Centar Informacijske Sigurnosti

Botnet mreže

lipanj 2011.

CIS-DOC-2011-09-026

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

Preuzimanje nadzora nad tuđim računalom ili barem dijelom njegovih resursa nekad je bilo motivirano samo stjecanjem statusa među prijateljima i drugim računalnim entuzijastima. Danas je, međutim, situacija podosta drugačija. Napade na računala i računalne sustave više ne izvode adolescenti željni pažnje, s osobnog računala u svojoj sobi. Računalni kriminal postao je unosan posao, a preuzimanje nadzora nad tuđim računalom, odnosno stvaranje cijelih mreža takvih „otetih" računala, poznatijih kao botnet, je potencijalno najunosniji vid takvog kriminala. Motivi za preuzimanje nadzora nad cijelim mrežama računala, odnosno izvođenju napada sa tih mreža na druge računalne sustave nekad nisu samo financijske prirode. Sve češći su i napadi okarakterizirani kao teroristički napadi, a zabilježeni su i napadi pokrenuti sa botnet mreže na neku tvrtku čisto iz osvete.

U ovom dokumentu biti će više riječi o botnet mrežama, koje su poznate još i pod imenom „vojska zombija" (eng. *zombie army*), načinu na koji rade i najčešće svrhe za koje se koriste, te vjerojatnim smjerovima razvoja same arhitekture takvih mreža.

2. Općenito o botnet mrežama

Procesorska snaga i računalni resursi općenito, mogu biti povećani umrežavanjem računala. Iako svako pojedino računalo nema impresivnu snagu, čak je možda i pomalo zastarjelo, svejedno doprinosi ukupnoj snazi tako dobivenog grozda[1] računala (eng. *cluster*). Samo višak procesorskog vremena na svim tim računalima mogao bi dostići snagu mjerljivu u Teraflopima (jedan Teraflop je trilijun operacija sa pomičnom točkom u sekundi), što naravno ovisi o količini računala u botnet mreži.

Važno je napomenuti da postoje legalne i legitimne mreže sa sličnim svojstvima, a glavna razlika je pristanak vlasnika računala da sudjeluje u toj mreži te preda višak svojih računalnih resursa na korištenje „vlasniku“ mreže. Takve mreže računala, odnosno njihova procesorska snaga se većinom koriste u znanosti prilikom obrade podataka nekih istraživanja. I to je neka vrsta botnet mreže, odnosno samo računalo te osobe je bot (skraćenica od robot) odakle dolazi i naziv botnet za tako umrežena računala (eng. *net* je mreža). Ovdje svakako treba spomenuti najpoznatiju takvu mrežu, SETI (eng. *Search for Extraterrestrial Intelligence*) koja je sastavljena od preko 500 000 upaljenih računala u svakom trenutku te mrežu distributed.net.

http://www.distributed.net/Main_Page

http://setiathome.berkeley.edu/

SETI koristi računalnu snagu umreženih računala za istraživanje svemira, točnije, obradu signala dobivenih radio teleskopima usmjerenim prema nebu. Mreža distributed.net koristi tu snagu za nekoliko istraživanja, a prvenstveno su to istraživanja sa područja matematike.

2.1. Botnet mreže nekad

Sami počeci zlonamjernog korištenja botnet mreža sežu do 2000. Godine. Tada je računalni entuzijast, poznat pod imenom Mafiaboy, iskoristio prvu sličnu mrežu zaraženih računala da izvede distribuirani napad uskraćivanjem usluga (eng. *Distributed Denial-of-Service*, DDoS). Napad je izveden na internetske stranice tvrtki CNN, Amazon eBay i Dell. Distribuirani napad uskraćivanjem usluga se radi na način da svako računalo kojim napadač upravlja pošalje zahtjev na određenu stranicu odnosno poslužitelj. Veliki broj takvih zahtjeva poslanih odjednom može preopteretiti poslužitelj i onemogućiti drugim korisnicima usluge koje on nudi. Kako tvrtke sve više ovise o uslugama koje pružaju korisnicima preko Interneta, nedostupnost njihovih poslužitelja može im nanijeti značajne financijske gubitke.

2.2. Botnet mreže danas

Danas je puno veća vjerojatnost da iza neke botnet mreže stoji kriminalna organizacija, a ne skupina računalnih entuzijasta. Glavni razlog tome je razlika u motivaciji, dok su prije 2000. godine botnet mrežama upravljali entuzijasti željni slave te ih koristili za međusobno „ratovanje“ i nadmetanje, danas je glavna motivacija profit. Botnet mreže se danas najčešće koriste za četiri vrste napada, a to su:

- Distribuirani napad uskraćivanjem usluga,
- slanje velikih količina neželjene elektroničke pošte (eng. *SPAM*),
- pokušaj krađe identiteta i privatnih korisničkih podataka (eng. *phishing*), te
- prevare klikom (eng. *Click fraud*).

[1] Grozd (eng. *cluster*) je skupina povezanih računala, najčešće brzom lokalnom mrežom, u svrhu povećanja performansi ili dostupnosti tako dobivenog „jednog računala“.

2.2.1. Distribuirani napad uskraćivanjem usluga

Svaki poslužitelj ima neku granicu propusnosti podataka, odnosno kapacitet koliko najviše radnji može napraviti u određenoj jedinici vremena. Ako se ta granica pređe, poslužitelj se može srušiti, odnosno postati nedostupan ili barem prespor za normalno korištenje. U današnje vrijeme većina tvrtki ovisi o svom „*on-line*“ identitetu, odnosno dostupnosti barem osnovnih informacija o tvrtki na Internetu. Štoviše, velik broj tvrtki obavlja barem dio svojih djelatnosti preko Interneta. U današnje vrijeme, obavlja se i većina financijskih transakcija preko Interneta.

Iz svega navedenog očito je da je danas svakoj tvrtki važna dostupnost, odnosno ispravan rad njihovog poslužitelja ili poslužitelja tvrtke koja za njih drži web stranice ili obavlja financijske usluge. Prilikom distribuiranog napada uskraćivanjem usluga, upravitelj botnet mreže naredi svim računalima koje nadzire, odnosno svim računalima u mreži da pristupe određenoj Internet stranici, usluzi, odnosno poslužitelju u isto vrijeme. Na taj način, ovisno o broju računala koja nadzire, ozbiljno ugrozi rad tog poslužitelja. Financijska motivacija iza ovakve vrste napada najčešće je iznuda novca od napadnute tvrtke za prestanak takvih napada. Međutim moguć je i scenarij u kojem konkurentska tvrtka plati napadačima oštećivanje konkurencije zbog povećanja svog tržišta ili neke vrste odmazde.

Distribuirani napad uskraćivanjem usluga korištenjem botnet mreže biti će detaljnije opisan u poglavlju [4.2.2].

2.2.2. Neželjena elektronička pošta

Zaražena računala pod nadzorom kriminalaca često se koriste i za slanje neželjene elektroničke pošte. Financijska korist ovakve vrste napada krije se u sadržaju te neželjene pošte. Naime, ona se najčešće koristi kao sredstvo marketinga određenog proizvoda, a prema istraživanju Sveučilišta u Kaliforniji, provedenom 2008. godine, uspješnost reklamiranja preko neželjene elektroničke pošte iznosi 0,00001%. Koliko god se ta brojka čini malena, kada se uzme u obzir količina neželjene pošte koju najveće botnet mreže, zvane i spambotovi, mogu poslati u jednom danu te cijenu reklamiranog proizvoda, dolazimo do dnevne zarade od preko 400 000 američkih dolara. Štoviše, prema riječima istraživača, većina spambotova, odnosno botnet mreža korištenih za slanje neželjene elektroničke pošte ima uspješnost od oko 2%, a najveći botnet koji se koristi za slanje neželjene elektroničke pošte, Cutwail, može poslati 74 milijarde neželjenih poruka na dan.

Svakako treba napomenuti da proizvod naveden u poruci ne postoji, te da se njegovom „kupnjom“ ustvari financira daljnje slanje neželjene pošte, odnosno kriminal.

Detaljniji primjer stvaranje botnet mreže i njenog korištenja za slanje neželjene elektroničke pošte biti će opisan i prikazan u poglavlju [4].

2.2.3. Krađa identiteta

Većina računala u botnet mreži je zaražena i nekom vrstom zlonamjernog programa koji prati aktivnost korisnika. Takvi programi poznati su i pod imenom (eng.) *spyware*. Ti programi su napisani tako da prate unos korisničkih podataka sa tipkovnice, a napadačima su prvenstveno zanimljive financijske transakcije, odnosno financijski podaci korisnika. Nakon krađe korisnikovih pristupnih podataka određenim financijskim uslugama, kao što je internet bankarstvo, PayPal ili broj kreditnih kartica taj program ih šalje upravitelju botnet mreže te on ima pristup financijama zaraženog korisnika.

2.2.4. Prevare klikom

Popularnost određenih Internet stranica i usluga se, između ostalog, mjeri i brojem posjeta tim stranicama. Prilikom prevare klikom, upravitelj botnet mreže pokušava umjetno podići popularnost određene stranice tako da naredi velikom broju računala da posjete tu stranicu, stvarajući prividno veliki interes za njenim sadržajem. Također, vlasnik te stranice može

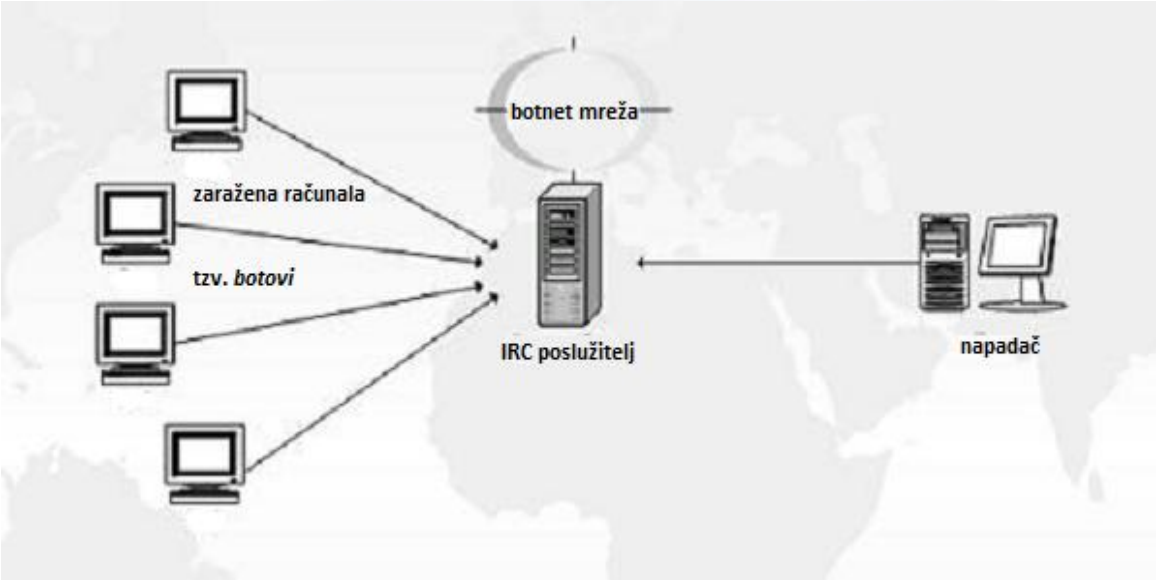
zarađivati oglašavanjem drugih tvrtki, i plaćen je po posjetu stranici, odnosno broju prikazivanja reklama.

S druge strane, ovakve prevare mogu biti korištene na financijsku štetu tvrtkama koje su žrtve napada. Kako, većina oglašavanja na Internetu funkcionira po principu naplate po broju prikaza ili posjeta, tvrtka plaća oglašivaču samo broj prikazivanja svog oglasa, a ne neku fiksnu cijenu. Botnet mreže mogu biti iskorištene za prikaz i posjet takvih oglasa, koštajući tvrtku koja se oglašava na taj način.

3. Arhitektura botnet mreža

3.1. Začeci botnet mreža

Od samih začetaka, odnosno genijalne ideje da se za komunikaciju i upravljanje drugim računalima iskoristi protokol za razgovor putem Interneta (eng. *internet relay chat,* IRC), napadači se prvenstveno oslanjaju na tu vrstu komunikacije u botnet mreži. Protokol IRC je razvijen za komunikaciju korisnika na forumima, masovnim porukama ili privatnim porukama, u stvarnom vremenu odnosno bez kašnjenja, stoga je posebno pogodan za izdavanje naredbi većem broju računala u istom trenutku. Napadač koji želi preuzeti nadzor nad drugim računalima, postavi jedno računalo kao IRC poslužitelj te ga koristi za komunikaciju sa drugim zaraženim odnosno ranjivim računalima. Preko tog poslužitelja napadač ustvari upravlja botnet mrežom, kako je prikazano na Slici 1.



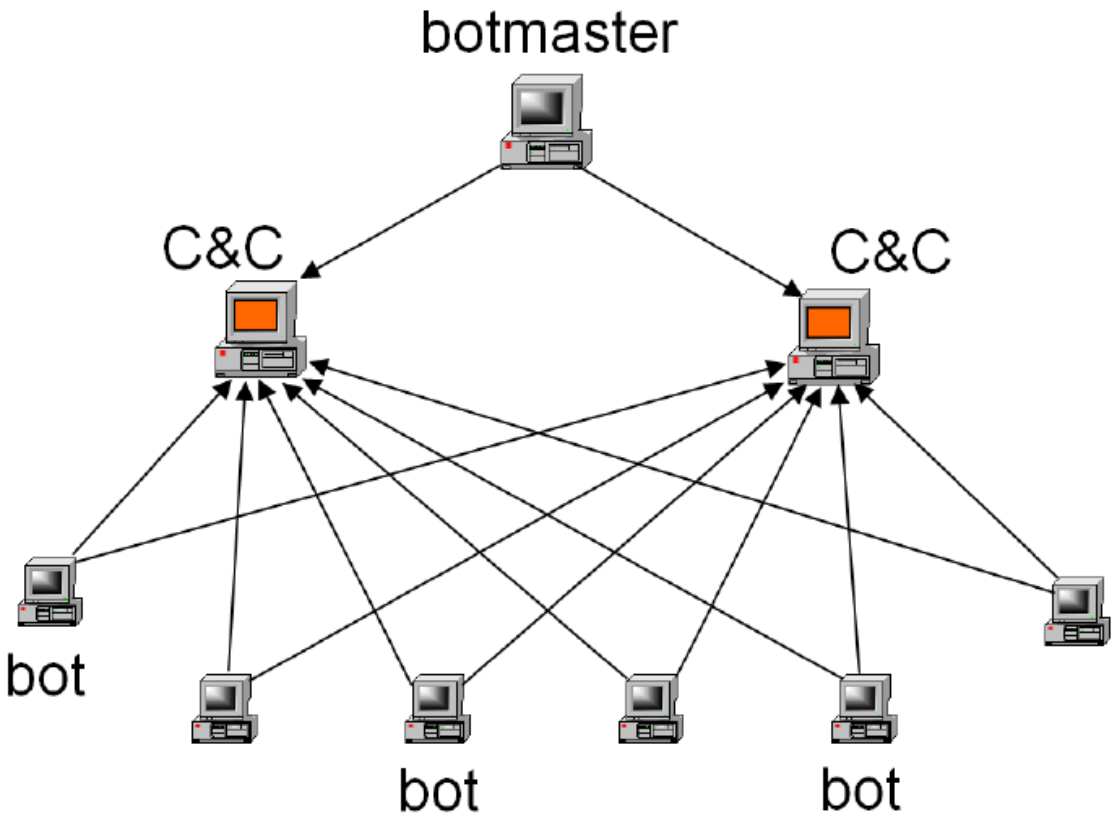
Slika 1. *Arhitektura botnet mreže*

Izvor: *Laboratorij za sustave i signale (LSS)*

3.2. Moderna arhitektura botnet mreža

U današnje vrijeme upravitelji botnet mreža, poznati i pod engleskim nazivima *botherder* ili *botmaster*, još uvijek primarno koriste neku vrstu protokola IM (eng. *instant messaging*) za upravljanje botnet mrežom, odnosno protokola za komunikaciju u stvarnom vremenu. Kako se ti protokoli koriste na većini socijalnih mreža, onemogućavanje tih protokola za zaštitu računala nije primjenjivo u većini slučajeva. Također se koristi i „klasičan“ komunikacijski protokol HTTP (eng. *Hypertext Transfer Protocol*) preko kojeg se odvija većina www (eng. world wide web) prometa na Internetu. Pritom sama arhitektura botnet mreža nije bitno promijenjena, međutim ono po čemu se današnje botnet mreže razlikuju od onih prije nekoliko godina jest redundantnost. Naime, *botmasteri* koriste dva, tri ili više poslužitelja za komunikaciju sa cijelom mrežom zaraženih računala. Arhitektura botnet mreže koja koristi dva komunikacijska poslužitelja prikazana je na slici 2, a lako se može zamisliti mreža sa više od dva takva poslužitelja. Ti poslužitelji poznati su još pod kraticom C&C koja dolazi od engleskih riječi za naredbe i kontrolu (eng. *command and control*). Više C&C poslužitelja se koristi za slučaj da neki budu otkriveni odnosno iz bilo kojeg drugog razloga nedostupni. U tom slučaju, bez dodatnih

poslužitelja, botnet mreža bi i dalje postojala, međutim nitko ne bi imao nadzor nad njom te ne bi mogao njome upravljati zbog nemogućnosti podjele zadataka zaraženim računalima.



Slika 2. *Arhitektura botnet mreže sa dva upravljačka poslužitelja*

Izvor: *Usenix*

4. Primjer botnet napada

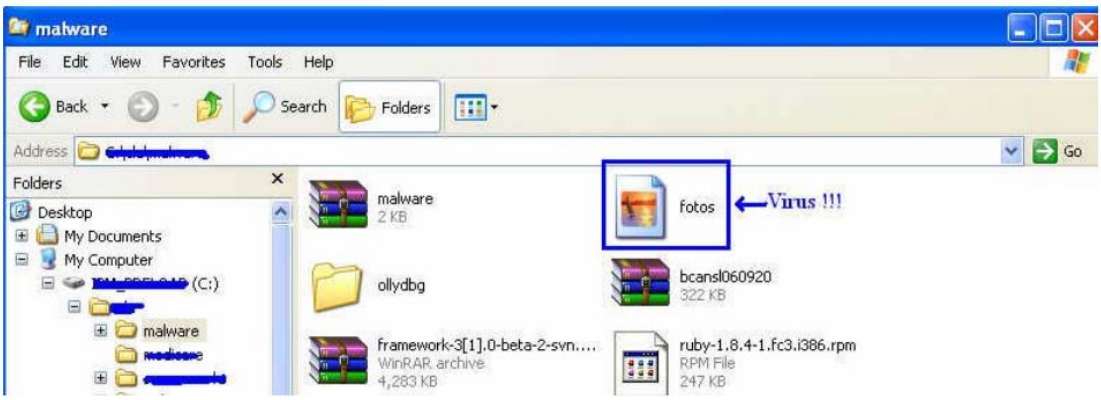
Važno je napomenuti da se upravitelji botnet mreža najčešće ne bave drugim vrstama kriminala, oni samo iznajmljuju računalne resurse zaraženih računala drugim kriminalnim organizacijama. Na taj način izbjegavaju kriminalnu odgovornost za ilegalne radnje za koje su botnet mreže iskorištene.

4.1. Stvaranje botnet mreže

Napadač, nakon postavljanja poslužitelja za upravljanje botnet mrežom kreće u „regrutaciju“ računala za botnet mrežu. Računala korisnika koja postanu dio botnet mreže najčešće ne sadrže posljednje sigurnosne zakrpe za operacijski sustav ili odgovarajući program za zaštitu računala. Postoje dva načina na koji se zlonamjerni program, odnosno klijent za botnet mrežu (bot) učitava na takvo računalo. Prvi od njih zahtjeva korisničku interakciju, odnosno napad računalnim virusom. Drugi način je napad računalnim crvom koji ne zahtjeva nikakvu korisničku interakciju, a sposoban je sam se dalje širiti.

4.1.1. Zaraza računala virusom

Računalni virus je vrsta zlonamjernog programa za računalo koji za svoje širenje treba datoteku domaćina, koja, da bi se zaraza proširila, treba biti otvorena. Najčešće virusi dolaze kao lažne fotografije, video ili tekstualne datoteke odnosno datoteke programa Microsoft Word, kako je prikazano na slici 3. Najčešće se šire socijalnim mrežama ili elektroničkom poštom, a koriste senzacionalističko ime ili opis, nešto kao: „ovo je presmiješno“, „moraš ovo vidjeti“ i slično.



***Slika 3.** Primjer lažne slike*

***Izvor:** CARNet CERT*

Ovakvom načinu zaraze računala dodatno pogoduju podrazumijevane postavke operacijskog sustava Windows, što se tiče sakrivanja troslovnih oznaka poznatih vrsta datoteka. Naime ova datoteka je punim imenom fotos.exe, gdje .exe dodatak označava izvršnu datoteku operacijskog sustava Windows. Prilikom pokušaja otvaranja te datoteke, korisnik će ustvari pokrenuti program fotos.exe koji će otvoriti komunikacijske kanale sa upravljačkim poslužiteljem botnet mreže. Taj program će tada svoju kopiju poslati svim korisnikovim kontaktima, bilo preko socijalne mreže ili elektroničke pošte te tako dalje širiti zarazu.

4.1.2. Zaraza računala crvom

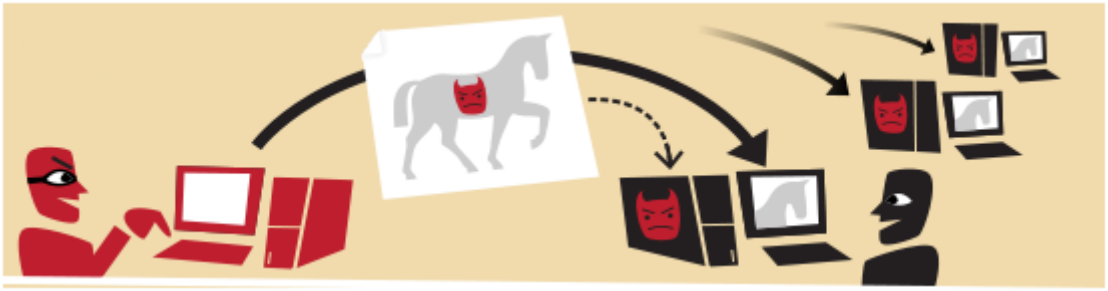
Računalni crv je vrsta zlonamjernog programa koji je sposoban sam širit zarazu, odnosno sposoban je „razmnožavati“ se bez korisnikove interakcije. Najčešće mrežom odnosno Internetom, ali može se kopirati i na vanjske memorije te tako nalaziti nova računala.

Ovo je učestaliji način širenja bot klijenata u posljednje vrijeme, a nakon uspješne zaraze odnosno instalacije na žrtvino računalo, crv provjerava mrežu za druga ranjiva računala na koja bi se mogao proširiti i instalirati bot klijent.

4.1.3. Primjer stvaranja botnet mreže

Na sljedeće dvije slike biti će prikazan i opisan način na koji napadač pokreće jednu botnet mrežu, od zaraze potencijalnih botova do uspostave komunikacijskog poslužitelja.

1. Napadač uspijeva proširiti zlonamjerni program (virus ili crv) koji će instalirati bot klijent na zaražena računala (slika 4).



Slika 4. *Širenje zaraze na potencijalne botove*

Izvor: *Wikipedia*

2. Nakon uspješne instalacije bot klijenta, zaražena računala se uspješno spajaju na upravljački poslužitelj te čekaju daljnje naredbe upravitelja botnet mreže (slika 5).

Slika 5. *Spajanje zaraženih računala na upravljački poslužitelj botnet mreže*

Izvor: *Wikipedia*

4.2. Napad botnet mreže na druge poslužitelje

Nakon uspješnog uspostavljanja botnet mreže, kako je opisano u poglavlju [4.1] tek sada slijede kriminalne radnje za koje je ona uspostavljena. Osim već opisane krađe podataka od vlasnika

zaraženih računala, te radnje najčešće uključuju iskorištavanje računalne moći mreže zaraženih računala, botova.

Upravitelj botnet mreže najčešće iznajmljuje računalnu snagu zaraženih računala, ili prodaje ukradene financijske podatke korisnika, drugim kriminalnim organizacijama sa specifičnim ciljevima.

4.2.1. Slanje neželjene elektroničke pošte

U našem primjeru, nakon uspješnog uspostavljanja botnet mreže, upravitelj mreže će iznajmiti svoje usluge (slika 6) trećoj strani, zainteresiranoj za reklamiranje svog lažnog i nepostojećeg proizvoda neželjenom elektroničkom poštom (slika 7).

1. Upravitelj botnet mreže prima narudžbu za posao koji zahtjeva upravljanje botnet mrežom.

Slika 6. *Iznajmljivanje botnet mreže za obavljanje kriminalnih radnji*

Izvor: *Wikipedia*

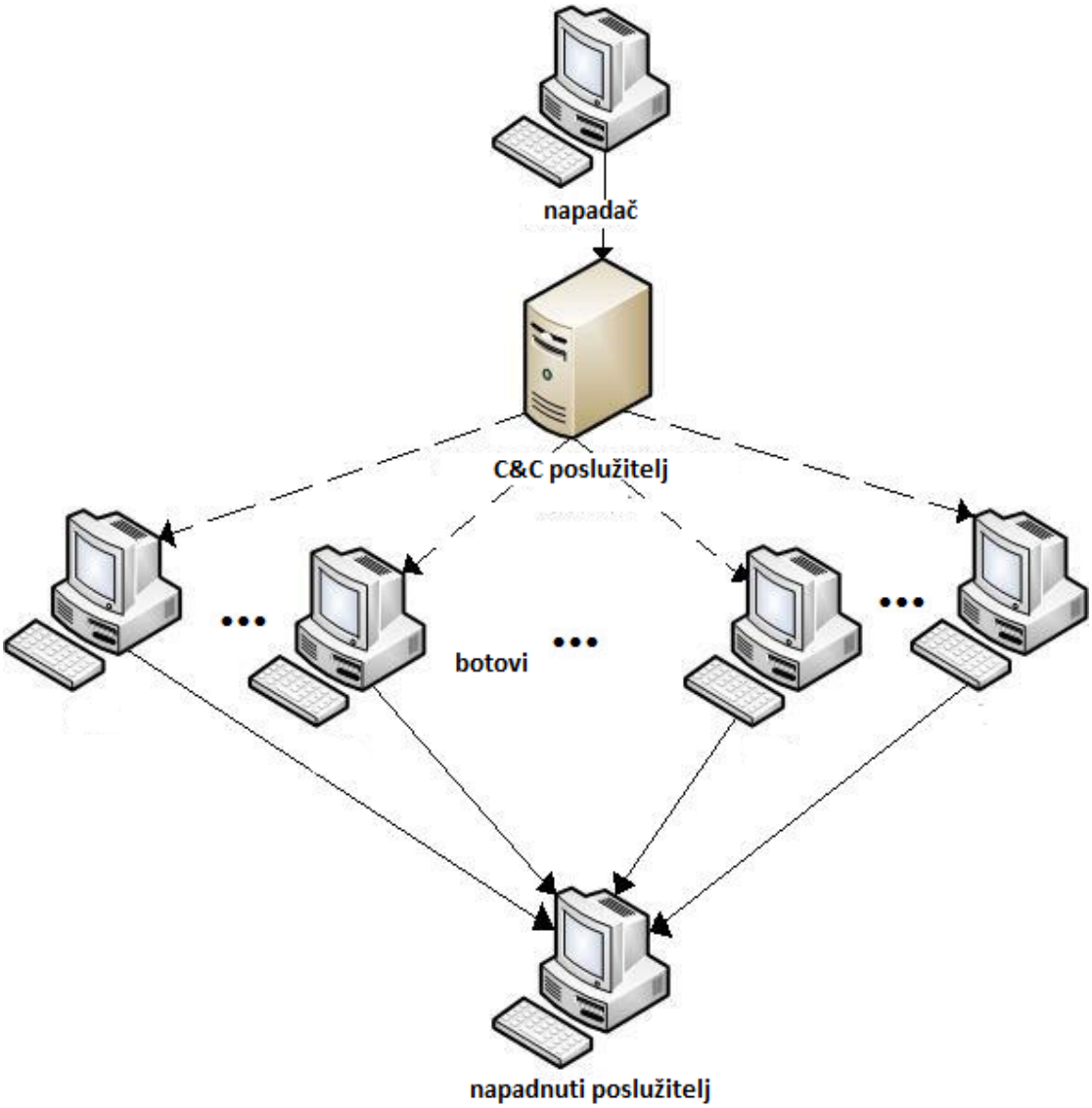
2. Nakon što naručitelj dostavi upravitelju mreže sadržaj poruke koju želi poslati u velikim količinama, upravitelj botnet mreže šalje neželjenu elektroničku poštu sa svih računala u svojoj botnet mreži.

Slika 7. *Slanje neželjene elektroničke pošte sa botnet mreže*

Izvor: *Wikipedia*

4.2.2. Distribuirani napad uskraćivanjem usluga

Nakon što je upravitelj botnet mreže uspostavio nadzor nad većim brojem računala, on njihovu računalnu snagu može iznajmiti i za izvođenje distribuiranog napada uskraćivanjem usluga (DDoS), kako je prikazano na slici 8. Sve ovisi o željama i potrebama kriminalne organizacije koja unajmljuje njegove usluge.



Slika 8. *Izvođenje DDoS napada pomoću botnet mreže*

Izvor: *Laboratorij za sustave i signale (LSS)*

5. Zaštita od botnet napada

5.1. Zaštita poslužitelja od DDoS napada botnet mreže

Zbog geografske raspršenosti računala u botnet mreži, velike količine zaraženih računala i činjenice da zaražena računala najčešće imaju promjenjivu, odnosno dinamičku IP (eng. Internet protocol) adresu, zaštita poslužitelja filtriranjem IP adresa nije primjenjiva. Ograničen uspjeh može biti postignut analizom specifičnosti operacijskih sustava računala koje izvode DDoS napad, te njihovim daljnjim onemogućavanjem pristupa poslužitelju (eng. Passive OS fingerprinting). Skuplja metoda zaštite je korištenje specijaliziranog NIDS (eng. network based intrusion detection system) sklopovlja.

Većina botnet mreža, odnosno botnet klijenta prima naredbe sa upravljačkog poslužitelja koji se nalazi iza stalne adrese. To najčešće nije statička IP adresa nego je poslužitelj registriran na nekoj od besplatnih usluga koje omogućuju tu funkcionalnost, kao što su DynDns.org, No-IP.com, i Afraid.org. Te adrese se mogu lako iščitati iz bot klijenta na zaraženom računalu, te se mogu poduzeti odgovarajuće mjere da se taj botnet poslužitelj onemogući u daljnjoj komunikaciji sa zaraženim računalima.

5.2. Zaštita osobnih računala od zaraze i ulaska u botnet mrežu

Iako odgovarajuće institucije onemoguće botnet upravljački poslužitelj u daljnjoj komunikaciji sa zaraženim računalima u botnet mreži, to ne znači da ta računala više nisu zaražena. Lako je moguće da botnet upravitelj na neki način uspije osvježiti bot klijente sa novom adresom botnet upravljačkog poslužitelja ili da neki drugi napadač preuzme nadzor nad tim zaraženim računalima, ubacivši u bot klijente adresu svog botnet upravljačkog poslužitelja.

Dobri pokazatelji da je računalo dio botnet mreže najčešće su povećan Internet promet na priključcima koje botnet upravitelji koriste za komunikaciju sa upravljačkim poslužiteljem:

- 445/TCP (eng. *Transmission Control Protocol*) kojeg koristi Microsoft-DS Service,
- 139/TCP (NetBIOS Session Service),
- 137/UDP (eng. *User Datagram Protocol*) kojeg koristi NetBIOS Name Service) i
- 135/TCP (Remote Procedure Call services, RPC).

Također je dobar pokazatelj i povećan promet na priključcima koje klijentski bot program najčešće koristi kako bi se proširio na druga računala:

- 42 – WINS (eng. *Windows Internet Name Service*) kojeg koristi Host Name Server,
- 903 – trojanski konj NetDevil Backdoor,
- 1025 – (eng. Microsoft Remote Procedure Call, RPC),
- 1433 - MS-SQL-S (eng. Microsoft-SQL-Server),
- 2745 - Bagle crv koji se koristi za slanje neželjene pošte,
- 3127 - MyDoom crv koji se koristi za slanje neželjene pošte,
- 3306 - MySQL korisnički definirane funkcije (eng. *User Defined Functions*, UDF),
- 3410 - Optix Backdoor trojanski konj,
- 5000 - UPNP (eng. Universal Plug and Play: MS01-059),
- 6129 – DameWare.

Metode zaštite su jednake onima od svih zlonamjernih programa, a najčešće su:

- korištenje najsvježijih inačica programa za zaštitu računala,
- redovito instaliranje zakrpa za operacijski sustav,
- povremeno provjeriti zapisnik o prometu lokalnog vatrozida,
- povećati sigurnost internet preglednika onemogućavanjem izvođenja skripta u istom,

- izbjegavati otvaranje sumnjivih priloga elektroničke pošte i posjetu sumnjivim internet stranicama te
- ograničiti prava korisničkog računa koji se koristi za svakodnevnu upotrebu, nema nikakve potrebe da se, pogotovo za pregledavanje sadržaja na internetu, koristi administratorski korisnički račun.

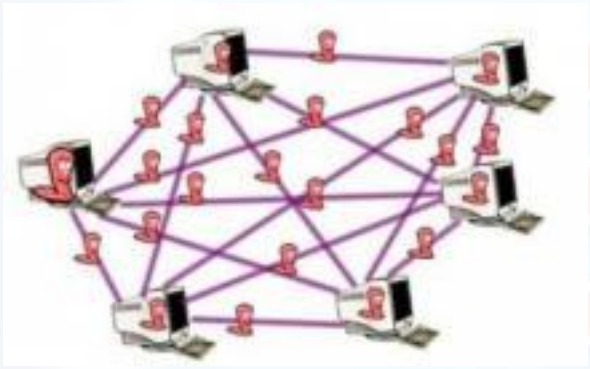
6. Budućnost botnet mreža

Jedno od zanimljivih svojstava novijih bot klijenata jest ugrađeni antivirusni program koji će provjeriti je li na računalu instaliran neki drugi bot klijent, od konkurentskog upravitelja botnet mrežom te će ga obrisati. Taj program će, ustvari popis svih programa učitanih u memoriju poslati na analizu nekoj od stranica koje nude besplatnu provjeru na zlonamjerne programe.

U posljednje vrijeme uočeni su i zlonamjerni programi koji pretvaraju mobilne uređaje u zombi računala, a jedan takav je "ANDROIDOS_ANSERVER.A.“ Također se za samo komunikaciju u botnet mreže sve više koristi protokol P2P(eng. *peer to peer*).

6.1. Prednosti protokola P2P za napadače

Upravo zbog ranjivosti botnet mreže na onemogućavanje upravljačkog poslužitelja u komunikaciji sa bot klijentima, u posljednje vrijeme pojavljuje se sve više botnet mreža koje koriste komunikacijski protokol P2P, kako je prikazano na slici 9. Taj protokol omogućuje redundantnost u komunikaciji jer je svako računalo povezano sa svim ili barem nekoliko drugih. Tako je upravitelju botnet mreže dovoljno ostvariti komunikaciju sa samo jednim računalom u mreži, a ono će najsvježije informacije proslijediti ostalima. Na taj način se gubi potreba za klasičnim upravljačkim poslužiteljem. Takve mreže su otpornije na pokušaje njihovog uklanjanja, a taj način komunikacije ima nekoliko nedostataka.



Slika 9. *Arhitektura botnet mreže koja koristi p2p komunikacijski protokol*

Izvor: *Physorg*

6.2. Nedostaci protokola P2P za napadače

Napadi koji zahtijevaju visoku stopu koordiniranosti velikog broja bot računala nisu lako izvedivi sa botnet mrežama koje koriste protokol P2P za komunikaciju. Taj problem se dešava baš zbog nedostatka središnjeg upravljačkog poslužitelja koji bi poslao naredbu svim računalima u isto vrijeme. Još jedan mogući problem se dešava prilikom slanja svježe inačice bot klijenta zaraženim računalima, zbog nedostatka hijerarhije u P2P mrežama, može doći do kolizije između dva računala. Točnije oko toga koje od njih ima više ovlasti instalirati program na drugo računalo, jer u takvoj botnet mreži svako računalo komunicira sa svakim te svako računalo pokušava ažurirati program na drugima.

7. Zaključak

Botnet mreže su već duže vrijeme najveća i najopasnija prijetnja na Internetu, a samim time i financijski najzanimljivija upraviteljima botnet mreža, ali i korisnicima njihovih usluga zbog učinkovitosti napada koji se njima ostvaruju. Programeri koji su najčešće i upravitelji tih mreža nude pravu programsku podršku, licence sa ograničenim vremenom trajanja te uklanjaju propuste u svojim programima brže nego to čini većina legalnih programa. Iz svega toga se lako zaključi kako je bavljenje ovom vrstom kriminala itekako isplativo. Upravo zbog toga stručnjaci se s razlogom pribojavaju budućem razvoju ovih mreža. Dodatno zabrinjava otkriven početak uključivanja mobilnih uređaja u takve mreže. Broj mobilnih uređaja, prvenstveno pametnih telefona, sa solidnom računalnom snagom u naglom porastu, a već postoje inačice sa dvojezgrenim procesorima i količinom radne memorije u gigabajtima. Svakako je otežavajuća okolnost različita percepcija mobilnih uređaja i osobnih računala među korisnicima. Možda je većina i svjesna prijetnji koje prijete osobnim računalima, ali mobilne uređaje još uvijek doživljavaju samo kao mobilne telefone, ne shvaćajući da su i oni postali prava mobilna osobna računala. Naravno takvi korisnici stoga ni ne brinu za zaštitu tih uređaja, a prava navala zlonamjernih programa na mobilne operacijske sustave kao što je Googleov Android, već je počela.

Zbog međunarodnih dimenzija botnet mreža, ovaj problem može biti riješen, ili barem smanjen, sveobuhvatnom suradnjom, ali prvenstven o boljom edukacijom korisnika. Ne treba ni zaboraviti motiv upravitelja botnet mreža i kriminalaca koji ih koriste, a to je novac. Naime, čak 95% financijskih transakcija za kriminal povezan sa botnet mrežama odvija se preko dvije banke, Azerigazbank iz Azerbajdžana te St Kitts & Nevis Anguilla National Bank iz Svetog Kristofora. Jedan od mogućih načina bi bio da ostale banke odbiju poslovati s dvije navedene banke dok god one surađuju sa kriminalcima.

8. Leksikon pojmova

SQL injection napad

Napad injekcijom SQL naredbe - Napadačka tehnika koja koristi sigurnosnu ranjivost kod pristupa web aplikacije bazi podataka. Na taj način moguće je ugroziti sigurnost web aplikacije koja konstruira SQL upite iz podataka unesenih od strane korisnika.

https://www.owasp.org/index.php/SQL_Injection

IP (Internet Protocol)

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

HTTP - HTTP protokol - HyperText Transfer Protocol

Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priključak 80), čekajući da klijent inicira komunikaciju.

http://hr.wikipedia.org/wiki/HTTP

Računalni virus

Virusi (eng. *Computer virus*) su programi koji se mogu kopirati i zaraziti računalo bez znanja ili dopuštenja korisnika. Računalo se može zaraziti na razne načine preko Internet-a, CD-a, USB-a... Virusi dolaze većinom sa drugim programima, kao što su npr. Trojanski konji kako bi maskirali svoj rad i kako bi ih bilo još teže za otkriti. Namjene virusa su različite, mogu služiti samo kako bi radili štetu no neki su manje štetni i samo usporavaju računalo i smetaju korisniku u radu. Virusi se spremaju u memoriju računala i pokreću se s operacijskim sustavom i inficiraju programe koji se pokreću.

http://www.ust.hk/itsc/antivirus/general/whatis.html

Spyware

Špijunski program (engl. Spyware) je program koji se tajno instalira na računalu kako bi presretao ili potpuno preuzeo kontrolu nad računalom bez dozvole korisnika. Iako bi se iz naziva moglo zaključiti da samo špijunira rad korisnika, većina Spyware-a radi puno više od toga. Mogu služiti kako bi sakupljali informacije o korisniku, mijenjali početnu stranicu u Internet pregledniku, instalirali dodatne programe na računalo i drugo.

http://os2.zemris.fer.hr/ns/2008_Mackovic/Spyware.htm

Računalni crv

Računalni crv je samo-replicirajući zlćudni program koji koristi mrežu računala kako bi poslao vlastite kopije na druge čvorove mreže bez pomoći korisnika. Ovakvo širenje računalnom mrežom je obično posljedica ranjivosti računala.

http://virusall.com/computer%20worms/worms.php

Trojanski konj

Trojanski konj je oblik zlćudnog programa koji se pretvara kao legitimna aplikacija. U početku se pretvara kao da obavlja korisnu funkcionalnost za korisnika, no u pozadini izvodi štetne radnje (na primjer, krađa informacija). Za razliku od crva, ovaj oblik zlćudnih programa se ne širi samostalno. http://www.webopedia.com/TERM/T/Trojan_horse.html

WWW (World Wide Web)

WWW (eng. World Wide Web) je jedna od najkorištenijih usluga Interneta koja omogućava dohvaćanje dokumenata. Dokumenti mogu sadržavati tekst, slike i multimedijalne sadržaje, a međusobno su povezani poveznicama (eng. hiperlink).

http://www.webopedia.com/TERM/W/World_Wide_Web.html

SQL

SQL je programski jezik za pohranu, upravljanje i dohvat podataka pohranjenih u relacijskoj bazi podataka. SQL je jedan od najrašireniji programskih jezik za upravljanje bazama podataka.

http://www.1keydata.com/sql/sql.html

9. Reference

[1] Chris Kanich, Christian Kreibich, Kirill Levchenko, Brandon Enright, Geoffrey M. Voelker, Vern Paxson, Stefan Savage: Analiza neželjene elektroničke pošte http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf, studeni 2011.

[2] Bruce Schneier: internet članak, http://www.wired.com/politics/security/commentary/securitymatters/2006/07/71471, studeni 2011.

[3] Richard A. Kemmerer: Krađa botnet mreže, https://www.youtube.com/watch?v=2GdqoQJa6r4, studeni 2011.

[4] The Honeynet Project, http://www.honeynet.org/papers/bots/ i http://www.honeynet.org/node/51, studeni 2011.

[5] Wikipedia, https://secure.wikimedia.org/wikipedia/en/wiki/Botnet, studeni 2011.