CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Crimeware i Zeus botnet

NCERT-PUBDOC-2010-10-314

Nacionalni CERT

Nacionalni CERT+

Sadržaj

1 Uvod

Danas je zlonamjerni kod izvor velike prijetnje za sigurnost računalnih sustava i podataka. O veličini opasnosti svjedoči broj različitih primjeraka zlonamjernog koda koji se mogu pronaći na Internetu. Osim toga, postoji mnogo različitih kategorija i vrsta zlonamjernog koda. Jedna od tih vrsta je i *crimeware* – zlonamjerni kod koji služi kao alat za izvršenje različitih kriminalnih radnji.

Rast *crimewarea* povezan je s rastom komercijalne isplativost Interneta. Sa sve većim brojem financijskih transakcija obavljenih putem Interneta, rastao je i broj kriminalaca koji su tu vidjeli šansu za velikom zaradom. Otvorena narav Interneta i slaba informatička pismenost korisnika znatno su im olakšali posao pa je danas *crimeware* najštetnija vrsta zlonamjernog koda. Procjenjuje se da poslovne organizacije, ali i privatni korisnici godišnje izgube milijune dolara na prijevarama, krađama ili ucjenama počinjenima uz pomoć *crimewarea*.

Zbog svega navedenog važno je poznavati *crimeware*, način na koji se širi, koje postupke njegovi autori koriste i kako se zaštiti od njega.

Ovaj dokument u prvom dijelu donosi definiciju, model širenja i postupke koje autori *crimewarea* koriste. Predloženi su i savjeti za zaštitu od ove vrste zlonamjernog koda.

Drugi dio dokumenta prikazuje anatomiju i funkcionalnost Zeus *botneta*. On je jedan od najraširenijih i najopasnijih *crimeware* programa. Posebno je dizajniran za krađu financijskih podataka. Iako je prvi puta otkriven 2007. godine i danas je mnoštvo računala zaraženo njime, a u određenim vremenskim intervalima pojavljuju se nove, različite verzije *botneta* s tisućama zaraženih računala.

2 Osnovno o *crimewareu*

Crimeware je svaki oblik zlonamjernog koda koji pomaže u obavljanju kriminalnih radnji putem računala. Najčešće, kriminalne radnje uključuju:

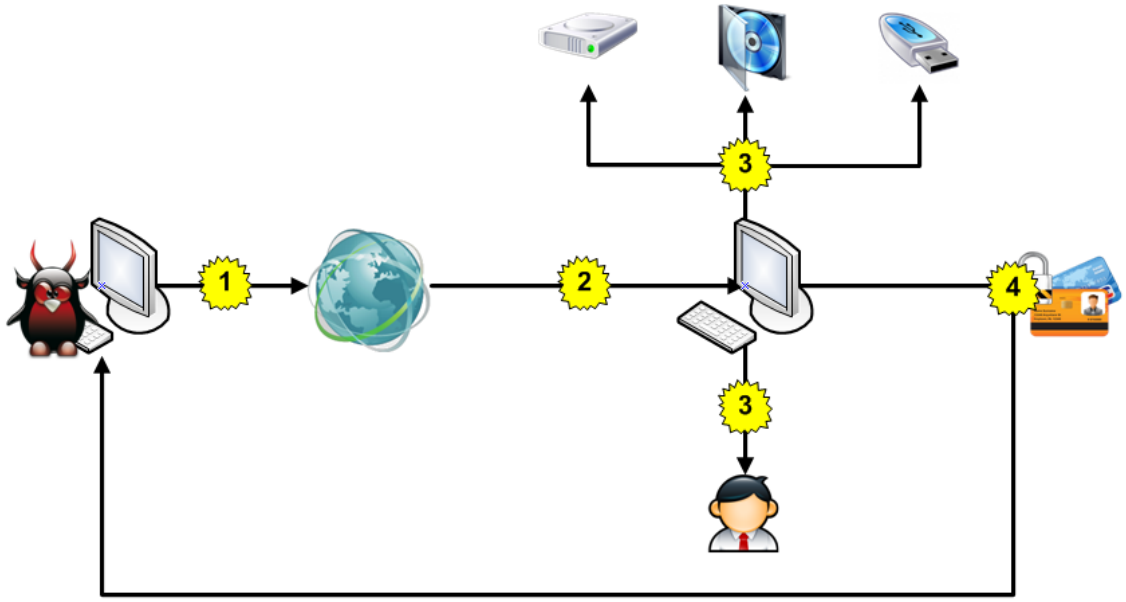
- Krađu identiteta
- Ucijene
- Krađu osobnih podataka
- Slanje neželjene elektroničke pošte

Ove kriminalne radnje kao krajnji cilj imaju ostvarivanje nekog oblika imovinske koristi za autore *crimewarea* ili one koji se njime koriste.

Sam termin *crimeware* prvi puta je spomenuo Peter Cassidy, glavni tajnik Anti-Phishing Group organizacije, kako bi tu vrstu zlonamjernog koda razlikovao od ostalih. Iako je po definiciji jasno koji zlonamjerni kod pripada u skupinu *crimewarea*, u praski je ponekad teško napraviti jasno razgraničenje. Mnogi primjerci zlonamjernog koda ne služe za obavljanje strogo kriminalnih radnji. Kao primjer možemo istaknuti *adware* programe, koji prikazuju brojne reklame i ometaju rad korisnika računala. No, samo reklamiranje u većini situacija nije kriminalna radnja. Neformalno, kada se spominje *crimeware* podrazumijeva se obavljanje težih kriminalnih djela. Krađa i stjecanje protupravne imovinske koristi spadaju u tu kategoriju.

2.1 Kako funkcionira *crimeware*?

Postoji mnogo različitih vrsta *crimewarea*. Njihovi autori su kreativni i tehnički vrlo inovativni. Često se događa da novi pojavni oblik *crimewarea* koristi do tada neviđene tehničke postupke zaobilaženja zaštitnih alata. Zbog velike brojnosti, gotovo je nemoguće izraditi taksonomiju *crimewarea* ili dati univerzalni model njihova ponašanja. Ipak, sljedeća slika u grubo prikazuje način rada *crimewarea*. Brojevi označavaju korake u životnom ciklusu *crimewarea*. Uočeno je da je svaki od tih koraka prisutan u bilo kojoj epidemiji *crimewarea*.



Slika 2.1 - Prikaz načina rada crimewarea

1. **Izrada i distribucija** – U ovom koraku napadač izrađuje *crimeware* i započinje s njegovom distribucijom. Kao što će kasnije biti prikazano, distribucija može biti u potpunosti automatizirana ili može zahtijevati interakciju moguće žrtve.

2. **Infekcija** – U ovom koraku *crimeware* alat zarazi pojedino računalo. Postoje brojni načini na koje on to može napraviti. U nekim slučajevima nema stalne zaraze već se zlonamjerni kod *crimewarea* jednokratno izvršava.

3. **Krađa informacija** – Ovo je sljedeći korak u kojem crimeware krade povjerljive informacije (lozinke, brojeve bankovnih računa, brojeve kreditnih kartica itd.). Krađa se obično odvija u dva smjera:

   a) Pretraživanje informacija na tvrdom disku žrtve – Ovdje *crimeware* pretražuje sve datoteke i direktorije na tvrdom disku u potrazi za povjerljivim informacijama. Potraga ne mora biti ograničena samo na tvrdi disk, moguće je pretražiti izmjenjive diskove, radnu memoriju računala i ostala mjesta na kojima su pohranjeni podaci.

   b) Preuzimanje informacija direktno od korisnika – U ovom slučaju *crimeware* povjerljive informacije preuzima od korisnika. Kako bi u tome uspio, *crimeware* pričeka da korisnik unese povjerljive informacije u neku aplikaciju i potom ih zabilježi. *Crimeware* može prijevarom nagovoriti korisnika na unos povjerljivih informacija (eng. *Phishing*) ili jednostavno može bilježiti unos svih znakova s tipkovnice – na taj način rade *keyloggeri*.

4. **Isporuka ukradnih podataka** - *Crimeware* putem nekog komunikacijskog kanala ukradene podatke isporučuje napadaču. Osim slanja ukradenih podataka, *crimeware* može napadaču omogućiti udaljenu kontrolu nad zaraženim računalom.

Kako bi napadač prošao neopaženo, on ne obavlja direktan prijenos sredstava s računa žrtve na svoj račun, već koristi posrednike. Napadač na račun posrednika uplaćuje ukradena sredstva, a posrednik mora u što kraćem vremenskom roku prebaciti sredstva na neki treći račun, najčešće u drugoj državi. Posrednici obično ne znaju da sudjeluju u pranju novca. Njih napadač angažira lažno se predstavljajući kao legitimna tvrtka koja traži nove zaposlenike. Od

njih se traži da sav novac koji im tvrtka uplaćuje na račun brzo proslijede na druge račune, pritom zadržavajući malu proviziju. Kako posrednici nisu svjesni da sudjeluju u pranju novca i da rade za kriminalce za njih se koristi engleski termin „money mule“. Taj termin često se može naći u različitim izvještajima o financijskim prijevarama putem interneta.

Crimeware nakon četvrtog koraka ponovo prelazi na treći, te se tako vrti u krug skroz dok ne bude otkriven i uklonjen s računala.

Različiti primjerci *crimeware* alata primjenjuju različite postupke za ostvarivanje svojih ciljeva. Neki samo kradu povjerljive informacije, drugi omogućavaju napadaču i kontrolu nad zaraženim računalom. Neki primjerci posebno su dizajnirani za krađu informacija iz web preglednika, dok drugi samo bilježe sve znakove koje žrtva pritisne na tipkovnici.

Kombinacija ima nebrojeno mnogo i svakom novom kombinacijom *crimeware* može izbjeći detekciju i dugo vremena ostati neopažen. Često se događa da autor prati vijesti vezane uz svoj *crimeware*, te kako sigurnosni stručnjaci razviju metodu za njegovo uklanjanje, tako on izda novu verziju koja opet prolazi neopaženo. Sljedeći dijagram najbolje ilustrira odnos između napadača i istražitelja.

Slika 2.2 - Prikaz odnosa između napadača i sigurnosnih stručnjaka

Dijagram je kružni što znači da se ovaj proces može odvijati jako dugo. Sa svakim punim krugom napadač je razvio jednu novu verziju svojeg *crimewarea* alata. Kao primjer ovog ciklusa može poslužiti poznati internetski crv *Conficker*. U razdoblju od studenog 2008. godine do travnja 2009. godine otkriveno je pet verzija tog crva. Svaka od njih se pojavila nakon što bi prethodna bila otkrivena i zaustavljena. Također, svaka od njih imala je veću funkcionalnost i pokazala veću otpornost na otkrivanje od prethodne.

2.2 Kako se *crimeware* širi?

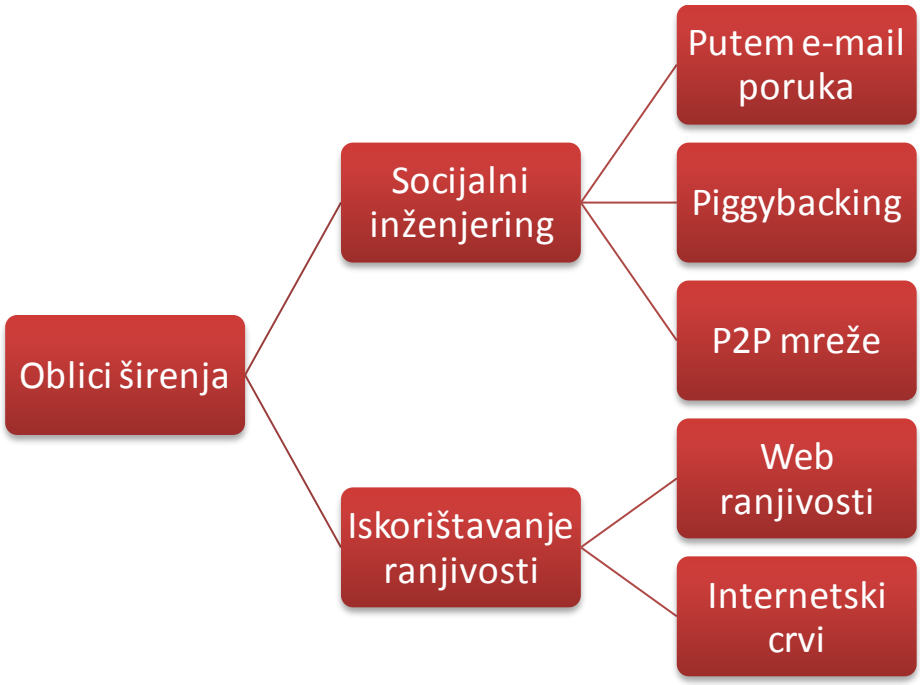
Gotovo svaki primjerak *crimewarea* dizajniran je tako da što prije zarazi što veći broj računala. Mnogo je postupaka koje napadači koriste za ostvarivanje ovog cilja. Bez obzira na brojnost, može ih se podijeliti u dvije osnovne grupe:

- Socijalni inženjering
- Iskorištavanje ranjivosti

Kod **socijalnog inženjeringa** napadač pokušava nagovoriti moguću žrtvu da sama preuzme i pokrene njegov primjerak zlonamjernog koda. On se pri tome služi različitim tehnikama prijevara, nagovaranja i sl. Važno je naglasiti da ovaj oblik širenja *crimewarea* zahtjeva interakciju žrtve.

Širenje *crimewarea* putem **iskorištavanja ranjivosti** ne zahtjeva interakciju s mogućom žrtvom. *Crimeware* se širi koristeći sigurnosti propust unutar nekog softverskog paketa kojeg žrtva koristi. Ovakav način širenja u potpunosti je automatiziran.

Postupci širenja mogu se i detaljnije klasificirati kako je prikazano sljedećim dijagramom.



Slika 2.3 - Načini širenja *crimewarea*

Širenje putem **elektroničke pošte** najčešći je oblik širenja *crimewarea*. Napadač šalje elektroničke poruke mogućim žrtvama. Poruka sadrži URL poveznicu na nepoznatu izvršnu datoteku. U tekstu poruke moguća žrtva se nagovara da na svojem računalu pokrene tu izvršnu datoteku. Nepažljivi korisnik može nasjesti na takav oblik nagovaranja i nakon što pokrene datoteku, njegovo računalo će biti zaraženo nekim oblikom *crimewarea*. *Crimeware* će potom s njegova računala početi slati elektroničku poštu drugim korisnicima.

Piggybacking je zanimljiv postupak nagovaranja korisnika da pokrene nepoznati program na svojem računalu. Općenito, *piggybacking* označava tehniku u kojoj se korisniku koji preuzima jednu datoteku s interneta nudi i druga datoteka za preuzimanje. Često se tako nešto može korisniku dogoditi ukoliko preuzme neki video s Interneta ili putem P2P mreže. Kada korisnik želi pogledati video, prikazuje mu se poruka o tome da nema potreban dekoder te mora preuzeti poseban softver za reprodukciju željenog video materijala. Taj posebni softver je zapravo zlonamjeran programski kod koji će na njegovo računalo instalirati neki oblik *crimewarea*.

P2P mreže idealno su mjesto za distribuciju zlonamjernog koda. Na njima ne postoji nikakva kontrola dijeljenih datoteka. Na nekim P2P mrežama gotovo 70% razmijenjenih izvršnih datoteka i arhiva sadrži zlonamjerni kod [1]. Usprkos tome, veliki broj korisnika ih i dalje koristi za razmjenu datoteka. Kako bi napadač raširio svoj primjer zlonamjernog koda putem P2P mreže jednostavno može zlonamjerni kod postaviti u zajedničku mapu i pričekati da ga neki drugi korisnik preuzme. Napadači obično svojim zlonamjernim datotekama daju takva imena koja će kod većine korisnika pobuditi zanimanje kako bi sami pokrenuli nepoznatu izvršnu datoteku.

Kod širenja putem ranjivosti, danas posebno mjesto zauzimaju različiti oblici **web ranjivosti**. Web ranjivosti omogućavaju napadaču pribavljanje neovlaštenog pristupa nekom web poslužitelju. Napadač potom na njega može postaviti vlastite web stranice. Ako je napadač uspio kompromitirati web poslužitelj u kojega korisnik ima povjerenja to može iskoristiti kako bi od korisnika zatražio da pokrene neku datoteku ili bilo koji drugi oblik zlonamjernog koda.

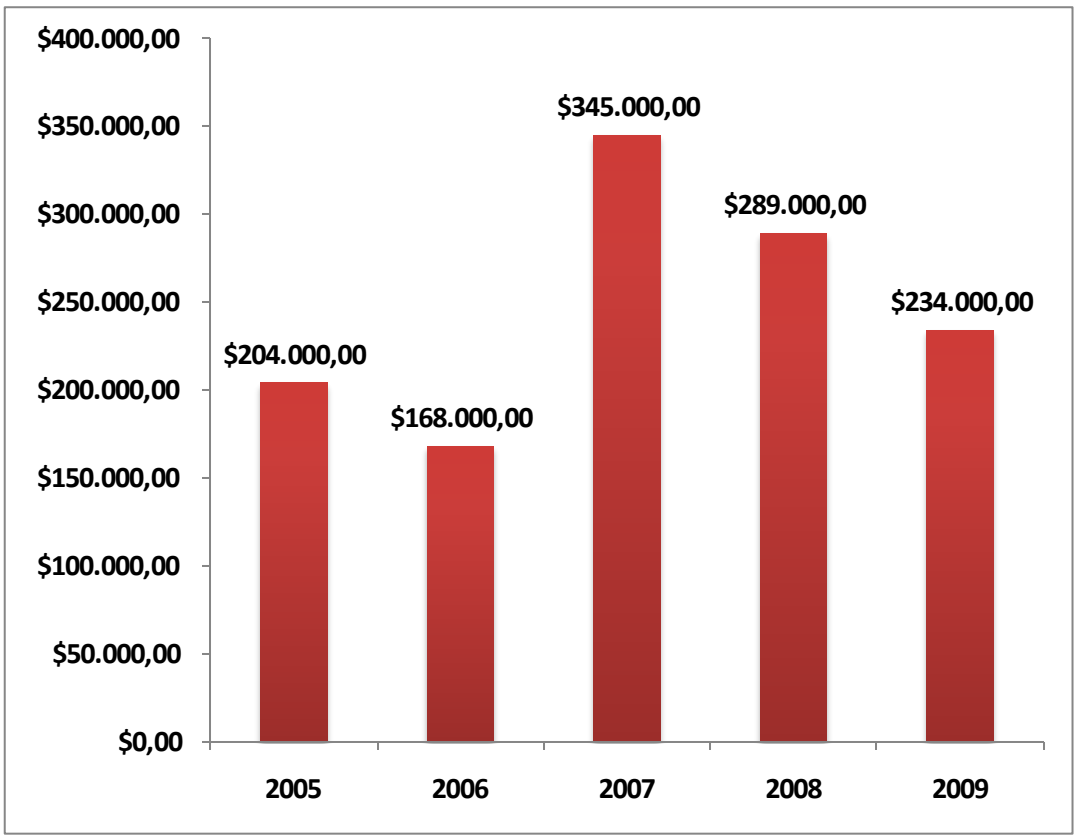
Uz web ranjivosti usko su povezane i ranjivosti unutar web preglednika. Danas su web preglednici postali najvažniji softver instaliran na računalu, mnogi korisnici ih gotovo isključivo koriste u svakodnevnom radu. Zbog toga se sve češće pojavljuju različite ranjivosti unutar popularnih web preglednika. Autori *crimewarea* iskorištavaju te ranjivosti kako bi mogli širiti svoj zlonamjerni kod putem interneta. Dovoljno je da napadač pripremi zlonamjernu web stranicu na Internetu i moguću žrtvu nagovori da posjeti tu stranicu. Budući da je stranica pripremljena tako da iskoristi ranjivost u web pregledniku, odmah prilikom otvaranja će se na računalo žrtve instalirati zlonamjeran kod bez njezina znanja. Iako ima mnogo različitih vrsta ranjivosti u web preglednicima, najčešće se radi o problemima unutar JavaScript-a ili nekih popularnih dodataka (npr. Flash Player).

Širenje *crimewarea* u obliku **internetskih crva** dobro je poznat način širenja. Internetski crvi su programi koji se sami mogu replicirati i proširiti putem Interneta na veliki broj računala. Za širenje obično koriste neke ranjivosti unutar operacijskog sustava ili drugih programskih paketa koji su popularni. Ovo je potpuno automatiziran način širenja, nema interakcije s mogućom žrtvom. Na ovaj način autori *crimewarea* mogu vrlo brzo stvoriti moćne mreže *botova*. Za primjer je moguće istaknuti *Conficker*, koji se u vrlo kratkom vremenu potpuno samostalno proširio na veliki broj računala na Internetu.

2.3 Kolike su štete od *crimewarea*?

Teško je procijeniti iznos štete koje *crimeware* alati nanose privatnim korisnicima i poslovnim organizacijama. Jedan dio organizacija koje su imale problema s *crimeware* alatima to nikada neće prijaviti u strahu od gubitka reputacije. Jedan dio njih možda nikada neće ni shvatiti da imaju problema s različitim *crimeware* alatima.

Određene podatke o štetama uzrokovanim *crimeware* alatima moguće je doznati iz FBI-eve godišnje ankete o stanju sigurnosti u poslovnim organizacijama. Na sljedećem grafu je prikazan prosječan novčani gubitak od različitih prijetnji informacijskoj sigurnosti unazad nekoliko godina.



Slika 2.4 - Prosječan financijski gubitak uzrokovan sigurnosnim incidentima

Izvor: [1]

Prema istom izvještaju, od svih prijetnji informacijskoj sigurnosti, najskuplja je krađa osobnih informacija i financijske prijevare uzrokovane zlonamjernim programima. Krađom osobnih informacija organizacije su oštećene za 710,000 dolara, a kod financijskih prijevara prosječna šteta je iznosila 450,000 dolara [1].

Osim izravne financijske štete, organizacije koje se suočavaju s *crimewareom* i posljedicama njegova djelovanja imaju problema s različitim zakonima koje oni krše. Većinom su to zakoni koji propisuju čuvanje i povjerljivost financijskih i osobnih podataka. Ukoliko *crimeware* ukrade povjerljive informacije, poslovna organizacija koja je oštećena krši zakon. To znači da bez obzira na to što je ona žrtva, može imati problema s zakonodavnim institucijama.

Osim izravne financijske štete i kršenja zakona, *crimeware* organizacijama može naštetiti ugledu. To je jedan od razloga zašto brojne organizacije ne prijavljuju incidente ili krađu. Svakoj organizaciji loš ugled u javnosti može direktno utjecati na ostvareni profit.

2.4 Kako se zaštititi?

Za ostvarivanje učinkovite zaštite od *crimewarea* dovoljno je slijediti općenite sigurnosne smjernice. Često je najjednostavnija zaštita i najučinkovitija.

Na računalo je svakako potrebno instalirati antivirusni alat. Poželjno je da u sklopu antivirusnog alata dolaze i različite funkcionalnosti kao što su zaštita od *spywarea*, vatrozid, tehnologija otkrivanja i prevencije nepoznatog zlonamjernog koda (eng. *host-based instrusion prevention system*) itd. Važno je osigurati redovite nadogradnje antivirusnog alata. No, budući da antivirusni alati ne mogu otkriti sve primjerke zlonamjernog koda, oni nisu dovoljna zaštita.

Dobra praksa je praćenje novosti vezanih uz *crimeware* i pojavu novih oblika zlonamjernog koda. Takva informacija može pomoći u prevenciji napada budući da obično uz izvještaje o novim prijetnjama dolaze i preporuke kako prijetnju neutralizirati.

Osim informiranja, važno je redovito ažurirati sav softver koji se na računalu koristi. Od operacijskog sustava do aplikativnog softvera. Ova preporuka se posebno odnosi na softver koji dolazi u kontakt s datotekama preuzetim s Interneta kao što su PDF čitači (Acrobat Reader, FoxitReader) ili web preglednici koji su danas izloženi velikim napadima s interneta.

Kod interakcije s drugim ljudima putem interneta treba postupati pažljivo. Preporučuje se ne slijediti nepoznate i sumnjive poveznice u porukama elektroničke pošte. Ukoliko neka poruka dolazi iz nepoznatog i sumnjivog izvora najbolje ju je pobrisati. Važno je razumjeti da banke nikada neće tražiti od svojih klijenata lozinke za pristup internet bankarstvu pa ukoliko se pojavi takva poruka znamo da je riječ o prijevari.

Treba pažljivo postupati i s porukama na društvenim mrežama. Ukoliko nas netko u porukama savjetuje da posjetimo sumnjivu stranicu ili pokrenemo neku sumnjivu datoteku na računalu moguće je da se radi o pokušaju prijevare.

3 Prikaz Zeus Botneta

Zeus je naziv alata za konfiguraciju i distribuciju zlonamjernog koda. Alat omogućuje izradu izvršne datoteke zlonamjernog koda i skup datoteka koje omogućuju izgradnju kontrolnog poslužitelja (PHP kod, slike, SQL naredbe). Izvršne datoteke izrađene istom verzijom alata razlikuju se samo u konfiguracijskim postavkama. Zbog toga se i same izvršne datoteke tog zlonamjernog koda nazivaju Zeus *botom*. Alat se nalazi u slobodnoj prodaji unutar internetskog podzemlja. Dostupne su verzije različitih mogućnosti s različitim cijenama.

Zeus je klasičan primjer opasnog *crimeware* softvera. Dizajniran je za krađu financijskih podataka s računala kojeg zarazi. Ukradene podatke Zeus dostavlja na udaljenje kontrolne poslužitelje. Osim krađe, Zeus omogućuje i udaljenu kontrolu nad zaraženim računalom.

Zeus je prvi puta otkriven 2007 godine kada je uspio ukrasti povjerljive podatke iz američkog ministarstva prometa. Vjeruje se da je potekao iz Rusije ili nekih od zemalja u kojima se koristi ruski jezik budući da je u prvim verzijama imao prateće datoteke sa sadržajem na ruskom jeziku. Ova pretpostavka do danas nije potvrđena budući da autori Zeusa nikada nisu pronađeni.

Od 2007. godine do danas, redovito su bile objavljenje nove verzije Zeusa. Svaka nova verzija donosila je nova poboljšanja i nove mogućnosti. Zahvaljujući tome, Zeus je stekao reputaciju iznimno kvalitetnog *bota* i danas je još uvijek aktivan. Svoju raširenost Zeus može zahvaliti činjenici da ga koristi mnoštvo različitih kriminalaca i kriminalnih skupina koje međusobno nisu povezane.

3.1 Globalna rasprostranjenost i širenje Zeusa

Pretpostavlja se da je Zeus od početka svog postojanja do danas ukupno zarazio milijune računala. Prema nekim izvještajima, samo je unutar Sjedinjenih Američkih Država oko 3,6 milijuna računala bilo pogođeno Zeusom. Impresivna je i brojka *phishing* poruka koje Zeus može poslati. Samo do listopada 2009. godine Zeus je poslao oko 1,5 milijuna *phishing* poruka na Facebook.

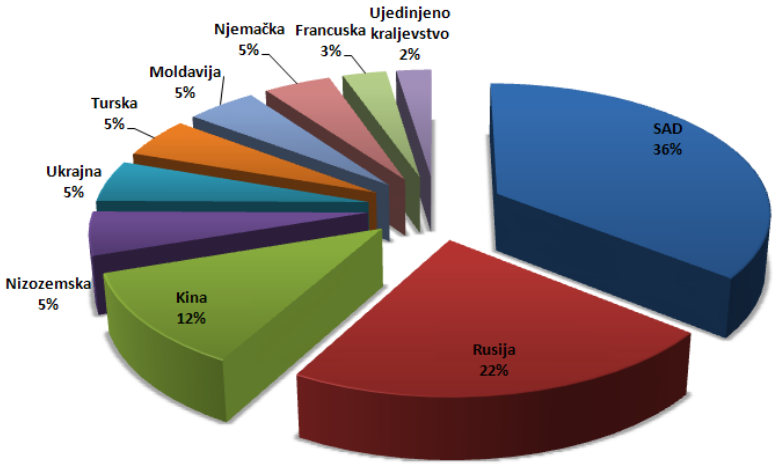
Zeusova geografska raspodijeljenost je globalna. Prisutan je u više od 196 zemalja. Sljedeća slika prikazuje trenutnu raspodjelu Zeusovih kontrolnih poslužitelja.

Slika 3.1 - Globalna rasprostranjenost Zeusovih kontrolnih poslužitelja

Izvor: [2]

Svaki crveni oblačić predstavlja jedan Zeusov kontrolni poslužitelj. Važno je naglasiti da jedan kontrolni poslužitelj može upravljati velikim brojem zaraženih računala, no kako je zaraženih računala jako puno, cijeli Zeus *botnet* je lakše pratiti po njegovim kontrolnim poslužiteljima.

Iz slike je jasna globalna prisutnost Zeusa. Udio pojedinih zemalja u raspodijeljenosti Zeusovih kontrolnih poslužitelja prikazan je na sljedećem grafu:

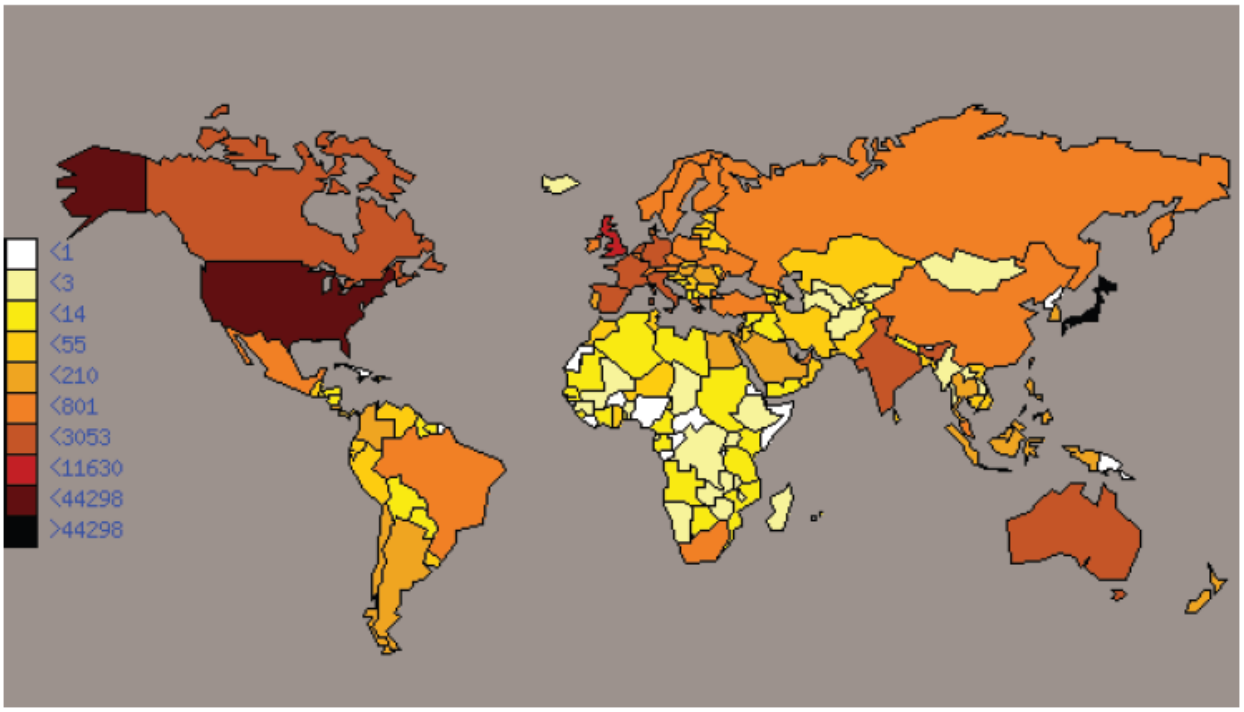


Slika 3.2 - Udio pojedinih zemalja u rasprostranjenosti Zeusa

Izvor: [3]

U SAD-u i Rusiji smješteno je više od pola kontrolnih poslužitelja. S distribucijom kontrolnih poslužitelja povezana je i distribucija zaraženih računala. Sljedeća slika prikazuje distribuciju samih zaraženih računala na svjetskoj karti. Slika vrijedi za listopad 2009. godine. Kako od

tog dana nije zabilježena nova velika pojava zaraženosti, slika vjerno oslikava i trenutno stanje.

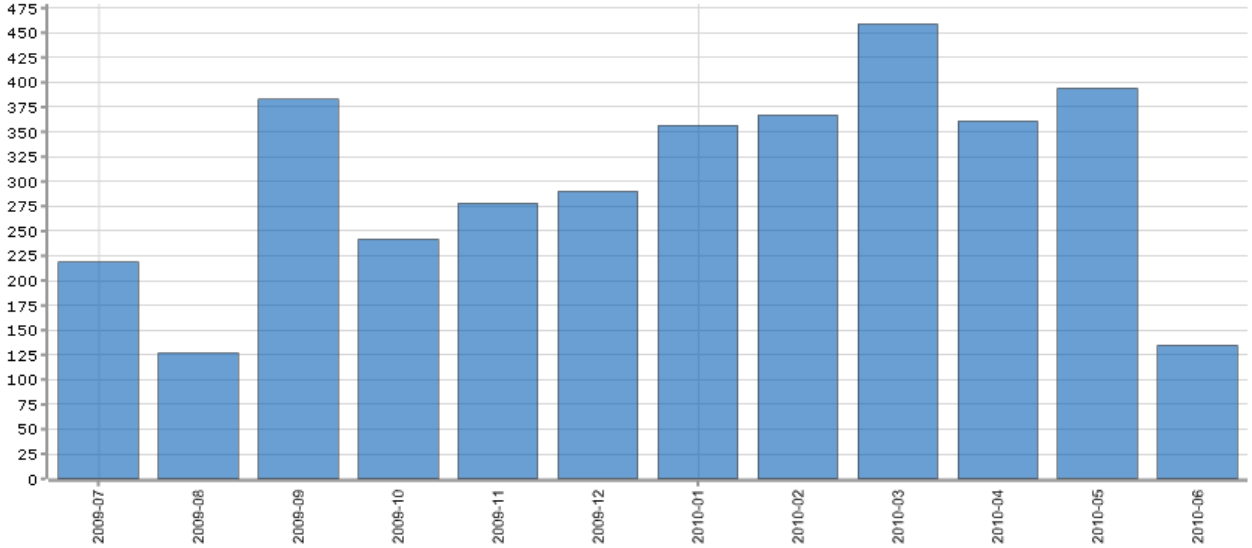


Slika 3.3 - Globalna rasprostranjenost računala zaraženih Zeusom

Izvor: [4 str. 2]

Ova slika samo je još jedan svjedok globalne rasprostranjenosti Zeusa i jasno upozorava na veliku opasnost koju on predstavlja za korisnike bilo gdje na svijetu.

Zeus je i danas aktivan što znači da se svaki dan pojavljuju nova računala koja su zaražena. Broj novih zaraženih računala unazad zadnjih nekoliko mjeseci prikazan je na sljedećem grafu.



Slika 3.4 - Broj novih zaraženih računala Zeusom unutar zadnjih nekoliko mjeseci

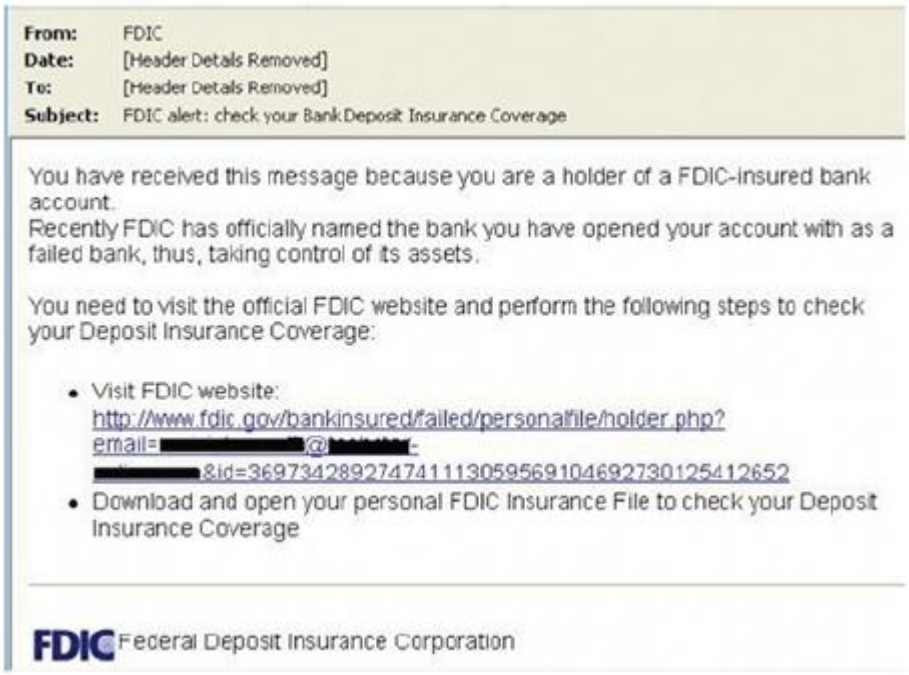
Izvor: [3]

Svaki mjesec je nekoliko stotina novih računala zaraženo Zeusom. Ovakav trend dokaz je otpornosti i fleksibilnosti Zeusa. Bez obzira što je Zeus poznat unazad tri godine, antivirusni alati ni danas ne mogu pružiti adekvatnu zaštitu korisnicima. Prema nekim izvještajima, potpuno ažurirani antivirusni softver može otkriti Zeus u samo 23% slučajeva [6].

Zeus ima nekoliko različitih načina širenja. No, dvije najpopularnije metode su putem:

- Društvenog inženjeringa
- *Drive-by downloads* tehnika

Društveni inženjering uključuje klasične tehnike varanja i nagovaranja moguće žrtve na instalaciju Zeusa. Zeus obično šalje velike količine SPAM poruka u kojima se predstavlja kao različite poznate organizacije (FDIC, MySpace, Microsoft, Facebook…) i od moguće žrtve traži da pokrene nepoznatu izvršnu datoteku. Jedna takva SPAM poruka prikazana je na sljedećoj slici:



Slika 3.5 - Primjer SPAM poruke koju šalje Zeus

Izvor: [4 str. 3]

U prikazanoj poruci korisnik se obavještava da navodno postoji problem s njegovim računom u banci. Korisnik se upućuje na rješavanje problema tako da posjeti određenu web stranicu s koje mora preuzeti nepoznatu izvršnu datoteku i pokrenuti ju. Naravno, izvršna datoteka je zapravo Zeus koji će nakon pokretanja zaraziti računalo.

Širenje putem ***drive-by downloads*** tehnike je automatizirani način širenja u kojemu nije potrebna interakcija korisnika. Zeus za ostvarivanje ove tehnike koristi sigurnosne propuste u web preglednicima kako bi mogao neopaženo na računalo žrtve preuzeti i pokrenuti vlastiti izvršni kod. Za žrtvu je dovoljno da posjeti zlonamjernu web stranicu koja će početi *drive-by download* napad. U toj vrsti napada, na računalo žrtve se bez njezina znanja i pristanka automatski preuzima neki sadržaj s interneta. To je moguće ostvariti putem ranjivosti unutar web preglednika ili ukoliko je web preglednik nepravilno podešen.

3.2 Tehnički detalji funkcioniranja Zeusa

Prilikom prvog pokretanja Zeus će se na računalo instalirati u nekoliko koraka. Koraci se razlikuju ovisno o tome da li Zeus ima administratorske ovlasti ili ovlasti običnog korisnika. Koraci koje Zeus izvršava kako bi se instalirao na računalo su:

1. Kopiranje izvršne datoteke u `%system32%` direktorij pod imenom `sdra64.exe`
2. Dodavanje putanje `%system32%\sdra64.exe` u registry ključ `HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon` pod vrijednost `UserInit` kako bi osigurao automatsko pokretanje prilikom podizanja računala.
3. Umetanje koda u proces `winlogon.exe`. Glavna izvršna datoteka u ovom trenutku završava s radom.
4. Kod umetnut u `winlogon.exe` umeće novi kod u proces `svchost.exe` – taj kod je zadužen za krađu podataka.
5. Kod umetnut u `winlogon.exe` kreira direktorij `%System%\lowsec`. U taj direktorij sprema dvije datoteke: `local.ds` i `user.ds`. Prva sadrži konfiguraciju, a druga ukradene podatke.

U slučaju da Zeus nema administratorske ovlasti koraci su slični, osim što se razlikuju lokacije na koje on postavlja svoje datoteke. Izvršnu datoteku će postaviti u direktorij `%UserProfile%\Application Data`. Kod neće umetnuti u proces `winlogon.exe`, već u proces `explorer.exe`, a kako bi osigurao pokretanje prilikom podizanja računala upisati će putanju do svoje izvršne datoteke u registry ključ:

`HKCU\Software\Microsoft\Windows\CurrentVersion\Run`

pod vrijednost `UserInit`.

Prisutnost navedenih datoteka u ovim direktorijima i prisutnost navedenih vrijednosti u *registry* ključevima znak su da je računalo zaraženo Zeusom. Iz procesa instalacije jasno je da je Zeus gotovo jednako opasan ukoliko se na računalo instalira s administratorskim ovlastima ili ovlastima običnog korisnika. Stoga, zaštita od Zeusa nikako ne može biti rad na računalu pod nisko privilegiranim računom.

3.2.1 Krađa povjerljivih podataka

Glavna namjena Zeusa je krađa povjerljivih osobnih podataka. Većinom se cilja na podatke potrebne za obavljanje financijskih transakcija putem interneta. Baš kao što je prikazano na slici 2.1, Zeus krade podatke i sa tvrdog diska, ali i od korisnika dok ih on unosi prilikom prijave na neku stranicu za obavljanje financijskih transakcija.

Nakon što se Zeus pokrene on će automatski početi s krađom privatnih podataka pohranjenih u PSTORE (eng. *Protected Storage*) spremištu Windows operacijskog sustava. Na toj lokaciji bilo koja aplikacija može pohraniti privatne podatke korisnika. Podaci su sigurno pohranjeni i nije ih moguće mijenjati, ali ih je moguće čitati i za Zeusa je to dovoljno.

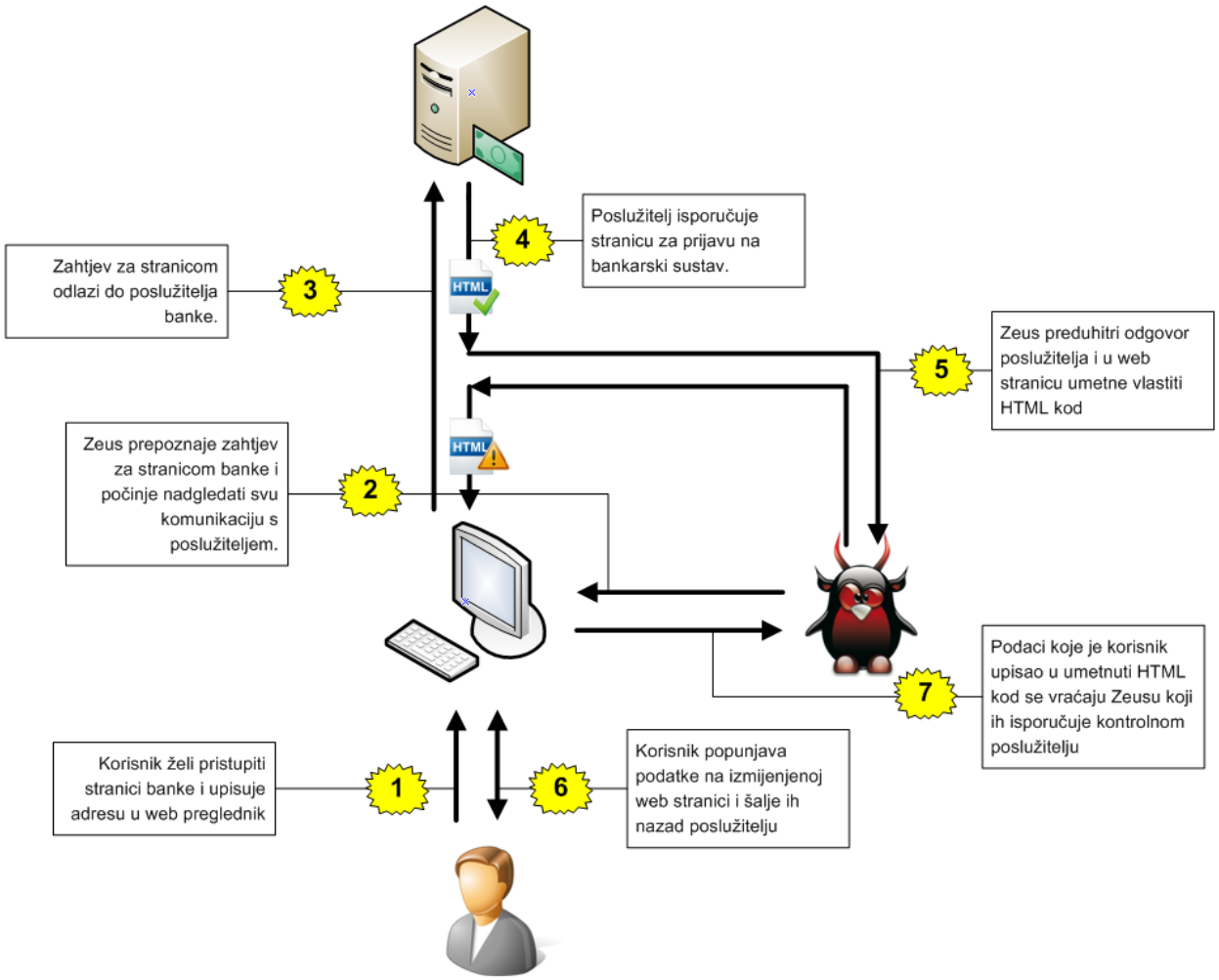
Također, Zeus će automatski presretati bilo koju nezaštićenu FTP ili POP3 komunikaciju kako bi mogao ukrasti lozinke za te servise.

Glavni način na koji Zeus krade podatke definira se uz pomoć dinamičke konfiguracije. Dinamička konfiguracija je pohranjena u datoteci `local.ds` i nju upravitelj bota može

mijenjati po volji. Postoje brojni parametri pomoću kojih je moguće odrediti ponašanje. Neki od njih su:

- `url_loader` – Lokacija za ažuriranje cijelog *bota*. S ove adrese *bot* skida novu verziju izvršne datoteke
- `url_server` – Adresa kontrolnog poslužitelja s kojeg Zeus preuzima nove verzije konfiguracijske datoteke i s kojeg prima naredbe.
- `WebFilters` – Lista URL-ova koje Zeus treba nadgledati. Bilo koje podatke poslane na neki od tih URL-ova Zeus će zabilježiti i poslati na kontrolni poslužitelj.
- `WebFakes` – Definira preusmjeravanja URL adresa. Jedan URL preusmjerava na drugi. Zeus to koristi kako bi radio *phishing* napade. Preusmjerava legalni URL na URL koji sadrži lažnu kopiju stranice neke banke. Kada korisnik unese podatke na toj lažnoj stranici oni se isporučuju napadaču.
- `DNSMap` – Unosi koje Zeus *bot* dodaje u *hosts* datoteku zaraženog računala. Na taj način Zeus može zabraniti pristup nekom poslužitelju ili preusmjeriti pristup s jednog na drugi poslužitelj. Opet, preusmjeravanjem Zeus može napraviti *phishing* napad.
- `file_webinjects` – Naziv datoteke u kojoj se nalazi HTML kod koji će Zeus ubaciti u stranice bankarskih i financijskih institucija kako bi od korisnika mogao ukrasti povjerljive podatke.

Glavni i najopasniji način krađe podataka je pomoću umetanja stranog HTML koda u web stranice koje korisnik posjećuje. Umetnuti HTML kod od korisnika traži da unese podatke koji zapravo nisu potrebni. Cijeli postupak napada umetanjem HTML koda prikazan je na sljedećoj slici:



Slika 3.6 - Napad umetanjem HTML koda u web stranice

Budući da Zeus HTML kod umeće direktno unutar web preglednika u zaštiti od ove vrste napada ne pomaže kriptiranje. Nažalost, korisnik teško može shvatiti da gleda web stranicu koja je izmijenjena na putu između legalnog poslužitelja i njega.

Na sljedećoj slici je prikazana i razlika između originalne i izmijenjene web stranice.

Slika 3.7 - Razlika između orginalne i izmjenjene web stranice

Izvor: [4 str. 5]

Zeus omogućuje i udaljenu kontrolu nad zaraženim računalom. Udaljena kontrola je ostvarena preko nekoliko različitih naredbi koje Zeus prepoznaje. Neke od naredbi su:

`reboot` – ponovo pokreće računalo,

`shutdown` – gasi računalo,

`rexec` – preuzima datoteku s interneta i pokreće ju na zaraženom računalu,

`lexec` – pokreće izvršnu datoteku na zaraženom računalu,

`getfile` – šalje datoteku ili cijeli direktorij upravitelju,

`block_url` – zabranjuje pristup određenom URL-u.

Zeus naredbe dobiva od kontrolnog poslužitelja nakon što pošalje ukradene podatke. Naredbe se Zeusu obično isporučuju u obliku skripte koju on u potpunosti mora izvršiti na zaraženom računalu.

3.2.2 Mrežna komunikacija Zeusa

Kako bi slao ukradene podatke i omogućio kontrolu, Zeus ima dobro razrađen mehanizam mrežne komunikacije.

Nakon što se Zeus pokrene na računalu, prvo šalje „M-SEARCH *“ upit na *broadcast* adresu 239.255.255.250, s UDP portom 1900. Riječ je o SSDP protokolu kojim Zeus pokušava otkriti postojanje različitih uređaja na mreži.

U prvom redu, Zeus cilja na otkrivanje različitih ADSL modema za širokopojasni pristup internetu. Ukoliko otkrije takav uređaj, pokušati će omogućiti napadaču da ga podesi putem UPnP protokola.

Komunikacija s kontrolnim poslužiteljem se odvija putem HTTP protokola, s time da se uspostavlja sigurni komunikacijski kanal u kojem su podaci kriptirani RC4 algoritmom. Ključ za kriptiranje se nalazi unutar same izvršne datoteke Zeusa i autor ga određuje prilikom izrade nove verzije izvršne datoteke.

Zeus prvo od kontrolnog poslužitelja dohvaća konfiguracijsku datoteku putem GET zahtjeva. Konfiguracijsku datoteku će dohvaćati u pravilnim vremenskim razmacima skroz dok bude aktivan.

Sve podatke koje Zeus prikupi šalje napadaču putem POST zahtjeva na URL adresu određenu u konfiguraciji. Slijedeća slika prikazuje jedan takav POST zahtjev. Važno je napomenuti da su na slici podaci prikazani u čitljivom obliku budući da su oni naknadno dekriptirani ključem kojeg Zeus koristi za kriptiranje.

Slika 3.8 - Prikaz podataka koje Zeus šalje kontrolnom poslužitelju (nakon dekripcije)

Izvor: [4 str. 5]

U ovom konkretnom primjeru podaci su ukradeni iz jedne HTML forme. Crvenom bojom je označen broj PIN-a koji Zeus šalje napadaču.

Za svaki POST zahtjev kontrolni poslužitelj će Zeusu odgovoriti s HTTP/200 OK. U odgovoru se mogu naći i naredbe koje Zeus mora izvršiti na zaraženom računalu. Dio jednog takvog odgovora prikazan je na sljedećoj slici. Crvenom bojom je označena naredba Zeusu da postavi početnu stranicu u web pregledniku na www.bing.com.

Slika 3.9 - Odgovor Zeusu s naredbom (nakon dekripcije)

Izvor: [4 str. 8]

Budući da Zeus za mrežnu komunikaciju koristi HTTP protokol, jako je teško odrediti pravila kojima bi njegova komunikacija mogla biti zaustavljena na nekom vanjskom vatrozidu. Situaciju dodatno otežava i činjenica da su svi podaci kriptirani tako da nije moguće napraviti ni uzorke pomoću kojih bi komunikacija bila zaustavljena.

3.2.3 Verzije i moduli Zeusa

Kao što je i prije bilo navedeno, Zeus je i danas u aktivnom razvoju i često se mogu pronaći nove verzije ovog zlonamjernog programa. U datotekama koje dolaze uz sam Zeus navodi se da su verzije brojčane oznake oblika: a.b.c.d, gdje promjena broja na mjestu:

- a označava kompletnu promjenu cijelog Zeusa
- b označava velike promjene koje mogu rezultirati smanjenom kompatibilnosti s prošlim verzijama
- c označava dodavanje novih mogućnosti, popravak pogreški i slično.
- d označava samo manje zahvate na kodu koji se provode kako bi Zeus izbjegao detekciju od strane antivirusnih alata

Zadnja javna verzija Zeusa je 1.2.7.19 [5]. S tom verzijom se aktivno trguje u podzemlju. Zadnja privatna verzija je 1.3.4 [5]. Ovom verzijom raspolaže autor i samo on je prodaje na crnom tržištu. Zanimljivo je da je autor zaštitio verziju Zeusa od kopiranja i daljnje distribucije.

Kada kupac prvi puta pokrene privatnu verziju Zeusa na računalu on generira jedinstvenu oznaku računala. Tu oznaku kupac mora poslati autoru kako bi dobio ključ s kojim može koristiti kupljenu verziju. Ovo je klasičan način zaštite autorskih prava prisutan u profesionalnom komercijalnom softveru. Kod Zeusa je prvi puta takva zaštita upotrjebljena za neki zlonamjerni kod.

Osim samog alata za izgradnju izvršne datoteke Zeusa, moguće je kupiti i dodatne module za njega. Svaki modul znatno unapređuje funkcionalnost Zeusa. Naravno, svaki modul ima i dodatnu cijenu koju kupac mora platiti. Neki od značajnih modula koji su prikazani u sljedećoj tablici, zajedno sa opisom i cijenom.

Tabela 3.1- Moduli Zeusa

Naziv modula	Cijena	Opis
Backconnect	1500$	Modul omogućuje napadaču da se spoji na zaraženo računalo i s njega obavlja financijske transakcije. Time zaobilazi provjere banke koje gledaju s koje lokacije neki korisnik obavlja transakcije.
Firefox form grabber	2000$	Modul koji omogućuje Zeusu da ubacuje HTML kod i u Firefox preglednik. Bez tog modula Zeus može

		izmijeniti web stranice samo kod Internet Explorer preglednika.
IM notifier	500$	Omogućuje napadaču da dobije ukradene podatke odmah nakon što ih Zeus ukrade. Podaci se isporučuju putem IM klijenta.
VNC	10 000$	Slično kao i backconnect, ali ovaj modul omogućuje potpunu prisutnost napadača na zaraženom računalu. Napadač dobiva pristup cijelom hardveru računala i svim programima. Čak mu je omogućen pristup i hardverskom čitaču *smart* kartica.
Windows 7 / Vista	2000$	Modul koji omogućuje Zeusu da zarazi i računala s Windows Vistom ili Windows 7 operacijskim sustavom.

3.3 Kako se zaštititi od Zeusa?

Nakon što su prikazane sve mogućnosti Zeusa postavlja se pitanje kako se zaštiti od tako naprednog oblika *crimewarea*. Nažalost, ne postoji jedinstvena metoda automatske zaštite. Zeus dolazi u mnogo različitih verzija i veliki broj tih verzija antivirusni alati ne prepoznaju. Čak ukoliko antivirusni alat može prepoznati neku verziju još uvijek ima problema u uklanjanju iste s zaraženog računala.

Zaštita se svodi na poštivanje standardnih sigurnosnih savjeta. Poslovnim organizacijama se preporučuje da za potrebe financijskih transakcija putem interneta koriste računalo koje se ne koristi za ništa drugo. Također, preporuča se i zamjena operacijskog sustava, ukoliko je moguće, organizacije bi morale koristiti operacijski sustav koji nije Windows XP.

Korisnicima se preporuča da nikako ne otvaraju sumnjive linkove unutar e-mail poruka koje dobiju. Važno je za korisnike da pripaze i na druge sumnjive poruke koje mogu doći putem Facebooka ili Myspacea. Čak ukoliko poruke dolaze od poznatih osoba treba kritički prosuditi njihov sadržaj.

Važno je da sav softver koji se koristi na računalu bude ažuriran zadnjim nadogradnjama, također potrebno je ažurirati i sam operacijski sustav, te redovito pratiti postoje li nove nadogradnje.

4 Zaključak

Crimeware je najopasniji oblik zlonamjernog koda. On može uzrokovati velike štete poslovnim, ali i privatnim korisnicima. Nažalost, s rastom komercijalne isplativosti interneta može se samo očekivati porast u broju novih primjeraka *crimeware* programa.

Na primjeru Zeusa pokazano je koliko štete može napraviti samo jedan oblik *crimeware* programa. Zeus zadivljuje svojim brojnim naprednim funkcionalnostima koje su u njemu implementirane. U vrlo kratkom roku je zarazio veliki broj računala i ukrao nebrojeno mnogo povjerljivih podataka. Zabrinjavajuće je što još danas nije pronađeno univerzalno rješenje za zaštitu od tog *crimewarea*.

Kako bi se mogla razviti zaštita od ovakvih zlonamjernih programa, potrebno je naporno raditi na obrazovanju i podizanju svijesti o informacijskoj sigurnosti. Samo velikim znanjem i pažljivim postupanjem u korištenju Interneta i svih njegovih resursa moguće je izbjeći neželjene probleme s *crimeware* alatima te pritom sačuvati svoju privatnost i financijska sredstva.

5 Literatura

[1]. **Kalafut, Andrew, Acharya, Abhinav i Gupta, Minaxi.** *A Study of Malware in Peer-to-Peer Networks.* Bloomington : Computer Science Department Indiana University, 2006.

[2]. **PIN Debit News Blog.** 2009 CSI Computer Crime and Security Survey. *PIN Debit News Blog.* [Mrežno] PIN Debit News Blog, 6. 1 2010. [Citirano: 14. 6 2010.] http://pindebit.blogspot.com/2010/01/2009-csi-computer-crime-and-security.html.

[3]. **abuse.ch.** Zeus Tracker. *Zeus Tracker.* [Mrežno] abuse.ch Zeus Tracker. [Citirano: 14. 6 2010.] https://zeustracker.abuse.ch/.

[4]. —. Zeus Tracker: Statistics. *Zeus Tracker.* [Mrežno] abuse.ch. [Citirano: 14. 6 2010.] https://zeustracker.abuse.ch/statistic.php.

[5]. **Falliere, Nicolas i Chien, Eric.** *Zeus: King of the Bots.* s.l. : Symantec, 2009.

[6]. **MalwareHelp.Org.** Find and remove Zeus. *Find and remove Zeus.* [Mrežno] MalwareHelp.Org, 19. 9 2009. [Citirano: 14. 6 2010.] http://www.malwarehelp.org/find-and-remove-zeus-zbot-banking-trojan-2009.html.

[7]. **Stevens, Kevin i Jackson, Don.** ZeuS Banking Trojan Report . *SecureWorks.* [Mrežno] SecureWorks, 11. 3 2010. [Citirano: 14. 6 2010.] http://www.secureworks.com/research/threats/zeus/?threat=zeus.

[8]. **Jakobsson, Markus i Ramzan, Zulfikar.** *Crimeware: Understanding New Attacks and Defenses.* Boston : Addison Wesley Professional, 2008. 0-321-55374-8.

[9]. **Emigh, Aron i Labs, Radix.** *The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond.* Whas : US Department of Homeland Security, 2006.

[10]. **Richardson, Robert.** *CSI Computer Crime & Security Survey.* s.l. : Computer Security Institute, 2009.

[11]. **Symantec.** *Symantec Global Internet Security Threat Report.* s.l. : Symantec, 2009.

[12]. **PANDA Security.** Crimeware: the silent epidemic. *PANDA Security info.* [Mrežno] PANDA Security. [Citirano: 14. 6 2010.] http://www.pandasecurity.com/homeusers/security-info/types-malware/crimeware/.

[13]. **Collins, Hilton.** CSI Computer Crime and Security Survey Shows Poor Security Awareness Training in Public and Private Sectors . *Computer Crime Research Center.* [Mrežno] Crime-Research, 12. 1 2010. [Citirano: 13. 6 2010.] http://www.crime-research.org/news/12.01.2010/3758/.

[14]. **Walsh, Sue.** Zeus Takes Aim at Firefox Users. *AllSpammedUp.* [Mrežno] 10. 5 2010. [Citirano: 14. 6 2010.] http://www.allspammedup.com/2010/05/zeus-takes-aim-at-firefox-users/.

[15]. **Microsoft.** PStore. *PStore.* [Mrežno] Microsoft, 13. 5 2010. [Citirano: 14. 6 2010.] http://msdn.microsoft.com/en-us/library/bb432403%28VS.85%29.aspx.