CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Botneti

NCERT-PUBDOC-2014-01-340

Nacionalni CERT

Sadržaj

Ovaj dokument pripremljen je uz financijsku podršku Europske unije. Sadržaj rada izražava mišljenje autora i ni na koji način ne izražava mišljenje i stavove Europske unije.

1 Uvod

Borba protiv botneta danas predstavlja jedan od glavnih izazova u svijetu računalne sigurnosti. Razvijatelji botnet mreža s vremenom izmišljaju nove načine kojima poboljšavaju širenje svojih mreža, njihovo prikrivanje i onemogućuju njihovu detekciju.

Botnet je skup računala koja su zaražena zlonamjernim programom koji omogućava osobi koja ga je stvorila određenu kontrolu nad zaraženim računalima. Pri tome korisnik zaraženog računala nije ni svjestan da mu je računalo zaraženo i da sudjeluje u raznim, obično zlonamjernim aktivnostima. Zaraženo računalno postaje *zombi* ili bot koji čeka instrukcije od glavnog računala (engl. *Bot master*).

Od samog početka pojave botneta vidljiv je njihov razvoj i napredak, pa tako danas imamo dvije glavne podjele botneta: centralizirane i peer to peer. Sve sa svrhom da se botneti teže detektiraju i iskorijene.

U samim počecima razvoja botneta njihova glavna svrha je bila širenje spam poruka, dok su danas uglavnom usmjereni na krađe osobnih podataka i brojeva bankovnih računa, slanje spam poruka, provođenje napada uskraćivanjem usluge i posluživanje zlonamjernog kôda i phishing stranica.

Botneti zauzimaju veliki dio u cjelokupnom računalnom kriminalu i predstavljaju infrastrukturu pomoću koje se čini šteta korisnicima Interneta koja se broji u milijunima eura. Europska unija prepoznala je njihov utjecaj i pokrenula ogromni projekt s ciljem suzbijanja postojećih botnet mreža i širenja novih.

Projekt je nazvan Advanced Cyber Defence Cetar i obuhvaća 28 partnera iz 14 zemalja Europske unije čiji je zadatak izgraditi platformu za detekciju i uklanjanje botneta.

2 Način rada botneta

Prilikom zaraze zlonamjernim programom na računalo se instalira backdoor ili program koji omogućava vlasniku botnet mreže komunikaciju i kontrolu nad zaraženim računalom. Nakon instalacije backdoora jako je teško isti maknuti s računala, čak i nakon instaliranja najnovijih sigurnosnih ažuriranja. Nakon zaraze računalo pokušava komunicirati s vlasnikom botneta. Zaraženo računalo može poslati hrpu informacija o računalu, uključujući vlastitu IP adresu, verziju operacijskog sustava, popis instaliranih zakrpa i mnoge druge. Jednom zaraženo računalo spremno je izvršavati akcije koje mu vlasnik mreže naredi.

Postoje razni načini na koji se računala mogu zaraziti i postati dio botneta:

Drive-by downloads: Najjednostavniji način zaraze računala je posjećivanje zaražene web stranice s računala koja nema instalirana najnovija ažuriranja na sebi.

Vlasnik botneta koristi SEO tehnike kako bi popularizirao web sjedišta koje sadrže zlonamjerne programe i na taj način privlači ostale korisnike na njih. Zlonamjerni kôd se preuzima i instalira na računalo putem spam poruka koje sadrže poveznicu na web sjedište koje poslužuje samoraspakirajući zlonamjerni kôd. Drive-by download se najčešće nalazi sakriven u zaraženim web stranicama (npr. nalazi se u iframe elementu). Posjetom takvog sjedišta korisnik instalira zlonamjerni kôd na svoje računalo.

Email: Stariji, ali još uvijek popularan način zaraze je otvaranjem elektroničke pošte sa zlonamjernim sadržajem. Mail je obično poslan s krivotvorenom adresom pošiljatelja, koja je u većini slučajeva lažno povezana s nekom institucijom (PayPal ili sl.). Poruka čak može biti poslana od nekog kome korisnik zna i vjeruje, ako je taj netko već zaražen.

Piratski programi: Zlonamjerni programeri često kriju zlonamjerni kôd u sklopu programa. Korisnici preuzimaju te programe, instaliraju ih na računalo i nisu svjesni da su s piratiziranim programom dobili i zlonamjerni program.

Vlasnici botneta zarađuju na vlastitim izgrađenim mrežama tako da iznajmljuju botnet drugim osobama za određenu aktivnost ili ga sami koriste. Neke od glavnih aktivnosti u kojima sudjeluju računala koja su dio botneta su:

a) **Raspodijeljeni napadi uskraćivanjem usluge (engl. *Distributed Denial of Service attack - DDoS)***
Namjena DDoS napada je slanje ogromnih količina upita ili paketa prema nekom poslužitelju. Premda poslužitelj nije u mogućnosti obraditi sve upite dolazi do njegovog zagušenja te poslužitelj nije u mogućnosti odgovarati na legitimne upite korisnika ili dolazi do zagušenja mrežne infrastrukture.

b) **Slanje spamova**
Na samom početku razvoja botneta jedna od njihovih namjena bila je upravo slanje neželjenih elektroničkih poruka odnosno spamova. Slanje spamova je i danas jedna od glavnih namjena. Zaraženi uređaji djeluju kao posrednici te šalju ogromne količine neželjenih poruka svaki dan. Neki od najvećih botneta u povijesti su slali milijune poruka po danu.

c) **Financijski kriminal**
U zadnje vrijeme botneti, odnosno zaražena računala koriste se za različite oblike financijskog kriminala. Mogućnost instaliranja dodatnog zlonamjernog programa na

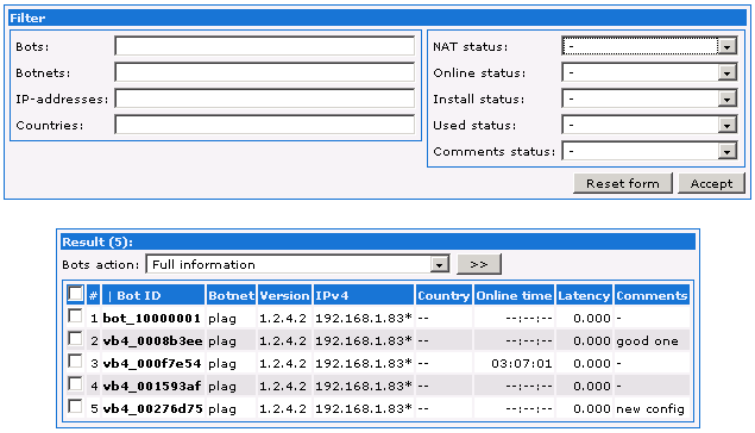
već zaraženo računalo omogućilo je prikupljanje važnih informacija o korisnicima koji ta računala koriste. Obično se radi o brojevima kreditnih kartica, identitetu korisnika, adresama, datumima rođenja i svim ostalim informacijama koje omogućuju efikasnu krađu novca s bankovnih računa i kartica.

d) Posluživanje phishing stranica ili malvera preko fast-flux domena

e) Pay-per-Click kriminal
Vlasnik botneta postavlja web stranicu na Internet i sklapa ugovor s oglašivačima. Ovisno o broju preusmjeravanja na taj plaćeni oglas dobiva proviziju. Kako ta osoba već ima cijelu mrežu računala s kojom upravlja koristi ih za prikazivanje lažnog prometa, te na taj način stječe financijsku korist od oglašivača.

2.1 Primjer botneta - Zeus botnet

Zeus botnet je najpoznatiji i najrašireniji botnet u svijetu. Od 2007. godine Zeus botnet mreže su u stalnom porastu. U 2013. godini imao je udio od skoro 58% svih botnet zaraza. Korisnici se uglavnom zaraze tako da otvore spam poruke koje na prvi izgledaju kao legitimne, slučaj je da se kao pošiljatelj navode i državne agencije.
Glavna namjena ove vrste botneta je krađa korisničkih podataka s raznih web stranica, poput online bankarstva i društvenih mreža.



Slika 1. Zeusov popis zaraženih računala

Postoji više verzija Zeus botneta, a najpoznatije od njih su TROJ_ZBOT.SVR (spamovi koji navodno dolaze od državnih agencija), TSPY_ZBOT.JF (napada AOL Instant Messenger korisnike) i TSPY_ZBOT.CCB (napada korisnike socijalnih mreža).
Nakon što se korisnici zaraze prati se njihova aktivnost na računalu. Obično se podatci kradu na način da se prikaže druga lažna stranica za prijavljivanje nakon prijave na orginalnu stranicu. Novije varijante koriste JavaScript kôd na način da ga ubace u legitimne web stranice banki koje posjećuju korisnici. Kôd se automatski ubacuje u preglednik prije nego li se prikaže stranica, npr. stranica za prijavu na bankovni račun. To omogućuje botnetu dodavanje polja za unos teksta ili prosljeđivanje informacija s legitimnih web stranica. Na slici 1 prikazan je prikaz zaraženih računala u Zeusovom administracijskom sučelju.

View report (HTTP request, 172 bytes)	
Bot ID:	**bot_10000001**
Botnet:	plag
Version:	1.2.4.2
OS Version:	XP Professional SP 2, build 2600
OS Language:	1033
Local time:	30.09.2009 14:16:03
GMT:	-8:00
Session time:	04:35:50
Report time:	30.09.2009 21:15:41
Country:	--
IPv4:	192.168.1.83
Comments for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Internet Explorer\iexplore.exe
Source:	http://www. bank.com/login.php

```
http://www. bank.com/login.php
Referer: http://www. bank.com/login.html
Keys: admintestswordfish1234567890
Data:

username=admintest
password=swordfish
pinnumber=1234567890
```

Slika 2. Zeusov ispis ukradene lozinke[1]

Kad osoba koja upravlja botnetom dođe do potrebnih informacija (slika 2), krade novac direktno od žrtve ili ih koristi kao posrednike. Ako ih koristi kao posrednike, prvo prebacuje novac s ukradenih računa na njihov račun te potom na svoj račun s ciljem težeg pronalaska stvarnog počinitelja krađe. Prikupljeni podatci se šalju HTTP POST zahtjevom na udaljene URL-ove (tzv. „drop zone“).
Upravo zbog svoje napredne taktike koja se oslanja na socijalni inženjering i sve napredniju tehniku slanja spamova ZBOT-ovi se šire velikom brzinom. Nemoguće ga je otkriti na zaraženom sustavu zbog svoje rootkit sposobnosti. Nakon instalacije, na računalu stvara datoteke s atributima postavljenim na „System“ i „Hidden“ i tako sprječavaju korisnike da ga pronađu i uklone. Naprednije verzije posjeduju mogućnost onesposobljavanja Windows vatrozida.

Slika 3. Koraci u zarazi Zeus botnetom[2]

[1] http://www.fortiguard.com/legacy/analysis/zeusanalysis.html

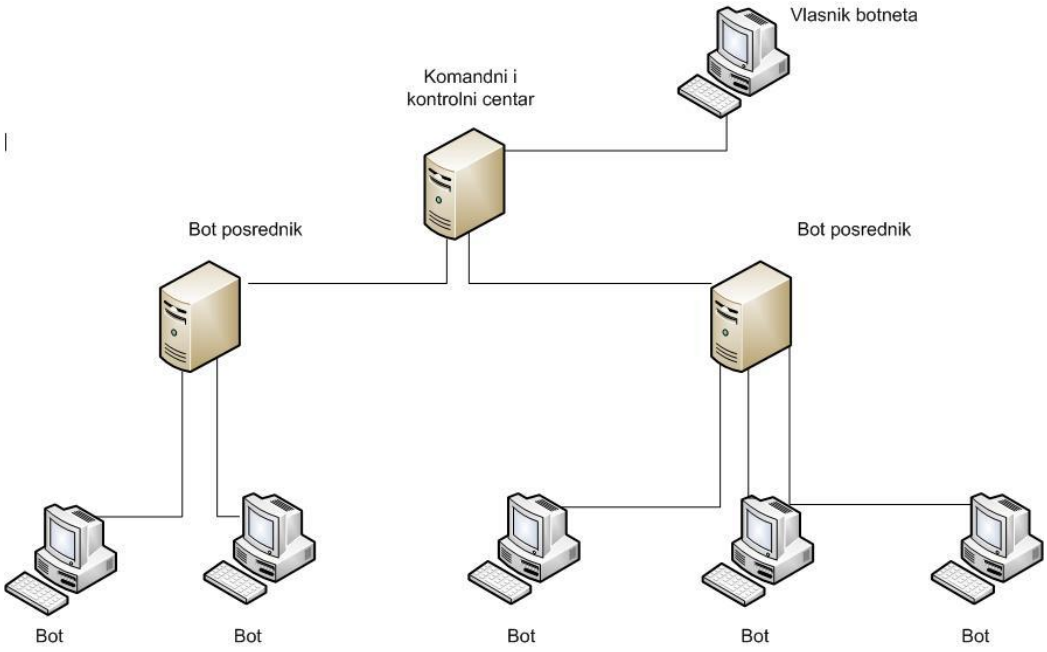
[2] http://threatinfo.trendmicro.com/vinfo/web_attacks/ZeuS_and_its_Continuing_Drive_Towards_Stealing_Online_Data.html

3 Podjela botneta

Postoje dvije glavne vrste botneta: centralizirani i decentralizirani (P2P).

3.1 Centralizirani botneti

Centralizirani botneti su vrsta botneta u kojoj su svi botovi povezani s jednim slojem komandnih i kontrolnih centara (engl. *Command and control centar - C&C*). C&C stalno osluškuje i čeka na nova zaražena računala. Kad se ostvari komunikacija s novim botom on ga registrira u svojoj bazi, prati njegov status i šalje naredbe koje treba izvršiti. Upravitelj botneta komunicira s C&C-om i na taj način upravlja cijelom mrežom. C&C komunicira s botovima preko niza posredničkih računala koja mogu opsluživati Fast-flux domene.



Slika 4. Centralizirani botnet

Način na koji botovi komuniciraju sa C&C poslužiteljem je najčešće preko HTTP ili IRC protokola što često omogućava prolaz paketa kroz sigurnosne uređaje (vatrozid, IPS i sl.).

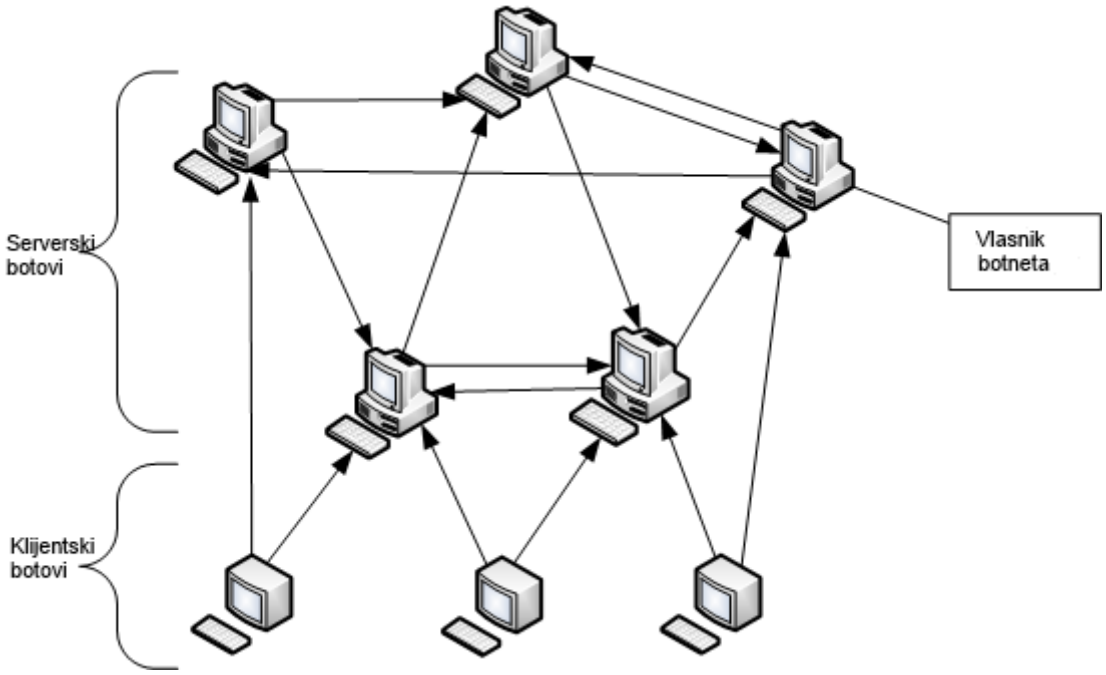
IRC protokol je dizajniran za tip komunikacije „jedan na više“ te time ne ograničava broj korisnika unutar jednog komunikacijskog kanala i to je primarni razlog zašto je postao popularan protokol za botnete. IRC pruža mogućnost direktne komunikacije i slanja naredbi samo određenim botovima.

Drugi način komunikacije u botnet mreži je putem HTTP protokola. Zbog svoje prisutnosti na Internetu rijetko kad je blokiran i filtriran. Upravo zbog toga se koristi u botnetima za upravljanje i kontrolu.

3.2 Decentralizirani (P2P) botneti

P2P botneti se temelje na ideji da su svi botovi jednako važni kako bi se uklonila potreba za centralnim poslužiteljem. Računala koja se nalaze iza NAT-a, vatrozida ili posredničkih poslužitelja ne mogu prihvatiti dolazne konekcije, ali zato mogu inicirati komunikaciju.

Nedostatak dolaznih konekcija od strane poslužitelja predstavlja problem u P2P infrastrukturi jer sprječava većinu botova da budu povezani s ostalim botovima. U centraliziranim botnetima nema ovog problema jer se botovi povezuju s poslužiteljem. Botovi koji su sposobni primati dolazne konekcije (ne nalaze se iza posredničkih poslužitelja, NAT-a ili vatrozida) se ponašaju kao poslužitelji i nazivaju se peerovi ili čvorovi. Botovi koji nisu sposobni primati konekcije („workeri“) se spajaju na jedan ili više čvorova kako bi primili naredbe. Čvorovi su praktički poslužitelji i njihova brojnost sprječava rušenje botnet mreže. Čak i ako se neki od čvorova otkriju i ugase, postoje drugi čvorovi koji će preuzeti posao.



Slika 5. P2P botnet[3]

„Workeri“ su distribuirani između više čvorova te u slučaju pada nekog čvora započinju komunikaciju i primaju naredbe od drugog. P2P botneti u praksi funkcioniraju jedino ako se sastoje od dovoljnog broja čvorova, koje je zahtjevno ugasiti. Čvorovi mogu biti i krajnja računala, a ne samo poslužitelji. Dok god se zlonamjerni kôd ne ukloni s računala oni su dio botnet mreže.

Kako bi naredbe kružile cijelom mrežom i došle do svakog „workera“, ali i čvora potrebno je povezati botove na više čvorova. Tako se botovi osiguravaju da uvijek imaju komunikaciju s mrežom ako padne čvor s kojim je do tad bio u vezi. Čvorovi se povezuju jedni s drugima te također izmjenjuju naredbe. Kako bi se bot priključio mreži potrebna mu je IP adresa od najmanje jednog čvora. Bot posjeduje listu adresa (adrese bootstrap poslužitelja) s kojima se povezuje nakon infekcije.

Posao bootstrap poslužitelja je održavanje cjelokupne liste IP adresa čvorova te slanje popisa tih IP adresa novim botovima koji imaju nekompletnu listu.

[3] http://www.intechopen.com/books/advances-in-data-mining-knowledge-discovery-and-applications/botnet-detection-enhancing-analysis-by-using-data-mining-techniques

4 Izbjegavanje rušenja botneta

Botneti koriste razne tehnike kako bi zaobišli postojeće metode otkrivanja i onemogućavanja komunikacije botova s glavnim C&C poslužiteljem.

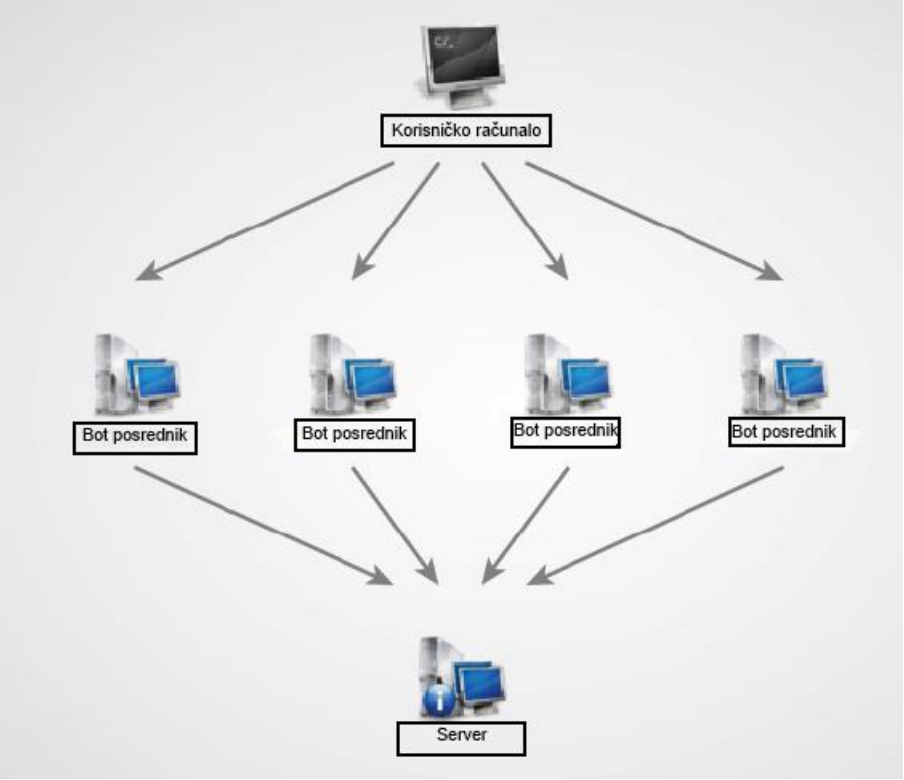
Jedna od starijih metoda je postojanje više poslužitelja. Ako nije moguća komunikacija s jednim poslužiteljem, bot pokušava ostvariti komunikaciju s ostalima. Botneti također koriste tehnike poput: DGA (engl. *Domain Generation Algorithms*) i Fast fluxa.

4.1 Fast flux tehnika izbjegavanja detekcije

Fast flux služi skrivanju glavnih C&C poslužitelja. U tu svrhu, koristi se imenički poslužitelj - DNS (engl. *Domain Name System*) koji omogućava dinamičke promjene u infrastrukturi.

Svrha Fast fluxa je iskoristiti mogućnost DNS-a da jednom FQDN-u (engl. *Fully Qualified Domain Name*) dodijeli na tisuće IP adresa. Iza tih IP adresa se kriju botovi (slika 6). Ti botovi funkcioniraju kao posrednički poslužitelji, prosljeđujući svu klijentsku komunikaciju do poslužitelja, koji se skriva iza posredničkog sloja. Iza tog sloja se mogu skrivati i maliciozni servisi poput phishing stranica, sumnjivih reklama ili arhivirani zlonamjeran sadržaj spreman za preuzimanje. Općenito, kod ove tehnike DNS zapisi imaju vrlo kratak period trajanja što rezultira brzom promjenom odgovora za istu domenu, tj. omogućava promjenu IP adresa u Internet domeni.

Čest pristup u borbi protiv botneta je blokiranje malicioznih domena.



Slika 6. Fast flux tehnika[4]

[4] http://blog.trendmicro.fr/asprox-is-back/

4.2 Domain Generation Algorithms tehnika izbjegavanja detekcije

Druga metoda je generiranje domenskih naziva (engl. *Domain Generation Algorithms*, skraćeno DGA). Ideja DGA je generiranje posredničkih domena (imena domena povezanih s DNS zapisima na C&C poslužitelje) koje se razlikuju po nekom uzorku - marker. Tim markerima mogu pristupiti botovi i upravitelji botneta. Markeri mogu biti vremenske oznake, podatci s poznatih web stranica poput društvene mreža i sl. Dok vremenske oznake pružaju mogućnost generiranja imena domena daleko unaprijed, korist dinamičkog web sadržaja eliminira taj element predvidljivosti. Veliki broj domena se može generirati u kratkim vremenskom roku. Tipično vrijeme perioda trajanja tih domena je jedan dan. Svaki pokušaj smanjivanja tog tipa botnet napada se svodi na ukidanje brojnih sumnjivih domena. Trud koji je potreban uložiti za obranu od takvih napada je velik, jer upravitelji botneta mogu odabrati bilo koju od mogućih domena, registrirati ju i omogućiti joj da pruža nove instrukcije ili ažuriranja tijekom trajanja te domene. Algoritam po kojem se generiraju novi tipovi domena nalazi se u zlonamjernom kôdu.

5 Kako prepoznati botnet i obraniti se od njega

5.1 Kako prepoznati da je vaše računalo bio botneta:

Kada vaše računalo postane bio botneta obično se na njemu pojave neki od simptoma:

- Sustav je sporiji nego inače
- Tvrdi disk radi stalno iako ne koristimo računalo
- Dolazi do nestajanja ili promjene strukture datoteka
- Kolege i prijatelji vam javljaju da su dobili mail koji niste poslali
- Vatrozid vas obavještava da se neki program pokušava spojiti na Internet
- Antivirusni ili drugi sigurnosni alat vas upozorava na sumnjive pojave

5.2 Kako se obraniti

Važno je imati na umu da Internet nije posve sigurno mjesto i da postoji konstantna prijetnja od različitog zlonamjernog sadržaja. Osim same edukacije o prijetnjama postoji par pravila kojih se moramo pridržavati u svakodnevnom korištenju Interneta.

1. Prilikom preuzimanja programa s Interneta dobro je koristiti legitimne web stranice, odnosno ukoliko je to moguće stranice proizvođača programa. Preuzimanjem s ostalih neprovjerenih stranica ili s torrenta riskiramo da instaliranjem takvih programa istodobno instaliramo dodatne zlonamjerne programe.
2. Sve aplikacije instalirane na računalu uključivši i web preglednik, skupa s operacijskim sustavom potrebno je redovito ažurirati najnovijim verzijama i sigurnosnim zakrpama.
3. Prilikom otvaranja poruka elektroničke pošte ne smijemo klikati na poveznice koje nam se čine sumnjive. Iza njih se obično kriju kompromitirane web stranice s raznim verzijama zlonamjernih programa. Ako primimo elektroničku poštu od nepoznate osobe potrebno je biti još oprezniji. Ukoliko na nekoj od društvenih mreža primimo poruku sa sumnjivim sadržajem i ako ta ista poruka sadrži poveznicu ne smijemo kliknuti na nju.
4. Prilikom prijave na web stranice koje traže upis podataka o bankovnim računima potrebno je biti izuzetno pažljiv (posebno ako od nas traže ponovni unos već upisanih podataka).

6 Advanced Cyber Defence Centar

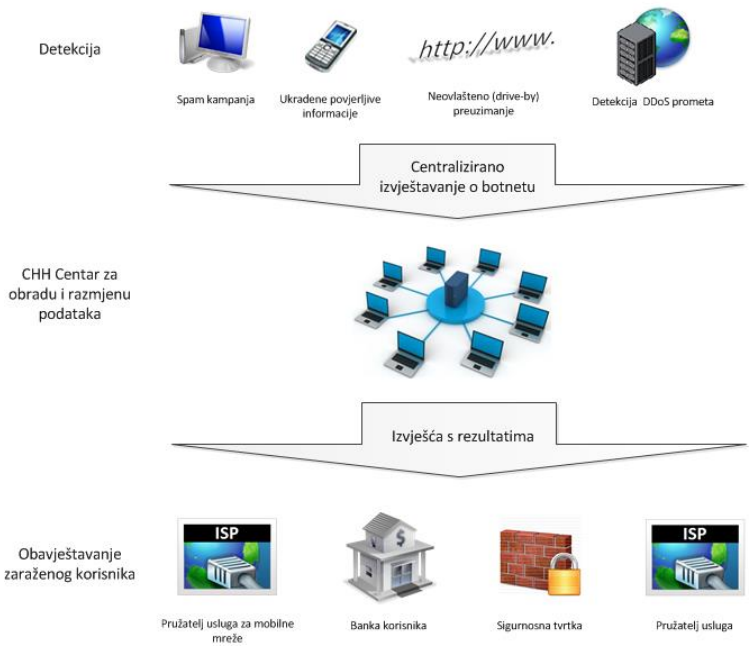
Advanced Cyber Defence Center (ACDC) je projekt financiran iz programa potpore politike za konkurentnost i inovacije u ICT (CIP-ICT). U projektu sudjeluje 28 partnera iz 14 europskih država. Na čelu konzorcija se nalazi njemačko udruženje internetske industrije ECO.

Glavni cilj projekta je borba protiv botneta i uspostava platforme Europske Unije. Projekt je započeo u veljači 2013. godine i uključuje: detekciju botneta, mjerenja, analize, prevencije i oporavka od šteta nastalih djelovanjem botneta.

Plan je uspostaviti osam nacionalnih centra podrške koji bi bili povezani s centrom za obradu i razmjenu podataka (engl. *Centralized Clearing house - CCH*). Centri podrške trebali bi pomoći krajnjim korisnicima da pomoću objavljenih usluga i alata na web sjedištu otklone, detektiraju ili spriječe sigurnosne probleme na svojim računalima. Na slici 7 prikazani su primjeri velikih korisnika koji imaju i mogućnost dobivanja rezultata vezanih za njihove mreže.

Infrastruktura ACDC platforme se sastoji od 3 glavna dijela (servisa):

a) Centar za obradu i razmjenu podataka (CCH) je središnja točka za pohranu i analizu podataka. Pristup podatcima će imati veliki korisnici zainteresirani za sudjelovanje u ACDC projektu.
b) Centri potpore (NSP) pružaju mogućnost preuzimanja alata za uklanjanje zlonamjernih programa i potporu za rješavanje pojedinačnih incidenata. S njega je moguće preuzeti alat Avira EU-Cleaner, prijenosni antivirusni program koji otkriva i uklanja zlonamjerne programe s vašeg računala. Uz njega je moguće preuzeti DE-Cleaner CD-a koji služi za spašavanje zaraženog operacijskog sustava. DE-Cleaner uklanja zlonamjerne programe s vašeg računala u slučaju da je računalo zaraženo u toj mjeri da se antivirusni program ne može ažurirati ili da se zaražene datoteke ne mogu pobrisati. Na stranicama web sjedišta NSP je moguće također aktivirati i online servise koji će povremeno skenirati web sjedište korisnika ili njegovo osobno računalo.
c) Alati za krajnje korisnike i senzori za identifikaciju i uklanjanje zlonamjernih programa, detekciju malicioznog mrežnog prometa, Fast flux-domena i malicioznih web sjedišta. Senzori za identifikaciju botova, zlonamjernih web sjedišta i Fast-flux domena su instalirani kod partnera koji su članovi ACDC konzorcija čija je uloga izvedba projekta



Slika 7. ACDC tok podataka

Partneri projekta su veliki pružatelji internetskih usluga, CERT-ovi, znanstvene ustanove, zakonodavna i administrativna tijela, predstavnici kritične infrastrukture, proizvođači sigurnosnih rješenja i ostali.

ACDC je važan dio računalne sigurnosti Europske unije. To je ujedno i prva inicijativa pokrenuta od strane EU u sklopu strategije za računalnu sigurnost[5]. Projekt će omogućiti bolju zaštitu računalnih mreža i sustava u borbi protiv zlonamjernih programa i botneta.

Centralna točka cijelog sustava je CCH koji dobiva izvješća o spam kampanjama, ukradenim podatcima, Fast-flux domenama, DDoS napadima, zlonamjernim web sjedištima i ostale izvještaje o aktivnostima botneta od članova projekta. CCH služi kao izvor podataka za velike korisnike koji su zainteresirani za rezultate te vrste.

Na taj način CCH može dostaviti podatke o incidentima u mreži davatelja Internet usluga, kasnije davatelj usluge može uputiti svoje korisnike na NSP gdje je moguće pronaći alate za čišćenje ili provjeru svojeg računala.

[5] EU Cyber Security Strategy - http://eeas.europa.eu/policies/eu-cyber-security/index_en.htm

7 Literatura

[1] The botnet Wars: a Q&A, http://bartblaze.blogspot.com/2010/10/botnet-wars-q.html, 24.10.2010.

[2] Peer-to-peer botnets resilient to takedown attempts, http://threatpost.com/peer-to-peer-botnets-resilient-to-takedown-attempts/100851, 31.5.2013.

[3] Number of peer-to-peer botnests grows 5x, http://threatpost.com/number-of-peer-to-peer-botnets-grows-5x/100871, 5.6.2013.

[4] Peer-to-peer botnets for beginners, http://www.malwaretech.com/2013/12/peer-to-peer-botnets-for-beginners.html, 21.12.2013.

[5] Anatomy of a botnet, http://www.fortinet.com/sites/default/files/whitepapers/Anatomy-of-a-Botnet-WP.pdf

[6] Botnet detection:Enchancing analysis by using Data Mining technique, http://www.intechopen.com/books/advances-in-data-mining-knowledge-discovery-and-applications/botnet-detection-enhancing-analysis-by-using-data-mining-techniques, 12.9.2012.

[7] Zeus and its continuing drive towards stealing online data, http://threatinfo.trendmicro.com/vinfo/web_attacks/ZeuS_and_its_Continuing_Drive_Towards_Stealing_Online_Data.html

[8] Zeus retains botnet crown, according to McAfee, http://www.v3.co.uk/v3-uk/news/2258398/zeus-still-king-of-the-botnets-say-researchers, 29.3.2013.

[9] http://blog.trendmicro.fr/asprox-is-back/, 6.3.2013.