CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

SpyEye – nasljednik Zeusa

NCERT-PUBDOC-2011-07-328

Nacionalni CERT

Sadržaj

1 UVOD 3
2 INTERNET PODZEMLJE I EKONOMIJA BOTNETA 4
2.1 AUTOR ZLONAMJERNOG PROGRAMA 5
2.2 SPAMMERI I EXPLOIT ALATI 6
2.3 ŽRTVE I POSREDNICI 7
3 ZEUS I SPYEYE 8
3.1 VLADAVINA ZEUSA 8
3.2 POJAVA SYPEYEA I BORBA S ZEUSOM 10
3.3 SPAJANJE 11
4 MOGUĆNOSTI SPYEYEA 13
4.1 BOT BUILDER 13
4.2 MAN IN THE BROWSER NAPAD 14
4.3 MAN IN THE MOBILE NAPAD 15
4.4 BOGUS BILLING 16
4.5 SCREEN CAPTURING 18
4.6 SUČELJE ZA UPRAVLJANJE BOTNETOM 19
5 ZAKLJUČAK 24
6 LITERATURA 25

1 Uvod

Prije nešto više od godine dana, točnije krajem 2009. u svijetu računalne sigurnosti ime Zeus bilo je sinonim za moćan botnet koji se proširio gotovo po cijelome svijetu. Iako Zeus botnet nije bio najveći ikada zabilježen, sigurno je bio najopasniji. Naime zeus je razvijen samo s jednom svrhom – da svojim upraviteljima osigura veliku zaradu kroz krađu privatnih podataka nevinih žrtvi, prvenstveno ciljajući na kreditne kartice i podatke za Internet bankarstvo. U većoj mjeri u tome je i uspio budući da se štete od Zeusa mjere u milijunima dolara.

Od kraja 2009. godine do trenutka pisanja ovog dokumenta (sredina 2011) situacija se iz temelja promijenila, nažalost ne na bolje. Zeus je dobio konkurenciju u vidu novog zlonamjernog bota naziva SpyEye. Zbivanja unutar tog razdoblja svjedoče o tempu promjena u internetskom podzemlju a samim time i svijetu računalne sigurnosti. SpyEye je donio nove vrste napada i tehnički je profinjeniji od Zeusa. U početku se borio protiv njega, a potom su se (pomalo neočekivano) udružili.

Ovaj dokument u većoj mjeri posvećen je SpyEye botu kao novoj prijetnji za korisnike i financijske institucije na Internetu. Prijetnja koja je prisutna i u Republici Hrvatskoj budući da je SpyEye globalni problem koji se proširio po cijelom internetu.

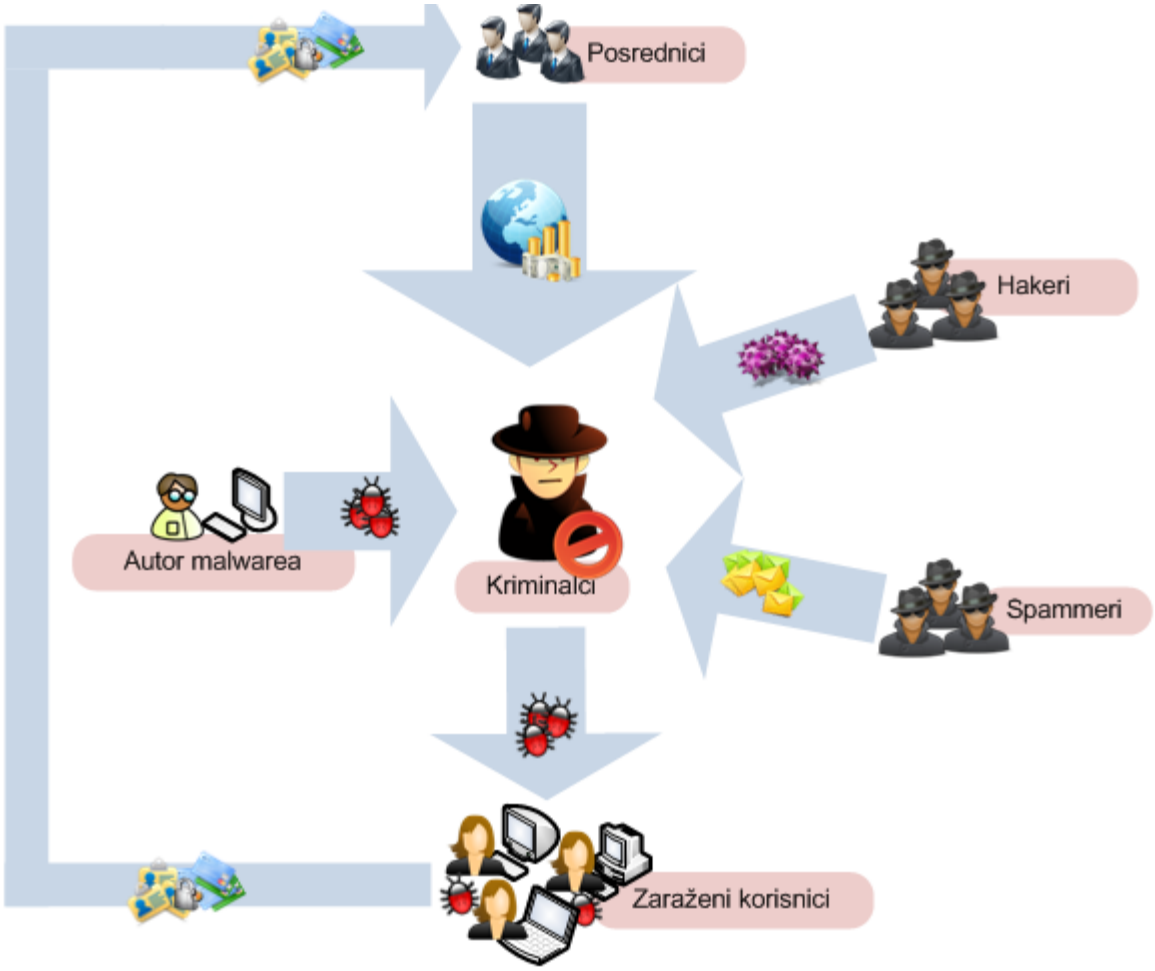
U prvom djelu dokumenta ukratko je opisan način funkcioniranja internetskog podzemlja s ciljem boljeg razumijevanja svih strana uključenih u funkcioniranje botneta. Drugi i treći dio dokumenta posvećeni su SpyEyeu. Opisana je njegova borba s Zeusom, udruženje te neke njegove značajnije mogućnosti.

2 Internet podzemlje i ekonomija botneta

U početku razvoja interneta i web-a sigurnosne prijetnje od zlonamjernih programa u usporedbi s današnjim prijetnjama bile su poput dječje igre. Tada je iza pojedinog crva ili virusa stajala samo jedna osoba koja ga je iz zabave proširila po Internetu. Najveća šteta koju je takav crv napravio bilo je rušenje ponekog poslužitelja ili zagušenje mrežne veze, a posljedice su se otklanjale relativno brzo.

Kako je sve više ljudi Internet počelo koristiti za kupovinu i bankarstvo, kriminalci su uočili priliku za zaradu putem pljačke nevinih korisnika. Kako bi u tome uspjeli kriminalcima su potrebni napredni zlonamjerni programi koji mogu krasti privatne podatke žrtava zaobilazeći razne sigurnosne mjere. Osim toga, potrebno im je i sredstvo širenja zlonamjernog programa te na kraju čitava mreža posrednika koji će ukradena sredstva prebaciti na račun kriminalca zamećući trag novca što je više moguće. Stoga, danas kada govorimo o botnetu ne govorimo o pojedincu koji je odgovoran za njega već o čitavom sustavu internetskog podzemlja koji ima dobro razrađenu ekonomsku stranu.

Sljedeća shema ukratko prikazuje način funkcioniranja cijelog tog sustava. Nakon sheme nalazi se pojašnjenje za pojedine sudionike unutar sustava.



Slika 2.1 - Prikaz sudionika u izgradnji botneta

U središtu cijelog sustava su **kriminalci**, tj. osobe koje žele zaraditi na krađi tuđih osobnih podataka. Oni će pokušati uspostaviti svoj botnet koji im osigurava zaradu. Iza jednog botneta ne mora stajati samo jedna osoba, već može biti riječ o čitavoj organizaciji pa u tome slučaju

možemo govoriti o organiziranom kriminalu. Kako bi uspješno uspostavili botnet oni se oslanjaju na druge sudionike u sustavu.

2.1 Autor zlonamjernog programa

Obično sve počne kada neki autor napravi zlonamjerni program koji može krasti kreditne kartice i podatke za Internet bankarstvo. Autor neće direktno koristiti svoj program da zarazi žrtve već će ga početi prodavati onima koji to žele – kriminalcima.

Najčešće autor oglašava svoj program na prikrivenim forumima gdje se okupljaju hakeri i kriminalci. Primjer jednog takvog oglasa dan je na sljedećoj slici. Radi se o oglasu za SpyEye bot.

Slika 2.2 - Oglas za prodaju SpyEye bota

Autor će svim zainteresiranim kupcima isporučiti svoj malware za određenu cijenu. Zanimljivo je da sve češće autor zapravo prodaje licence i baš kao što je slučaj s profesionalnim komercijalnim softverom licence imaju ograničen vijek trajanja, a sam malware brojne zaštite od korištenja neovlaštenih licenci. Osim toga, autor može prodati različitu funkcionalnost malware-a za različitu cijenu. Riječ je o posebnim dodacima koji omogućuju neki dodatni napad na korisnike. Cijena se formira na tržištu i ovisi o trenutnoj ponudi i složenosti pojedinih dodataka.

Autor malwarea kupcima obično isporučuje dvije komponente. Prva od njih je ***builder* za bot**. *Builder* kupcima omogućuje izradu primjerka malware-a koji oni moraju distribuirati. Koristeći *builder* kupci mogu razviti vlastitu konfiguraciju bot-a, odrediti koje mogućnosti žele koristiti i gdje će biti komandni poslužitelji. Na slici je prikazano sučelje *buildera* za SpyEye.

Slika 2.3 - Prikaz sučelja SpyEye buildera

Izvor: [1]

Druga komponenta koja se kupcima isporučuje je C&C poslužitelj. Najčešće je to web aplikacija koja kupcima služi za kontrolu svih zaraženih računala. Putem ove aplikacije kriminalci mogu izdavati naredbe botovima, prikupljati ukradene podatke ili ugasiti cijeli botnet.

Na kraju, za autore je važno naglasiti da su oni vješti programeri s velikim znanjem o funkcioniranju operacijskih sustava i sigurnosnih zaštitnih mjera, a budući da svoj softver ne koriste sami znatno manje su izloženi progonu.

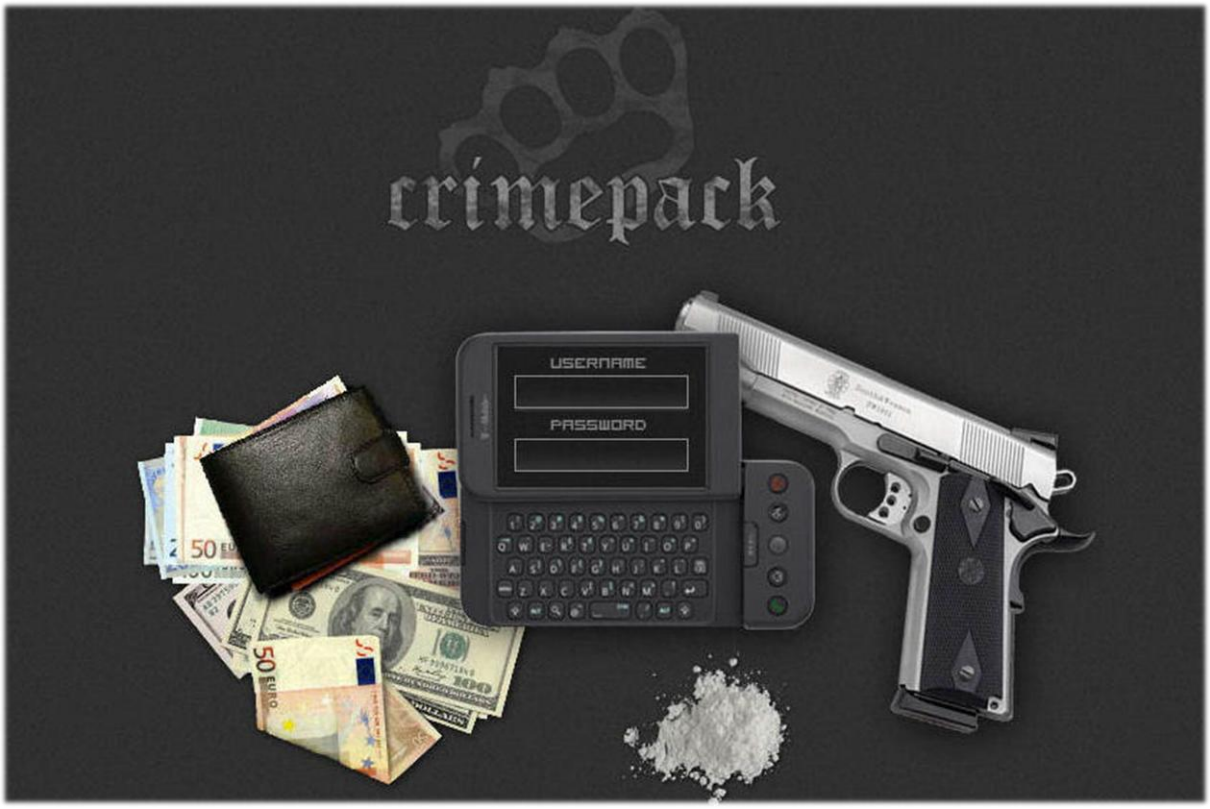
2.2 Spammeri i exploit alati

Kriminalac koji je kupio bot mora ga proširiti kako bi skupio dovoljan broj zaraženih računala da mu se njegov „pothvat“ isplati. Većina botova za krađu osobnih podataka nema mogućnost automatskog širenja – oni su programirani samo da zaraze računalo žrtve. Zbog toga kriminalci mogu u „suradnji“ s **spammerima** dogovoriti slanje velikih količina spam poruka u kojima se korisnike nagovara na instalaciju njihovog primjerka malware-a.

Također, postoje i alati posebno dizajnirani za automatsko širenje zlonamjernih programa. Takvi alati iskorištavaju ranjivost u nekom popularnom softveru (web preglednik, PDF preglednik itd.) kako bi neprimjetno izvršili programski kod na računalu žrtve. Programski kod koji se izvrši instalira bot na računalo žrtve.

Ovisno o tome koje programe napadaju, cijena tih alata može znatno varirati. Za alat koji se može širiti iskorištavajući ranjivost unutar popularnih web preglednika (Firefox ili Internet

Explorer) ili PDF preglednika cijene mogu biti iznimno visoke. Sljedeća slika prikazuje osnovno sučelje jednog exploit alata.



Slika 2.4 - Osnovno sučelje Crimepack exploit alata

Izvor: [2]

Riječ je o *crimepack* alatu. Kako exploit alati nisu tema ovog dokumenta navodimo samo imena nekih od njih: *Phoenix Exploit's kit*, *Fragus*, *Yes Exploit Kit* itd.

2.3 Žrtve i posrednici

Žrtve su ona računala na koja se uspješno instalirao bot i koja su od tog trenutka pod kontrolom kriminalaca. Često se u svijetu računalne sigurnosti takva računala nazivaju i zombi računalima. Njihov vlasnik nije svjestan činjenice da netko drugi upravlja njegovim računalom. Osim klasičnih računala u novije vrijeme ovdje se može govoriti i o pametnim telefonima. Kao što će kasnije biti pokazano, SpyEye može napasti i takve uređaje.

Kriminalci koji su s žrtvinih računala uspjeli ukrasti podatke za Internet bankarstvo i kreditne kartice neće financijska sredstva direktno prebaciti na račun pod svojom kontrolom. Time bi se izložili i povećali mogućnost da budu pronađeni. Za prijenos sredstava oni koriste cijeli niz **posrednika** iz različitih zemalja svijeta. Posrednici imaju zadatak novac s jednog računa, za malu proviziju, prebaciti na drugi. Često ne znaju da sudjeluju u pranju novca budući da ih kriminalci zapošljavaju na prijevaru, a osim u direktnom prijenosu sredstava, posrednici mogu sudjelovati i u kupovini lažne robe. U tome slučaju kriminalci uspostavljaju on-line trgovine u kojima se prodaje lažna roba.

3 Zeus i SpyEye

Zeus i SpyEye nisu jedini primjerci velikih botnet mreža koje su se pojavile u svijetu internet sigurnosti. Kao drugi primjer možemo istaknuti botnet naziva *Mariposa* koji se sastojao od 8 do 12 milijuna zaraženih računala. No, Zeus i SpyEye najpoznatiji su primjerci široj javnosti posebno zbog toga što su oni dizajnirani kao bankarski trojanci. Njihov primarni cilj nije generiranje spam poruka ili provođenje DoS napada, njihov primarni cilj puno je opasniji i to je vjerojatno razlog zašto su oni postali puno poznatiji.

U ovom djelu dokumenta osvrćemo se na funkcioniranje SpyEye zlonamjernog programa. Biti će prikazano kako onaj tko je kupio SpyEye izrađuje svoj primjerak zlonamjernog koda, kako on inficira žrtvu te kako se kontrolira cijeli botnet. Navedeno je i nekoliko napada kojima SpyEye zaobilazi sigurnosne zaštite unutar Internet bankarstva. No, prije svega, slijedi kratak osvrt na prilike u internetskom podzemlju – od vladavine Zeusa, preko borbe Zeusa i SpyEyea sve do njihovog ujedinjena.

3.1 Vladavina Zeusa

Zeus je prvi puta otkriven 2007. godine kada je uspio ukrasti povjerljive podatke iz američkog ministarstva obrane. Potječe iz Rusije, a njegov autor u internetskom podzemlju poznat je pod nadimkom *Slavik* ili *Monstr*.

U godini svojeg pojavljivanja Zeus nije zabilježio veći stupanj infekcije i samim time nije predstavljao veću opasnost za korisnike interneta. No, tijekom 2008. i 2009. godine situacija se drastično mijenja. Zahvaljujući neprestanom izdavanju novih verzija, Zeus je vrlo brzo uspio zaraziti mnogo računala i postao je jedan od najvećih botnetova na Internetu. To ilustrira i podatak od 3,6 milijuna zaraženih računala u SAD-u tijekom 2009. godine. Sljedeća slika prikazuje prostornu raspodijeljenost Zeusovih kontrolnih poslužitelja za vrijeme 2009. godine.

Slika 3.1 - Prostorna raspodijeljenost zeusovih poslužitelja 2009. godine

Zeus je zaista zavladao gotovo cijelim svijetom budući da je bio prisutan u više od 196 zemalja. Najviše su bile pogođene SAD, Rusija i Kina.

Ono što je Zeus činilo posebno uspješnim bila je brzina izdavanja novih verzija od kojih je svaka donosila nova poboljšanja i nove tehnike zaobilaženja antivirusnih alata.

Zanimljiva je i sama ekonomija vezana uz Zeus botnet. Autor Zeusa prodavao je licence za korištenje svojeg bota, a sam bot je imao ugrađenu zaštitu protiv kopiranja tako da je dozvoljavao izvršavanje na samo jednom računalu (odnosi se na alat za izgradnju botova). Cijena osnovnog paketa kretala se oko 4000 dolara, a bilo je moguće kupiti i pojedine dodatke koji su koštali mnogo više. Slijedi popis nekoliko dodataka s njihovim cijenama i kratkim opisom:

Tabela 1 - Neki od dodataka za Zeus bot

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.

3.2 Pojava SypEyea i borba s Zeusom

Krajem 2009. godine sigurnosni stručnjaci primijetili su pojavu novog zlonamjernog koda pod nazivom SpyEye. Riječ je bila o malwareu posebno dizajniranom za krađu podataka za Internet bankarstvo. Iako je tada imao nešto skromnije mogućnosti od Zeusa imao je iste ciljeve kao Zeus i bio mu je izravna konkurencija. O tome svjedoči i činjenica da je SpyEye imao mogućnost uklanjanja Zeusa s računala koje je on sam inficirao. Takva rivalstva između različitih skupina u internetskom podzemlju su česta i SpyEye je bio odlučan u namjeri da oduzme udio na tržištu od Zeusa.

Sljedeća slika prikazuje izgled starije verzije SpyEye *buildera* koja vlasniku nudi uključivanje opcije za deinstalaciju Zeusa (*Kill Zeus*).

Slika 3.2 - Sučelje SpyEye buildera

Izvor: [3]

Svaki bot kojemu je uključena ova opcija će prilikom infekcije žrtve potražiti znakove prisutnosti Zeusa, te ga ukloniti ukoliko te znakove i pronađe.

S tehničke strane, mogućnost uklanjanja Zeusa, izvedena je vrlo jednostavno. SpyEye nakon što inficira računalo žrtve traži komunikacijski kanal koji je na računalu prisutan samo ukoliko je ono već zaraženo Zeusom. SpyEye potom kroz komunikacijski kanal Zeusu pošalje naredbu da prekine s radom i obriše svoje izvršne datoteke. Kako Zeus nije programiran tako da raspoznaje tko šalje poruke putem komunikacijskog kanala on će naredbu izvršiti (ovo je jedan od mehanizama kojima se koriste i antivirusni alati u uklanjanju Zeusa). Važno je istaknuti da SpyEye ne uklanja sve tragove koji upućuju na zaraženost Zeusom već samo njegove izvršne datoteke.

Osim tehničkim trikovima, SpyEye se protiv Zeusa borio i na ekonomskom planu, nudeći znatno niže cijene od Zeusa. Osnovna verzija SpyEye koštala je samo 500 dolara.

Autor SpyEyea koristio je i agresivniji marketing za svoj proizvod. Ostavljao je poruke na brojnim hakerskim forumima. Imao je prijatelja koji mu je pomagao u reklami, budući da sam autor nije bio vješt s engleskim jezikom, a čak je pristao i na intervju preko interneta s Benom Koehlom – sigurnosnim stručnjakom iz Malware Intelligence organizacije. Slijedi prikaz nekoliko zanimljivih pitanja iz intervjua koja se tiču Zeusa i SpyEye-a, prevedenih na hrvatski jezik (Izvor: [4]). U ovom razgovoru autor SpyEyea ima nadimak *Gribodemon* a još je poznat i pod nadimkom *Harderman*.

Ben: Misliš li da SpyEye može postati velik i popularan kao Zeus?

Gribodemon: Da, mislim da hoće.

Ben: Da li je ekipa koja stoji iza Zeusa ljuta na tebe budući da si dodao mogućnost uklanjanja Zeusa s zaraženih računala?

Gribodemon: Ne.

Ben: Nisu ljuti jer bez obzira na to i oni zarađuju puno novaca?

Gribodemon: Da.

Ben: Misliš li da zarađuju više od 1kk (1 milijun) dolara godišnje?

Gribodemon**:** Zarađuju više od 1kk =)

Ben: Kako ti se čini konkurencija na tržištu za sada?

Gribodemon: Mislim da će uskoro svi trojanci imati ugrađen kvalitetan antivirusni softver kako bi mogli ukloniti druge, konkurentske, trojance s zaraženog računala.

Ben: To bi bilo nešto veliko, ali zar to nije puno posla za implementirati jednom autoru malwarea kao što si ti?

Gribodemon: Ni najmanje. Trojanac može samo prikupiti sve datoteke i programe koji se pokreću zajedno s računalom, poslati ih na viritest.com =) Ako je neka od tih datoteka zaražena – trojanac će ju obrisati.

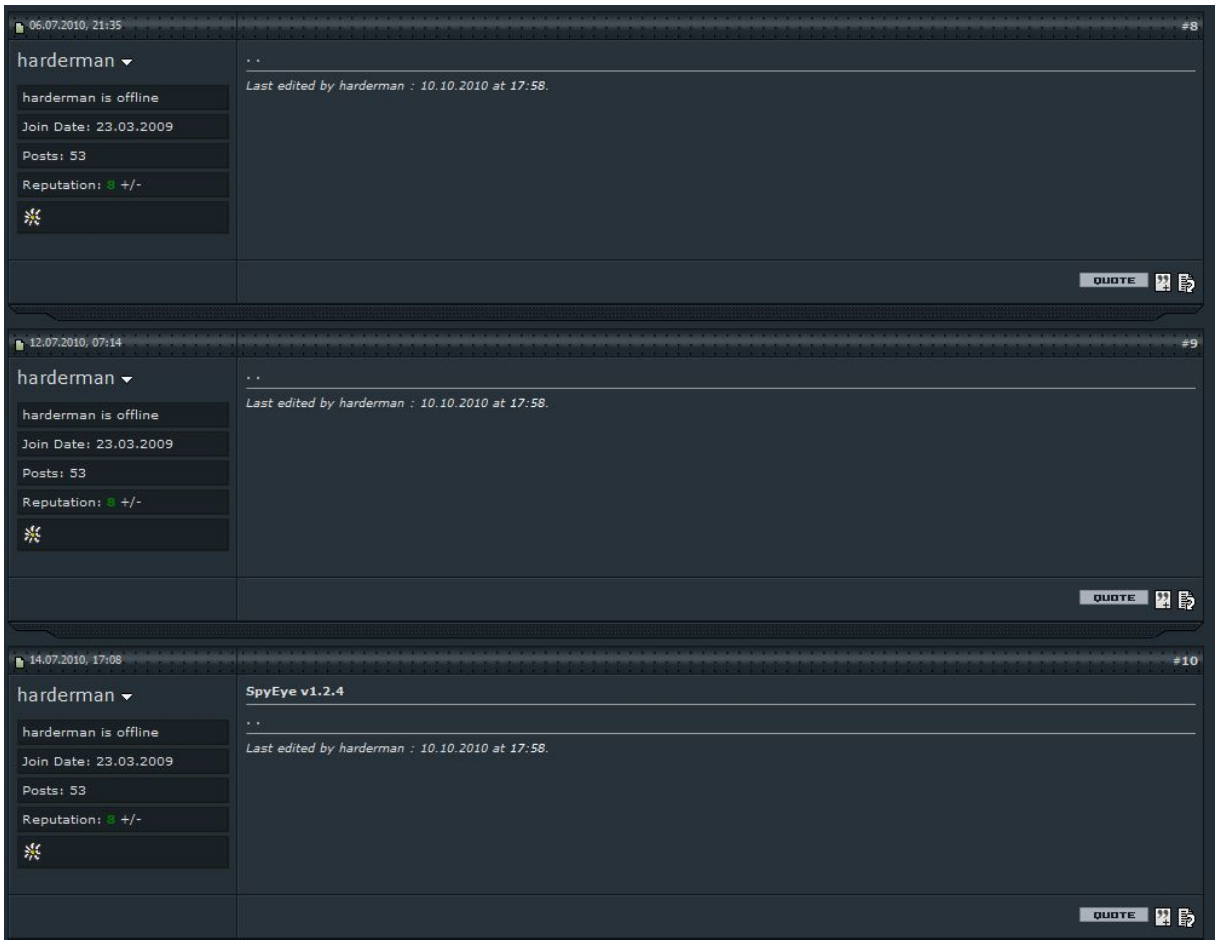
3.3 Spajanje

Kao što je već rečeno SpyEye se pojavio krajem 2009 godine. Dok nije prošao prvi kvartal 2010 godine. SpyEye nije imao značajniju ulogu u internetskom podzemlju, tada je počela borba protiv Zeus-a. No, borba nije trajala dugo. Već na jesen 2010. godine počele su se širiti glasine od ujedinjenu ova dva opasna primjerka zlonamjernog koda. Brian Krebs, novinar koji se specijalizirao za izvještavanje o temama iz računalne sigurnosti jedan je od prvih koji donosi ove vijesti na svojem blogu.

Početkom listopada korisnici na forumima internetskog podzemlja počeli su se žaliti kako ne mogu kontaktirati Hardermana (autora SpyEyea) za podršku. Nakon toga, 11. listopada Harderman je poslao poruku na jedan hakerski forum u kojem pojašnjava da će od toga dana

on biti zadužen za održavanje Zeus-a budući da mu je autor Zeusa predao izvorni kod i zamolio ga da on nastavi dalje. Istaknuo je da će svi klijenti koji posjeduju Zeusa dobiti 30% popusta na SpyEye i da će uskoro oba malwera biti ujedinjena u jedan moćniji i kompletniji malware.

U isto vrijeme Harderman je na svim forumima na kojima je reklamirao SpyEye mijenjao svoje kontakt podatke i brisao stare poruke s reklamama za SpyEye. Sljedeća slika prikazuje obrisane postove na jednom hakerskom forumu.



Slika 3.3 - Autor SpyEyea uklanja starije postove

Izvor: [5]

Prošlo je još neko vrijeme dok nisu zabilježeni prvi primjerci novog malwarea – koji se sastojao od Zeusa i SpyEyea. No, u siječnju 2011. godine postalo je jasno da vijest o udruženju nije samo glasina. Antivirusna Kuća TrendMicro prva je izvijestila i donijela slike nove verzije SpyEyea na svome blogu. U zaključku posta stoji kako je Harderman imao pomoć u izradi ove verzije SpyEyea (Izvor: [6]).

Ovakva nagla promjena u samo godinu dana svjedoči o tome koliko su Internet kriminalci prilagodljivi i nepredvidljivi. To stavlja veliki stres na antivirusne kuće i sigurnosne stručnjake koji moraju pronaći rješenja za sve nove prijetnje i zaštiti svoje korisnike. Pri tome se ne smiju iz vida ispustiti ni starije prijetnje. Sam Zeus je još i danas aktivan. Iako ne u istoj mjeri kao prije dvije godine, još uvijek može biti opasan budući da Internet kriminalci mogu koristiti starije verzije kako bi zarazili nespremne žrtve.

4 Mogućnosti SpyEyea

Ovaj dio dokumenta ukratko opisuje neke mogućnosti SpyEye malwarea. Iako je termin jedan, uvijek se misli na tri komponente:

- Bot builder – alat koji služi za izradu konfiguracije bota
- Bot malware – program koji inficira žrtvina računala i krade podatke
- C&C poslužitelj – poslužitelj koji kontrolira sve zaražene botove.

Svaka od ovih komponenti biti će ukratko opisana zajedno s nekim zanimljivim napadima koje SpyEye provodi. Nisu navedeni svi napadi budući da njih ima mnogo, već je kriterij bio izdvojiti one napade koji ciljaju na kompromitaciju sustava Internet bankarstva i online plaćanja.

4.1 Bot builder

Autor SpyEye malwarea svojim kupcima ne distribuira pripremljenu izvršnu datoteku već im daje poseban program nazva *builder* koji ima mogućnost izrade izvršne datoteke koja može inficirati računala korisnika. *Builder* je nužan. On omogućuje izradu različitih izvršnih datoteka ovisno o parametrima koje kupac unese.

Parametri se odnose na osnovni izgled i funkcioniranje izvršne datoteke. Kombinacijom različitih parametara kupac može izraditi različite verzije SpyEye malwarea i stvoriti različite botnet mreže. Sljedeća slika prikazuje izgled *buildera* za SpyEye verziju 1.3.34.

Slika 4.1 - Izgled SpyEye buildera za verziju 1.3.34

Iz samog sučelja može se iščitati koje parametre kupac SpyEyea proizvoljno određuje. Mora se upisati ključ za kriptiranje konfiguracijskih datoteka. Kupac može izabrati koje preglednike želi napasti s SpyEyeom. Također, moguće je odrediti ime izvršne datoteke i uključiti ili isključiti podršku za kompresiju.

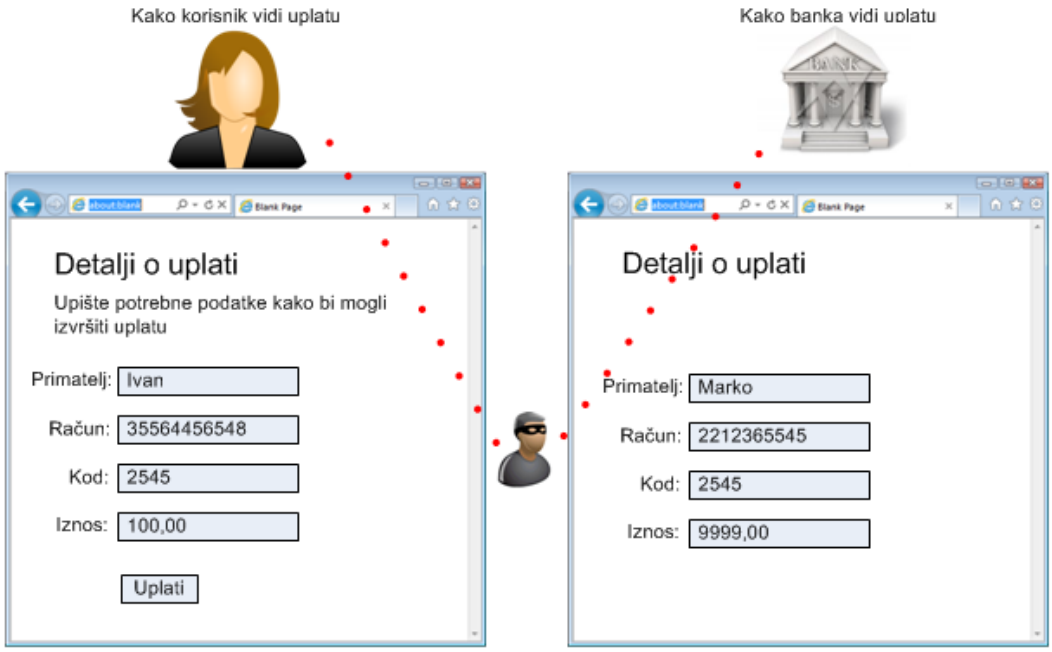
Važno je razumjeti da se builder ne koristi za upravljanje botnetom. Postoji poseban set softvera (najčešće u obliku web aplikacije) koji omogućuje uspostavu C&C poslužitelja i kontrolu nad čitavom mrežom botova putem konfiguracijskih datoteka. Zadaća *buildera* relativno je jednostavna. On omogućuje kupcima izradu osnovne verzije izvršne datoteke s kojom treba zaraziti računalo žrtve.

4.2 Man in the browser napad

Man in the browser (MITB) napad posebno je opasan oblik napada na korisnike Internet bankarstva kojim malware (kao što je SpyEye) može ukrasti povjerljive podatke ili financijska sredstva s računa korisnika.

Ulaz u Internet bankarstvo obično je zaštićen kriptografskim protokolima koji osiguravaju tajnost. Banke imaju valjanje certifikate što korisnicima služi kao dokaz identiteta, a koristi se i dvostruka autentikacija gdje se korisnik autenticira s bankom putem neke informacije koju samo on zna i onoga što samo on ima (npr. token uređaj). Sve ove mjere onemogućuju kriminalcima da kompromitiraju tuđe račune budući da im ne mogu ukrasti lozinke ili prisluškivati promet.

Zbog toga je razvijen MITB napad koji zaobilazi sve ove mjere zaštite. Napad se temelji na umetanju zlonamjernog koda u web preglednik koji korisnik koristi za pristup Internet bankarstvu. Zlonamjerni kod se može umetnuti putem dodataka ili ekstenzija koje podržavaju svi moderni preglednici. Budući da je zlonamjerni kod umetnut unutar preglednika on će imati pristup svim informacijama koje korisnik izmjenjuje s bankom i to nakon autentikacije. Također, kriptiranje neće pomoći u zaštiti budući da zlonamjerni kod može vidjeti podatke prije kriptiranja i nakon dekriptiranja. Sljedeća slika pokazuje što se u tome slučaju može dogoditi s Internet bankarstvom korisnika.



Slika 4.2 - Slikoviti prikaz MITB napada

U ovom pojednostavljenom modelu Internet bankarstva korisnik upisuje račun na koji želi prebaciti novčana sredstva i iznos sredstava. Kada klikne na *Uplati* zlonamjerni kod unutar preglednika će, bez znanja korisnika, promijeniti broj računa primatelja i iznos te zahtjev proslijediti banci. Zbog toga banka vidi drukčiji zahtjev za uplatom od onoga kojeg je korisnik izdao. Kada banka od korisnika zatraži konačnu potvrdu transakcije zlonamjerni kod će izmijeniti podatke o plaćanju na one koje je korisnik na početku upisao i potom korisniku predstaviti zahtjev.

Ovakav napad moguće je provesti protiv svih modernih web preglednika budući da svi dopuštaju ugradnju proizvoljnih programskih dodataka (eng. *extensions, plugins*). Zlonamjerni programski kod koji provodi napad mora biti prilagođen za određenu vrstu Internet bankarstva, zato što različite banke imaju različite sustave Internet bankarstva. Zbog toga se autori koncentriraju na najpoznatije i najpopularnije banke.

Jedina učinkovita mjera zaštite protiv ovakvog napada je verifikacija transakcije nekim drugim komunikacijskim kanalom koji ne uključuje web preglednik.

4.3 Man in the mobile napad

Man in the mobile napad sličan je prethodno opisanom napadu s zlonamjernim kodom unutar web preglednika. No za razliku od tog napada, ovdje se radi o napadu na one sustave Internet bankarstva koji koriste mobilne uređaje za autentikaciju i verifikaciju pojedinačnih transakcija. Sve veći broj banaka svojim korisnicima omogućuje korištenje mobilnih telefona za autentikaciju u sustavu Internet bankarstva. Procedura uključuje nekoliko koraka:

1. Korisnik dolazi na stranicu banke i prijavljuje se sa svojim korisničkim imenom i lozinkom
2. Banka potom korisniku šalje SMS poruku koja sadrži TAN broj
3. Korisnik TAN broj iz SMS poruke upisuje na stranici banke i dobiva pravo pristupa Internet bankarstvu.

Osim za autentikaciju, mobitel se koristi i za verifikaciju svake transakcije. Banka će prije nego provede nalog korisnika poslati SMS poruku na njegov mobitel u kojem pišu detalji o nalogu (iznos i broj računa). Kada se korisnik uvjeri da je to ispravan nalog on će ga potvrditi. Ovakva verifikacija čini *man in the browser* napade neučinkovitim budući da korisnik putem SMS poruke može provjeriti koji nalog je banka zaprimila. Ukoliko se ti podaci ne slažu s onima što je korisnik upisao, on će zaustaviti transakciju.

SpyEye (i Zeus) imaju mogućnost infekcije mobilnih telefona korisnika s ciljem manipuliranja SMS porukama i zaobilaženja procesa autentikacije i verifikacije. Proces započne onda kada se korisnik sa zaraženog računala putem web preglednika prijavljuje za Internet bankarstvo svoje banke. U web preglednik je ubačen zlonamjerni kod koji će u ovom slučaju u web stranicu za prijavu na Internet bankarstvo ubaciti dvije dodatne forme koje korisnik mora popuniti. Tamo će korisnik morati odabrati model svojeg mobilnog telefona te upisati IME i telefonski broj. Sljedeća slika prikazuje kako forma izgleda na slučaju jedne španjolske banke.

Slika 4.3 - Lažna polja za unos podataka o mobitelu

Podaci se traže pod izlikom da je potrebno obaviti nadogradnju sigurnosnog certifikata na mobitelu. Korisnik koji tražene podatke unese dobiti će SMS poruku u kojoj ga se upućuje da novi sigurnosni certifikat preuzme s web stranice. Naravno, nije riječ o pravom sigurnosnom certifikatom već o verziji malwarea za mobilni uređaj korisnika. Jednom kada korisnik prihvati instalaciju malware-a on će zaraziti mobitel i u pozadini nadgledati sve SMS poruke koje stižu.

Time malware, kao što je slučaj bio s *man in the browser* napadima može mijenjati sadržaj SMS poruka koje služe za verifikaciju transakcije ili sadrže TAN broj. Malware također ima mogućnost slanja podataka s mobitela putem SMS poruke kontrolnom poslužitelju.

Važno je naglasiti da SpyEye može zaraziti samo tzv. pametne telefone i trenutno samo one koji imaju BlackBerry ili Symbian operacijski sustav. Razumna je pretpostavka da će u skoroj budućnosti na meti autora SpyEye biti i mobitel s Android operacijskim sustavom ili čak iOS operacijskim sustavom.

4.4 Bogus billing

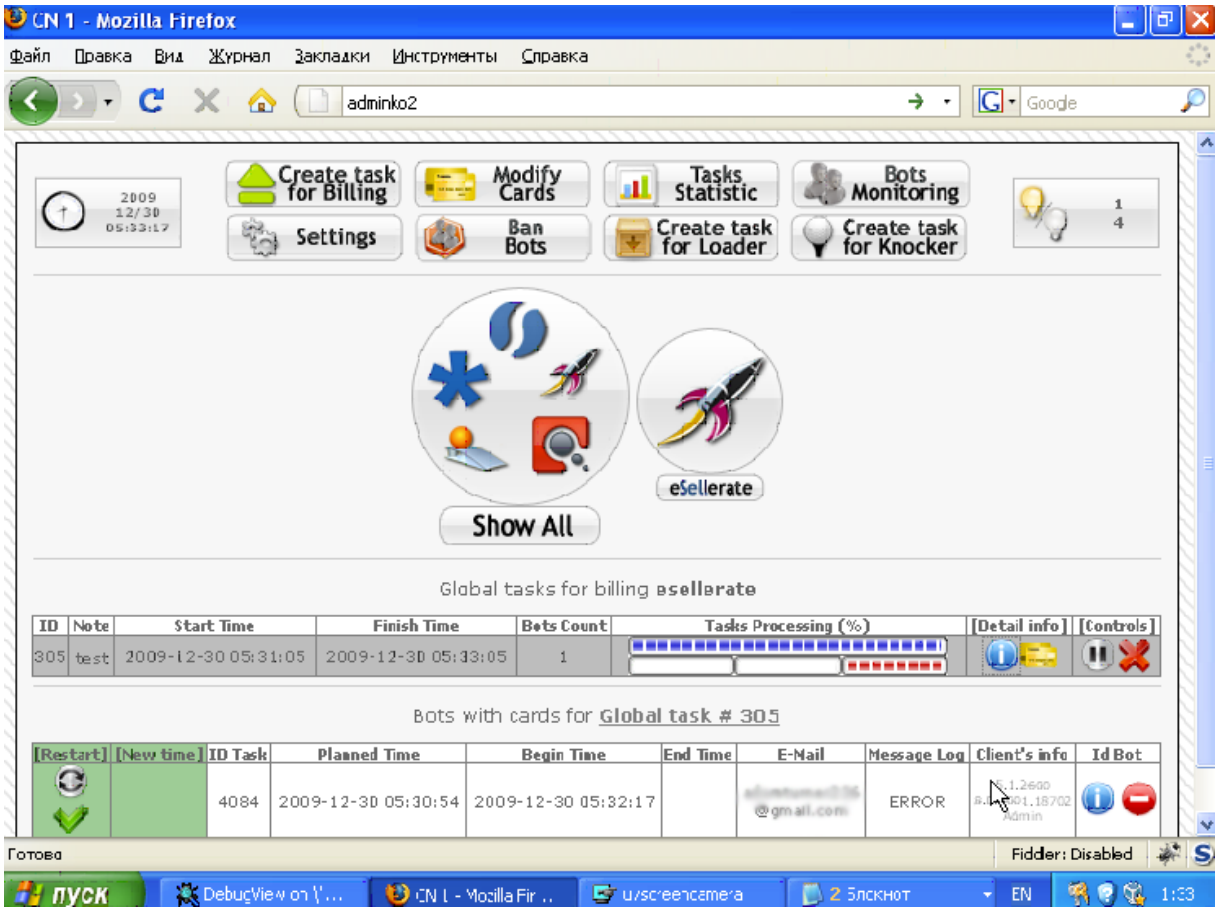
Još jedan u nizu kreativnih napada koje SpyEye može izvesti je i lažno naplaćivanje (eng. *bogus billing*). Ovaj napad orijentiran je na korisnike kreditnih kartica i kriminalcima omogućuje brzu krađu financijskih sredstava s korisničkih računa.

SpyEye malware ima mogućnost obavljanja automatske kupovine putem interneta koristeći brojeve ukradenih kreditnih kartica. Time on, ne samo da može krasti podatke o kreditnim karticama i isporučiti ih svojem vlasniku, već može obavljati uplate direktno s zaraženog računala.

Cijeli sustav funkcionira tako da kriminalac prvo nabavi robu koju želi prodavati. Najčešće se radi o lažnom ili ukradenom softveru koji ima samo malo promijenjeno ime i izgled. Kriminalac potom uspostavlja web shop gdje će SpyEye kupovati lažnu robu. Za uspostavljanje web shopova kriminalci često koriste već gotove on-line sustave koji omogućuju lakšu prodaju softvera i prikupljanje financijskih sredstava. Neki od takvih sustava su: *ClickBank, FastSpring* i *SetSystems.*

Kada je uspostavio web shop kriminalac se potom prijavljuje u kontrolno sučelje svojeg C&C poslužitelja i naređuje botovima da počinju s kupnjom njegovog softvera na web shopu na kojem se on nalazi. Autor pri tome može definirati razne parametre kao što su broj botova koji sudjeluju u kupovini, vremenski interval između dvije kupovine, početak kupovine, kraj

kupovine itd. Sljedeća slika prikazuje kontrolno sučelje SpyEye malwarea u kojem su prikazani zadaci za bogus billing.



Slika 4.4 C&C sučelje za bogus billing napad

Izvor: [7]

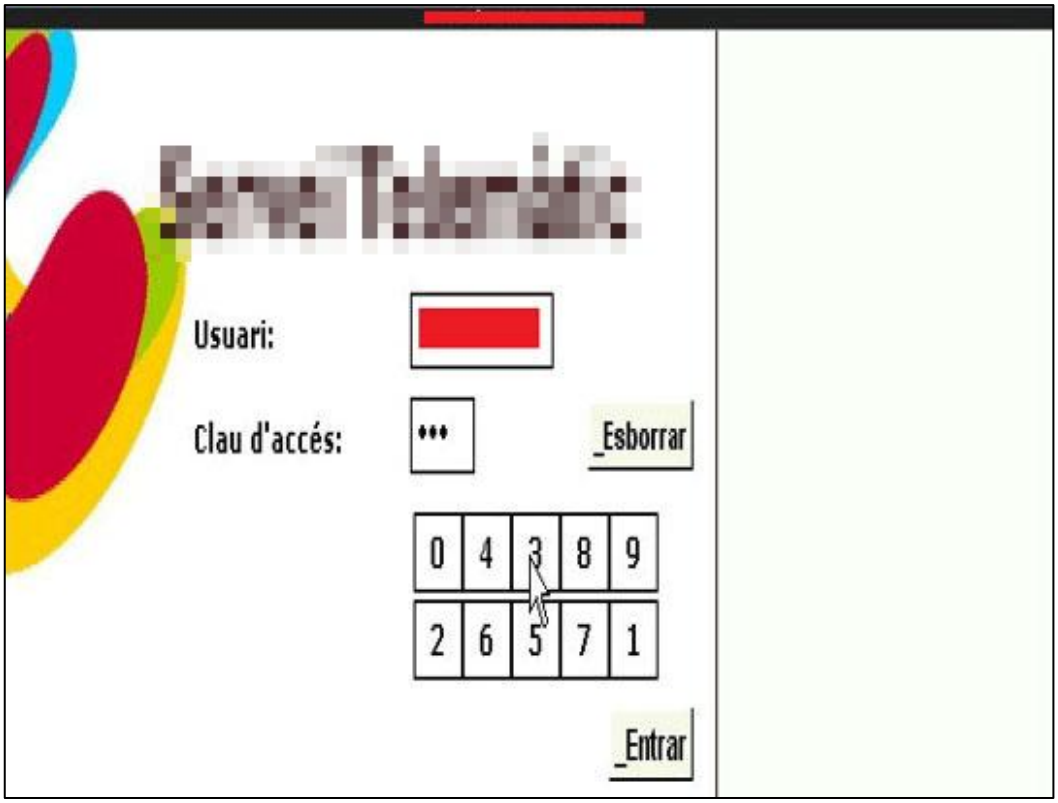
Zanimljivo je da SpyEye nudi mogućnost postavljanja lažnog proizvoda na vlastiti web shop sustav ili korištenje već gotovih webshop sustava koje je izgradio sam autor SpyEyea. Osim toga, SpyEye zaobilazi i zaštite od neovlaštenog korištenja kreditnih kartica koje se temelje na provjeri lokacije kupca. Zaštita funkcionira tako da zabrani kupnju ukoliko se kupac trenutno nalazi na neuobičajenoj lokaciji (daleko od svoje kućne adrese). SpyEye razumije tu zaštitu, te će za svaku ukradenu kreditnu karticu pokušati osigurati da kupnja dolazi s one IP adrese koja se fizički nalazi blizu kućne adrese ukradene kartice. SpyEye preusmjerava zahtjeve za kupnjom unutar svoje mreže botova.

4.5 Screen capturing

SpyEye ima ugrađeni keylogger koji omogućuje bilježenje svih pritisnutih tipki na zaraženom računalu. Time se mogu rekonstruirati sve informacije koje je korisnik unosio prilikom rada na računalu. To uključuje: korisnička imena, lozinke, poruke, brojeve kreditnih kartica…

S druge strane, postoje web stranice i programi koji pružaju zaštitu od keyloggera tražeći od korisnika da lozinku i korisničko ime unese pomoću miša služeći se pri tome tipkovnicom koja je prikazana na zaslonu računala (eng. *on-screen keyboard*).

Kako bi i u ovom slučaju mogao ukrasti lozinke SpyEye primjenjuje tehniku snimanja sadržaja zaslona. Svake sekunde će napraviti sliku cjelokupnog sadržaja zaslona na kojoj je prikazana pozicija miša, slike će redom kojim su slikane poslati na komandni poslužitelj. Slijedi prikaz jedne takve slike:



Slika 4.5 - Slika zaslona koju je SpyEye napravio

Izvor: [8]

Na slici se jasno vidi položaj miša. Niz od nekoliko ovakvih slika može otkriti bilo koju lozinku koju ili tajni podatak koji korisnik unosi putem virtualne tipkovnice.

SpyEye uzima sadržaj zaslona samo ukoliko korisnik posjeti neku web stranicu koja koristi ovakav način prijave. Drugim riječima rečeno, SpyEye ima okidače koji pokreću snimanje sadržaja zaslona samo kada se korisnik prijavljuje na poznate stranice koristeći virtualnu tipkovnicu. Ukoliko bi SpyEye stalno izrađivao slike zaslona zaraženog računala, bilo bi previše podataka za poslati kontrolnom poslužitelju.

4.6 Sučelje za upravljanje botnetom

Zadnje poglavlje ovog dokumenta posvećeno je kontrolnom sučelju SpyEyea. Ovdje se misli na sučelje koje kriminalcima omogućuje kontrolu nad svojim botnetom. Prije nego što budu izneseni detalji i slike sučelja važno je napomenuti da SpyEye danas vjerojatno ima drukčije sučelje nego ono što je ovdje prikazano. Čestim promjenama verzija SpyEye osigurava da ga je jako teško pratiti te time predstaviti njegovo sučelje.

No, bez obzira što slike nisu točne do najsitnijih detalja, one pružaju uvid u način rada SpyEye botneta, njegove kontrole i osnovne ideje – da upravljanje i održavanje botneta bude moguće uz nekoliko klikova mišem.

Osnovno sučelje, prikazano na slici, nudi izbornik iz kojega se mogu odabrati sve opcije za rad s SpyEye botnetom.

Slika 4.6 - Osnovni izbornik SpyEye C&C poslužitelja za SpyEye

Izvor: [8]

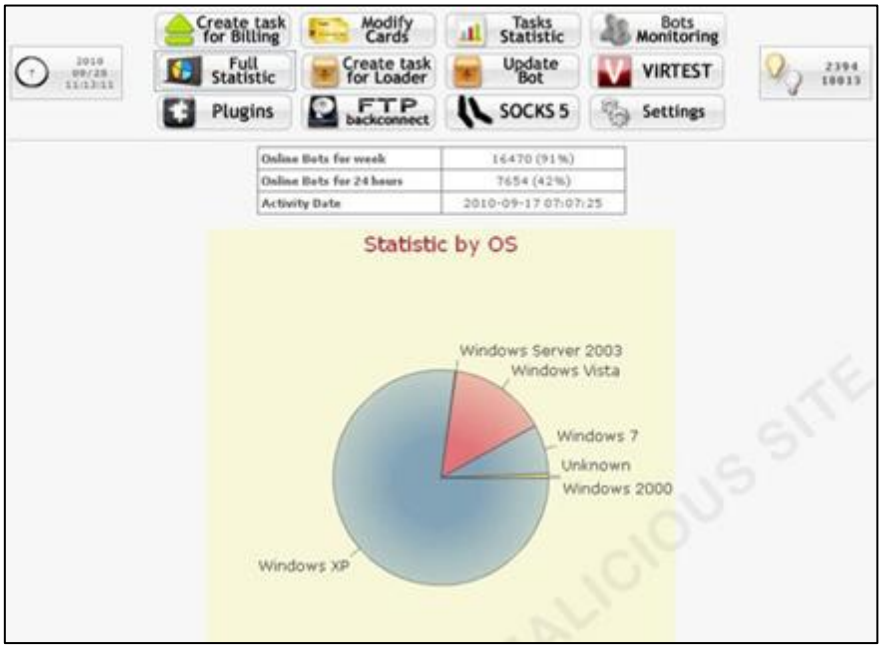
Osim izbornika prikazan je trenutni datum u lijevom uglu i broj aktivnih te svih botova u desnom uglu. Prva stavka na izborniku je opcija koja kriminalcima omogućuje izradu zadatka za *bougus billing* napad koji je opisan ranije u dokumentu. Samo sučelje za izradu tog zadatka prikazano je na sljedećoj slici:

Slika 4.7 - Sučelje za izradu BogusBilling zadatka

Izvor: [8]

Upravitelj botneta može odabrati vrijeme početka i završetka napada, upisati web stranicu na kojoj bot treba obavljati lažne uplate te upisati dodatne parametre ovog zadatka (brojeve kreditnih kartica itd.).

SpyEye omogućuje i različite statističke prikaze za svoje upravitelje. Na sljedećoj slici prikazan je raspored operacijskih sustava unutar zaraženih računala. Najveći postotak otpada na Windows XP računala.



Slika 4.8 - Statistika unutar SpyEyea

Izvor: [8]

Od ostalih opcija zanimljivo je istaknuti onu koja se krije pod nazivom *Create task for Looder*. Ovo opcija upravitelju omogućuje postavljanje zadatka botnetu da stalno posjećuje određenu stranicu kako bi generirao profit od reklama. Njezino sučelje prikazano je na sljedećoj slici:

Slika 4.9 - Sučelje za izradu zadatka za stvaranje lažnih klikova

Izvor: [8]

Zanimljivo je kako je moguće izabrati i Hrvatsku kao zemlju iz koje će dolaziti posjete za željenu stranicu.

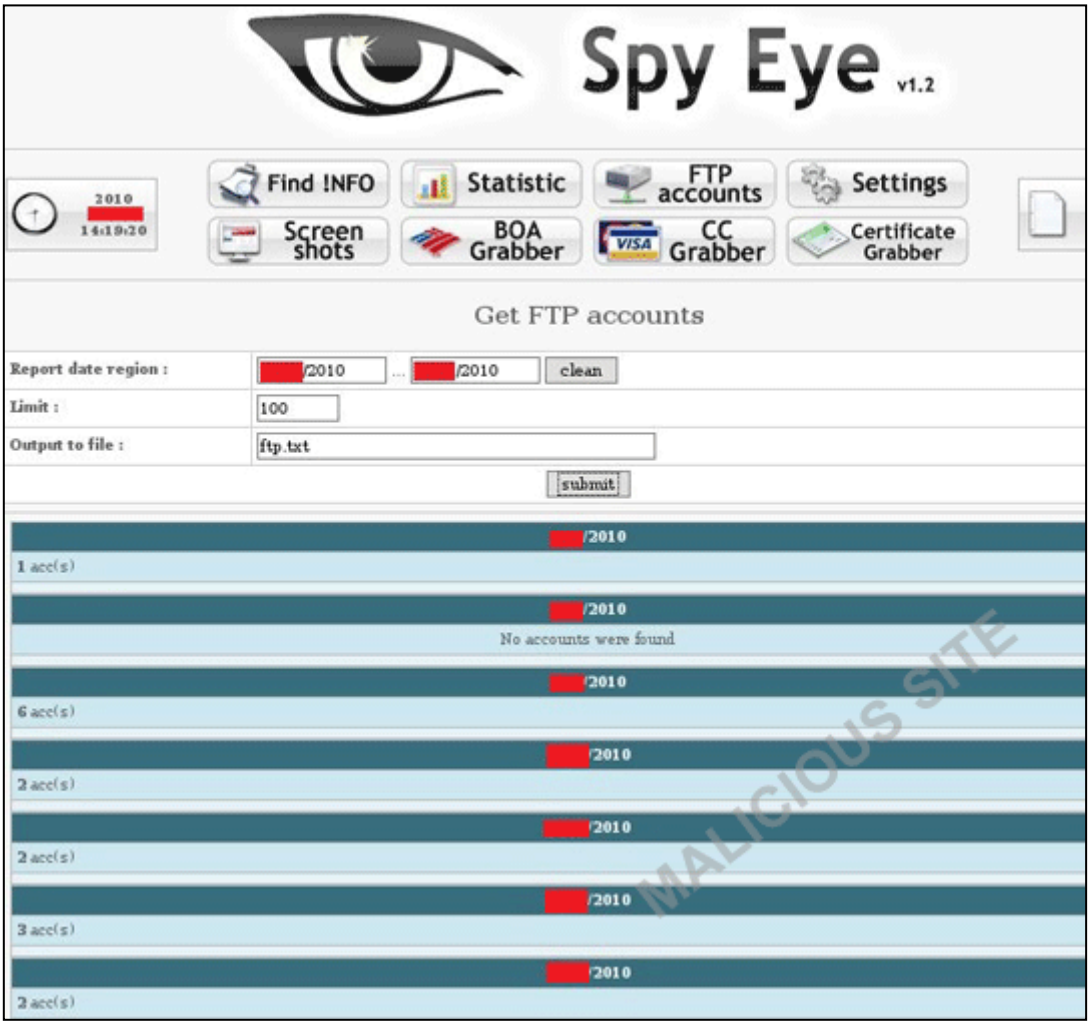
Gore prikazane slike odnose se na prvi dio SpyEye sučelja. On upraviteljima omogućuje kontrolu botneta, ažuriranje, unos novih zadataka, pregled statistika itd. SpyEye ima i drugi dio sučelja isključivo namijenjen pregledu ukradenih podataka (lozinke, brojevi kreditnih kartica itd.) Kao i prvi dio i drugi ima početni izbornik s nekoliko stavki (prikazan na sljedećoj slici).

Slika 4.10 - Početni izbornik sučelja za pregled ukradenih podataka

Izvor: [9]

Prva opcija na ovom izborniku je pretraživanje. Ona upravitelju omogućuje pretraživanje cjelokupne baze. Pretraživanje je moguće po jedinstvenoj oznaci bota, datumu, URL-u ili bilo kojem nizu znakova.

SpyEye omogućuje krađu FTP korisničkih računa. Ukradeni računi mogu se pregledati pod trećom opcijom u prvom redu izbornika. Kada upravitelj klikne na tu opciju vidi zaslon prikazan na sljedećoj slici.



Slika 4.11 - Pregled ukradenih FTP podataka

Izvor: [9]

Ovdje može odabrati u koju datoteku želi spremati ukradene FTP račune, a SpyEye će također prikazati koliko korisničkih računa je ukrao na koji dan.

Pod stavkom *settings* SpyEye upravitelju omogućuje odabir postavki za izradu redovitih kopija cijele svoje baze. Slika prikazuje kako izgleda sučelje.

Slika 4.12 - Postavke SpyEyea za izradu sigurnosnih kopija baze

Izvor: [9]

Upravitelj može upisati adresu na koju želi dobivati redovite sigurnosne kopije baze, učestalost izrade sigurnosne kopije, a također može podesiti SpyEye da izbriše cijelu bazu kako je nitko ne bi mogao pronaći.

U drugom redu postoji opcija za pregled ukradenih brojeva kreditnih kartica, certifikate te slika zaslona koje je SpyEye napravio. Klikom na opciju *Screen Shoots* SpyEye upravitelju nudi pregled svih slika zaslona koje je bot prikupio. Upravitelj prvo mora odabrati od kojeg bota želi pogledati slike. Potom dobiva sve slike zaslona koje je bot prikupio. Primjer takve slike već je dan u prošlom poglavlju, riječ je o slici na stranici 18.

Slično je i s ukradenim brojevima kreditnih kartica i certifikatima. SpyEye upravitelju omogućuje pretragu baze po kriterijima kao što su jedinstvena oznaka bota, vrijeme kada su podaci ukradeni, vrsti kreditne kartice itd.

5 Zaključak

Bankarski trojanci i botnet mreže veliki su problem informacijske sigurnosti. Sigurno je da ih razvijaju dobro organizirani programeri koji na njima ostvaruju veliki profit. Kriminalci koji ih koriste za izgradnju velikih botnet mreža također su dobro organizirani. Teško ih je otkriti i koriste sporost pravnog sustava i činjenicu da je za onesposobljavanje botneta potreba međunarodna suradnja.

SpyEye trenutno je najmoderniji primjerak bankarskih trojanaca. Uspješno zaobilazi veliki broj zaštitnih mjera ugrađenih u sustave Internet bankarstva, a činjenica da može zaraziti i neke mobilne telefone nagoviješta još jedan neugodan trend u kojem će se bitka za sigurnost korisnika preseliti i na mobitele.

Samo podizanjem svijesti o računalnoj sigurnosti i zajedničkom suradnjom svih uključenih strana se ovakve prijetnje mogu svesti na minimum.

6 Literatura

[1]. **Softpedia.** First Toolkit Resulting from ZeuS-SpyEye Merger Hits the Underground Market. [Mrežno] [Citirano: 13. 5 2011.] http://i1-news.softpedia-static.com/images/news2/First-Toolkit-Resulting-from-ZeuS-SpyEye-Merger-Hits-the-Underground-Market-3.jpg.

[2]. **McAfee.** An Overview of Exploit Packs. [Mrežno] 28. 5 2010. [Citirano: 20. 6 2011.] http://blogs.mcafee.com/mcafee-labs/an-overview-of-exploit-packs.

[3]. **Symantec.** Symantec. *Symantec.* [Mrežno] [Citirano: 10. 6 2011.] http://www.symantec.com/connect/sites/default/files/images/SpyEyeBuilder.JPG.

[4]. **Ben, Koehl i Jorge, Mieres.** *SpyEye Bot Conversations with the creator of crimeware.* s.l. : MalwareIntelligence, 2010.

[5]. **Krebs, Brian.** SpyEye v. ZeuS Rivalry Ends in Quiet Merger. [Mrežno] 24. 10 2010. [Citirano: 25. 5 2011.] http://krebsonsecurity.com/2010/10/spyeye-v-zeus-rivalry-ends-in-quiet-merger/.

[6]. **TrendMicro.** SpyEye/ZeuS Toolkit v1.3.05 Beta. [Mrežno] 24. 1 2011. [Citirano: 20. 6 2011.] http://blog.trendmicro.com/spyeyezeus-toolkit-v1-3-05-beta/.

[7]. **Krebs, Brian.** SpyEye Botnet's Bogus Billing Feature. [Mrežno] 17. 9 2010. [Citirano: 17. 6 2011.] http://krebsonsecurity.com/2010/09/spyeye-botnets-bogus-billing-feature/.

[8]. **TrendLabs.** The SpyEye Interface, Part 1: CN 1. [Mrežno] TrendLabs, 3. 10 2010. [Citirano: 13. 6 2011.] http://blog.trendmicro.com/the-spyeye-interface-part-1-cn-1/.

[9]. —. The SpyEye Interface Part 2: SYN 1. [Mrežno] TrendLabs, 15. 9 2010. [Citirano: 13. 6 2011.] http://blog.trendmicro.com/the-spyeye-interface-part-2-syn-1/.