromnog broja botova u mreži. Pored toga, ovakav „servis” može da bude dodatno upotrebljen i za tzv. „žetvu e-mail adresa” - *e-mail address harvesting*, kao i za *phishing* i druge slične namene.

3. **Sniffing** – botovi mogu da imaju ugrađenu funkciju prisluškivanja i registrovanja mrežnog saobraćaja. Na mrežnom segmentu u kojem su instalirani, ovi sniferi detektuju i registruju osetljive sadržaje, kao što su korisnička imena i lozinke. U specijalnim slučajevima, kada je neki računar kompromitovan više od jednom (i tako postao član više botnetova u isto vreme) sniferska funkcija može jednom napadaču da otkrije osetljive delove komandno-kontrolnog saobraćaja drugog napadača. To pruža mogućnost za „preotimanje” i prisvajanje tuđih botova, što je dosta čest slučaj.
4. **Keylogging** – U slučaju da je komunikacija enkriptovana, snimanje saobraćaja ne može biti efikasan način za pribavljanje osetljivih informacija. U tom slučaju, botovi mogu da snimaju direktan ulaz sa tastature, klikove miša, sadržaje ekrana, sadržaj radne memorije ili lokalnih fajlova. U njima su često implementirani pametni algoritmi filtriranja, tako da se izbegne poplava nekorisnih informacija. Na primer, bot može biti podešen tako da reaguje na neke ključne reči i da tek tada započne registrovanje.
5. **Širenje malicioznog koda** – U najčešćem slučaju, botovi služe za propagaciju novih botova. Ako posedujemo malicioznu mrežu, možemo je upotrebiti za instalaciju neke potpuno nove mreže ili bilo kojeg drugog malicioznog softvera. Ovo je vrlo lako pošto većina botova ima module za *FTP* odnosno *HTTP download*. Ovakva mreža može da „lansira” novi virus ili *backdoor* veoma brzo, putem velikog broja e-mail poruka. Poznati virus *witty* [22] koji je napadao neke proizvode firme *ISS* lansiran je tako što su prvo e-mail porukama napadnute mašine na kojima uopšte nije bilo *ISS* softvera, pa je tek tada usledio konačni napad na glavnu metu (*ISS ICQ parsing protocol*).
6. **Instalacija oglašivača i BHO-a (Browser Helper Objects)** – Ovo je jedan od načina da se maliciozne mreže komercijalno upotrebe. Najpre se postavi web sajt sa oglasima. Operator ovog sajta zatim sklapa sporazum o „plaćanju klikova” na ovim oglasima. Uz pomoć maliciozne mreže može se proizvesti ogroman broj „klikova” za kratko vreme, čime se obezbeđuje velika zarada. Ovo se dalje može unaprediti „otmicom” brauzera na kompromitovanoj mašini (*browser hijacking*) nakon čega se odgovarajući „klikovi” dogode svaki put kada žrtva uključi brauzer.
7. **Zloupotreba Google AdSense servisa** – Ovaj servis pruža mogućnost korisnicima da na svoje sajtove postavljaju reklame u saradnji sa Google pretraživačem i na taj način zarade novac. Tipičan ugovor predviđa da se broje „klikovi” na ovim reklamama i da se za svakih, recimo 10.000 „klikova” plati određena suma. Botovi mogu biti upotrebljeni da automatski generišu lažne posete ovim reklamnim oglasima i da tako ostvare veliku zaradu.
8. **Napadi na IRC mreže** – Ovo je zapravo još jedna vrsta *DDoS* napada, samo specifična za *IRC* protokol. Mreža botova dobija zadatak da se priključe na neku *IRC* mrežu, tako što će svaki od njih priključiti na hiljade „klonova” istovremeno. Izabrana *IRC* mreža tako dobija ogroman broj korisnika u ogromnom broju kanala, i to sve odjednom – u takvom slučaju najčeći rezultat biva trenutni i potpuni otkaz servisa.
9. **Manipulisanje raznih on-line igara i glasanja** – Botovi mogu biti upotrebljeni za automatsko odazivanje na razna glasanja u cilju sticanja „izborne pobede” u korist željene strane. Slično je i sa popularnim igrima u kojima se igrači kandiduju za neku nagradu, gde se angažovanjem maliciozne mreže napadaču značajno podižu šanse za dobitak.

10. **Masovna krađa identiteta** – Kombinovanjem nekih od nabrojanih tehnika može se doći do sredstava za masovnu krađu identiteta, što je jedna od kriminalnih aktivnosti sa najvećom stopom rasta na Internetu. Botovi mogu kroz već opisani *spam* mehanizam da distribuiraju veliki broj tzv. *phishing* poruka. U ovim porukama se obično nalazi sadržaj čiji dizajn predstavlja vernu kopiju nekog autentičnog sajta. Najčešći primer je simulacija nekog bankarskog on-line servisa. Žrtva upada u zamku i, prateći instrukcije iz *phishing* poruke, umesto na sajt svoje banke zapravo dospeva na lažni sajt koji je postavio napadač. Ove lažne sajtove moguće je takođe postaviti putem mreže botova. U poslednjih par godina registrovani su ovakvi napadi na veliki broj korisnika bankarskih usluga, *eBay*, *PayPal* i mnogih drugih servisa na Internetu.
11. **Ilegalni servisi, „hostovanje” ilegalnih podataka** – Ovo je već dugo prisutan i rastući trend: kompromitovana mašina postaje deo mreže za razmenu ilegalnih podataka (piratizovani softver, filmovi, muzika, slike, pornografija itd.). Praktično svi IRC botovi su razvijeni tako da mogu da posluže kao komponente *file-sharing* mreže ili kao *FTP* serveri.
12. **„Ustupanje” propusnog opsega** – Botovi sa veoma brzim pristupom imaju veliki komunikacioni potencijal i veoma su atraktivni za razne hakerske potrebe. Vlasnik koji je spreman da ovakve botove stavi „kolegama” na raspolaganje može da očekuje odgovarajuću, često značajnu, finansijsku nadoknadu. Ovaj spisak demonstrira ogroman potencijal koji maliciozne mreže danas imaju. Rizici kojima se izlažu korisnici Interneta su ogromni, iako ne uvek tako očigledni. U slučaju malicioznog umrežavanja, žrtva se praktično uvek nalazi „prema prilici” a vrlo retko „prema izboru”. Međutim, kada god je moguće, napadači sužavaju svoj izbor na grupe računara u kojima je veća verovatnoća da će „naći dobru priliku”. Faktori koji na ovu verovatnoću direktno utiču su sledeći:
  - **Široki propusni opseg, brzi dostup Internetu:** Računari sa kablovskim ili ADSL pristupom predstavljaju veoma poželjnu metu, pre svega zbog široke upotrebljivosti. Ovakve računare je veoma lako pretvoriti u efikasne servere, a u slučaju izvođenja DDoS napada pružaju veliki amplifikacioni efekat.
  - **Raspoloživost:** Računari sa neprekidnom vezom prema Internetu, „visoko su cenjeni” kao meta napada, iz jasnih razloga.
  - **Niska svest korisnika, slab nadzor i održavanje:** Korisnici koji nemaju dovoljna znanja ili ne vode dovoljno računa o problematici informatičke sigurnosti posebno su laka meta napada. Propusti u redovnom ažuriranju operativnog sistema i aplikativnog softvera, prisustvo nepotrebnih servisa i odsustvo mera i sredstava zaštite pružaju priliku za instalaciju malicioznog softvera i za njegov dug i neprimećen rad.
  - **Lokacija:** Napadači uvek teže da svoje maliciozne mreže formiraju na geografski udaljenim lokacijama i to iz više razloga. Pre svega, time se otežava traganje za njima i eventualno otkrivanje. Dalje, ako se napadnuti računari nalaze u zemljama u kojima su zakonodavstvo i policija nedovoljno pripremljeni za ovu vrstu kriminala, to dodatno i u velikoj meri olakšava situaciju u kojoj se napadač nalazi.

## 4. STANJE U DOMAĆEM INTERNETU

Srbija se nalazi u fazi ubrzanog razvoja širokopojasnog Interneta. Kablovski, bežični i ADSL pristup je u poslednje vreme u velikoj ekspanziji.

Tipični korisnici su sve češće mala i srednja preduzeća i domaćinstva. To su upravo one korisničke kategorije kod kojih su prisutni praktično svi faktori koji stimulišu verovatnoću i uspeh napada: nizak nivo zaštite (bilo zbog nedostatka svesti i znanja,

bilo zbog nedostatka sredstava), kvalitetna infrastruktura (propusni opseg u rasponu od 256kbps do 1Mbps), sve češći neprekidan rad itd.

Sa druge strane, provajderi Internet usluga najčešće pružaju veoma slabu ili nikakvu zaštitu svojim korisnicima.

Usluge pristupa, koje obično idu „u paketu” sa uslugom elektronske pošte (i eventualno nekim prostorom na serveru za potrebe elementarnog web hostinga) praktično su potpuno nezaštićene od ovakvih napada. Jedina mera koja se standardno preduzima jeste antivirusna zaštita elektronske pošte, premda i to sa neujednačenim kvalitetom. Problem je u tome što je *e-mail* samo jedan od mnogobrojnih napadačkih vektora. Šta je sa ostalima? Korisnici dobijaju javne *IP* adrese. One se dodeljuju iz statičkih, nepromenljivih adresnih opsega, koji se lako otkrivaju. Čak i kada individualna adresa korisnika nije statička, uspešni napadi su i dalje realno mogući. Brzi uvid u nekoliko popularnih *ADSL* adresnih prostora otkrio je niz slabosti: nezaštićene *TCP* i *UDP* portove, nekorišćene a aktivne servise (uključujući i *file sharing*) itd. Situacija sa bežičnim pristupom je još mnogo gora – neke domaće mreže prosto „traže” da budu inficirane botovima.

Usluge *web* hostinga postoje već dugo, ali su i dalje relativno nerazvijene. Zbog toga je većina korisnika sa potrebama za ambicioznijim web aplikacijama još uvek sklona da svoje sajtove postavlja na serverima van Srbije. Domaći serveri još uvek većinom nose statičke i tehnološki ne previše napredne sajtove. Iako se neka tačna i objektivna ocena ne može dati bez ozbiljnog IT audita, ipak se stiče utisak da je stanje zaštite na serverima veoma neujednačeno i često u velikoj meri ispod poželjnog. Već jedan kratak i površan uvid koji je autor napravio za potrebe ovog teksta otkriva dosta lošu sliku.

Za domaći Internet se verovatno može reći da je nedostatak svesti i znanja još veći problem od nedostatka sredstava. Edukacija i konsultantske usluge u ovoj oblasti su još uvek veoma nerazvijene. Iako izvesna ponuda u ovoj oblasti postoji, ona je nedovoljna i po obimu i po kvalitetu.

Verovatno najteži problem u ovoj oblasti leži u tome što trenutno u Srbiji praktično nema konsaltinga koji je tehnološki nezavisan. Naime, bilo da se radi o potrebi ocene postojećeg stanja informatičke sigurnosti korisnika, analizi rizika i sl, bilo da se radi o iznalaženju rešenja za zaštitu – planiranju, dizajnu, izboru i implementaciji – korisnici su upućeni na nekog od isporučilaca hardvera ili softvera velikih svetskih proizvođača. Čak i tamo gde su prisutni znanje i stručnost, u većini slučajeva izostaje objektivnost. Usluge audita IT sigurnosti praktično se i ne nude, pre svega zbog nedostatka potražnje. U retkim slučajevima kada se ovakve usluge traže, obično se insistira na penetracionim testovima (*Pen-tests*) i tzv. „etičkom hakerisanju” što dodatno svedoči o tome kakva je dominantna percepcija ove problematike. Veliki broj tehničkih rešenja se zato svodi jednostavno na nabavku, pri čemu se briga o informatičkoj sigurnosti lako zamenjuje brigom o čistoj savesti.

Opšti zaključak bi bio da sa daljim razvojem širokopojasnog pristupa domaći Internet postaje veoma atraktivan kao poligon za maliciozno umrežavanje. Ukoliko se na taj trend na vreme ne obrati dovoljna pažnja, mogu se očekivati veoma štetne posledice.

## **5. ŠTA ČINITI ? NEKE MOGUĆNOSTI ZA DETEKCIJU I PREVENCIJU**

Tema zaštite od opasnosti koje donosi maliciozno umrežavanje je previše široka da bi mogla biti obrađena u jednom ovakvom tekstu. Veliki deo preventivnih mera predstavljaju zapravo generičke mere, mere opšteg karaktera, koje se odnose na informatičku zaštitu u celini. One su uglavnom dobro poznate, jer predstavljaju neizbežni deo razmatranja bilo kojeg aspekta informatičke sigurnosti uopšte. Ovde ih

možemo samo pomenuti bez dubljeg razmatranja, dok bi nešto više pažnje obratili na ono što je specifično upravo za same maliciozne mreže:

- Politike, procedure i uputstva
- Edukacija, obuka i trening
- IT audit – redovna provera IT sigurnosti
- Redovno održavanje IT sigurnosti, posebno *Patch Management*
- Primena adekvatnih tehnoloških rešenja – *Firewalls, Anti-Virus, IDS/IPS* itd.  
Pored toga, evo nekih specifičnih anti-bot i anti-DDoS rešenja i strategija:
- **Egress Filtering** – Ovo je tehnika kojom korisnik ne štiti sebe od drugih već druge od sebe. Kada bi (hipotetički) sve korisničke mreže na Internetu pravilno isfiltrirale svoj odlazni saobraćaj, problemi sa zlonamernim mrežama bi verovatno skoro potpuno nestali. Ako ništa drugo, praktično bi bio eliminisan *IP Spoofing* kao jedan od stubova na kojima počivaju današnje bot-mreže. Nažalost, ovo se masovno potcenjuje i gubi iz vida pri konfigurisanju i administriranju korisničkih graničnih rutera
- **Service Level Agreements** – Korisnici i provajeri usluga generalno previđaju pitanja informatičke sigurnosti prilikom stupanja u poslovne odnose. Čak i onda kad to nije slučaj, previše su fokusirani na tehnološka pitanja, kao da se pitanje IT sigurnosti može rešiti isključivo kroz izbor tehnologije. Međutim, dobro formulisani zahtevi u jednom ugovoru o nivou usluga mogu često biti daleko bolja i efikasnija mera zaštite nego, recimo, jedan loše konfigurisan paketski filter.
- **DNS** – Ovaj protokol je verovatno najosetljivija tačka stabilnosti i bezbednosti svake mreže, pa i Interneta u celini. Savremeni botovi se služe uslugama dinamičkih *DNS* servisa, što im daje mogućnost da se kontrolni centri sele sa adrese na adresu a da pritom zadrže ista imena. Ova činjenica je dobro poznata i moguće ju je iskoristiti protiv napadača na veoma jednostavan i efikasan način. Potrebno je da korisnik postojeću konfiguraciju svojih *DNS* servera redovno dopunjava tako što će *DNS* imena poznatih botnetova usmeriti na nepostojeće *IP* adrese. Ova tehnika se zove *nullrouting* ili *sinkhole* i može veoma mnogo da pomogne u sprečavanju ili ograničavanju efekata bot infekcija.
- **Honeypots, Honeynets** – Postavljanje pojedinačnih ili umreženih sistema koji simuliraju određene slabosti i tako privlače napadače pokazalo se kao veoma uspešna strateško – taktička aktivnost. Ovakvi sistemi registruju čitave tokove napada i daju analitičarima materijal od neprocenjive vrednosti. Mnogi savremeni botovi otkriveni su na taj način. U svetu je već duže aktivna zajednica *Honeynet.org* koja okuplja pojedince i organizacije i u okviru koje oni sarađuju na razvoju i praktičnoj primeni ovakvih sistema. Nedavno je i u Srbiji registrovano jedno takvo udruženje, što nam trenutno daje lidersku poziciju u odnosu na neposredno okruženje. Vreme će pokazati da li ćemo biti u stanju da to i održimo.
- 

## 6. ZAKLJUČAK

Iz izloženog se vidi da su sredstva i tehnike za maliciozno umrežavanje za relativno kratko vreme prešli razvojni put od sporadičnog i incidentnog do veoma široko rasprostranjenog i izuzetno moćnog sredstva u rukama kompjuterskih kriminalaca za nanošenje štete i sticanje direktne koristi. U tekstu je učinjen napor da se neki prividno nepovezani primeri različitog malicioznog softvera posmatraju i prikažu kao faze u razvoju jedne složene i vrlo sofisticirane napadačke tehnologije. Takođe, skrenuta je pažnja na postojeću opasnost da mere i sredstva zaštite u dovoljnoj meri ne prate ovaj razvoj, te da je prisutan veliki rizik od rastućeg zaostajanja u tom pogledu, posebno u domaćim uslovima.

## 7. REFERENCE

1. <http://staff.washington.edu/dittrich/misc/trinoo.analysis.txt>
2. <http://staff.washington.edu/dittrich/misc/tfn.analysis>
3. [http://news.zdnet.com/2100-9595\\_22-518461.html](http://news.zdnet.com/2100-9595_22-518461.html) (Mixer Interview for ZDNet)
4. <http://staff.washington.edu/dittrich/misc/stacheldraht.analysis>
5. <http://staff.washington.edu/dittrich/misc/mstream.analysis.txt>
6. [http://packetstormsecurity.org/distributed/TFN2k\\_Analysis-1.3.txt](http://packetstormsecurity.org/distributed/TFN2k_Analysis-1.3.txt)
7. <http://rr.sans.org/malicious/trinity.php>
8. <http://www.sophos.com/virusinfo/analyses/vbsloveleta.html>
9. <http://www.securityfocus.com/infocus/1230>
10. [http://linux.tfmgroup.ro/index.php/Ramen\\_Worm\\_Analysis](http://linux.tfmgroup.ro/index.php/Ramen_Worm_Analysis)
11. <http://www.auscert.org.au/render.html?it=94>
12. <http://www.sophos.com/virusinfo/analyses/trojsubseven.html>
13. <http://www.caida.org/analysis/security/code-red/>
14. <http://www.caida.org/dynamic/analysis/security/nimda/>
15. [http://arachnid.homeip.net/papers/VB2005-Bots\\_and\\_Botnets-1.0.2.pdf](http://arachnid.homeip.net/papers/VB2005-Bots_and_Botnets-1.0.2.pdf)
16. <http://news.bbc.co.uk/1/hi/technology/4579623.stm>
17. [http://www.theregister.co.uk/2005/10/07/dutch\\_police\\_smash\\_zombie\\_network/](http://www.theregister.co.uk/2005/10/07/dutch_police_smash_zombie_network/)
18. <http://www.infectionvectors.com/vectors/kitchensink.htm>
19. <http://swatit.org/bots/>
20. [http://www.symantec.com/security\\_response/writeup.jsp?docid=2002-013013-1836-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2002-013013-1836-99&tabid=2)
21. [http://www.theregister.co.uk/2004/08/27/ddos\\_mafia\\_busted/](http://www.theregister.co.uk/2004/08/27/ddos_mafia_busted/)
22. <http://www.netsecure.shawbiz.ca/witty-analysis.html>
23. <http://www.honeynet.org>