ZAVOD ZA ELEKTRONIKU, MIKROELEKTRONIKU, RAČUNALNE I INTELIGENTNE SUSTAVE
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA
SVEUČILIŠTE U ZAGREBU

DIPLOMSKI RAD br. 1857

Određivanje reputacije autonomnih sustava zasnovano na praćenju neželjene pošte

Tomislav Friščić

Zagreb, rujan 2010.

Zahvaljujem svima koji su mi pomogli u izradi ovog diplomskog rada, posebice dr. sc. Stjepanu Grošu na stručnom vodstvu. Veliko hvala djevojci Ivani na pruženoj podršci i strpljenju.

Sažetak

U ovom diplomskom radu opisuje se problematika neželjene elektroničke pošte. Opisani su dijelovi poruke elektroničke pošte, pripadajući protokol SMTP kojim se poruke prenose od izvorišta do odredišta. Primjeri lažiranih poruka elektroničke pošte su također navedeni kao i metode kojima se pošiljatelji neželjene elektroničke pošte služe. Za potrebe praktičnog dijela opisani su i autonomni sustavi i način na koji se dolazi do više informacija o njima. Također, opisani su i sustavi koji se bave praćenjem pošiljatelja neželjene elektroničke pošte.

Kao praktični dio razvijen je sustav za praćenje reputacije autonomnih sustava temeljen na količini poslane neželjene elektroničke pošte, a prikazana je i statistika za nekoliko najvećih.

Abstract

This diploma thesis describes the problem of unsolicited e-mail known as SPAM. Parts of an e-mail messages are described along with the associated SMTP protocol by which the messages are transmitted from it's source to destination. Examples of falsified e-mail messages are given along with the methods that spammers use. Autonomous systems, along with the way the informations about them can be retrieved are described for the purpose of the reputation system. Systems that are engaged in tracking the spammers are also described.

A reputation system was developed as a practical part of this thesis. The reputation system monitors autonomous system based on the number of spam. The statistics for the several of the largest spamming autonomous systems is shown.

Sadržaj

1. Uvod....1
2. Poruke elektroničke pošte....3
2.1. Dijelovi poruke elektroničke pošte....3
2.2. Protokol za razmjenu poruka elektroničke pošte....7
2.3. Lažiranje poruke elektroničke pošte....10
2.4. Neželjena elektronička pošta....12
2.5. Mreže kompromitiranih računala....13
2.6. Tehnike zaustavljanja neželjene elektroničke pošte....17
2.6.1. DKIM....20
2.6.2. SPF....22
3. Autonomni sustavi....25
3.1. Protokol Whois....26
3.2. Primjeri malicioznih sustava....28
3.2.1. McColo mreža....28
3.2.2. Russian Business Network....29
4. Liste pošiljatelja neželjene elektroničke pošte....30
4.1. Spamhaus....31
4.2. Spamcop....38
4.3. Project HoneyPot....42
4.4. SORBS....48
4.5. APEWS....50
5. Reputacijski sustav....52
6. Zaključak....77
7. Literatura....78

1. Uvod

Internet se sastoji od mnoštva međusobno povezanih i administrativno nezavisnih autonomnih sustava koji su mahom usmjereni na komercijalne usluge. Prioritetni cilj je povećanje dobiti, tako da administratori autonomnih sustava nisu potaknuti na ulaganja u poboljšanja koja bi koristila Internetu kao cjelini, već samo na povećanje profita. Ovakvo stanje posljedica je nepostojanja središnjeg autoriteta koji bi jamčio za autonomne sustave i pratio njihov rad. Jedan od mogućih pristupa razrješenju tog problema je korištenje odgovarajućeg reputacijskog sustava za određivanje kvalitete autonomnih sustava koji se temelji na mjerenju određenih parametara, između kojih se ističe intenzitet generiranja neželjene elektroničke pošte.

Neželjena elektronička pošta (engl. *SPAM*) u današnje je vrijeme velik problem jer više ne predstavlja samo običnu smetnju, već i velik sigurnosni rizik, kao i povećane troškove korisnicima i pružateljima Internetskih usluga. Europska agencija za mrežnu i informacijsku sigurnost (ENISA) je pred kraj siječnja 2010. objavila istraživanje u kojem stoji da manje od 5% elektroničke pošte završi u sandučićima, tj. da je 95% neželjene elektroničke pošte [1].

Izvješće Spamhouse-a za lipanj 2010.[2] navodi izvore neželjene elektroničke pošte po regijama:

- Sjedinjene Američke Države – 44%
- Kina – 13%
- Rusija – 5.5%
- Velika Britanija – 5.2%
- Argentina – 5%
- Njemačka – 4.4%
- Brazil – 4.3%
- Kanada – 4.1%
- Rumunjska – 2.3%
- Japan – 2.3%

Izvješća drugih tvrtki, poput Cisco i Symantec prikazuju rezultate vrlo slične onima Spamhaus-a [4, 5].

No u zadnje vrijeme vidljiv je porast pružatelja Internetskih usluga u Europi koji žele korisnicima pružiti kvalitetnu uslugu pa tako ulažu velika sredstva u borbu protiv neželjene elektroničke pošte. 25% malih pružatelja izdvaja i do preko 10.000 EUR godišnje, dok trećina većih i preko 1.000.000 EUR [1]. Pri tome koriste razne tehničke i pravne metode. Najčešći tehnička metoda sprečavanja neželjene elektroničke pošte su crne liste (engl. *Blacklist*). Jedan od velikih razloga pozitivnog pomaka u borbi protiv neželjene elektroničke pošte je i mišljenje pružatelja Internetskih usluga da će boljom zaštitom privući više korisnika. Drugi razlog su veliki troškovi, budući da je slanje elektroničke

pošte relativno jeftino, dok je primanje i procesiranje višestruko skuplje, tako da se pružateljima Internet usluga borba protiv neželjene elektroničke pošte višestruko isplati. Problem je što pružatelji Internetskih usluga ne surađuju međusobno i ne razmjenjuju podatke što usporava cjelokupni proces.

Cilj ovog rada nije otkrivanje pošiljatelja neželjene elektroničke pošte, već pokušati pronaći pružatelja Internetskih usluga, tj. autonomni sustav s kojeg ta pošta pristiže. Pošiljatelji neželjene elektroničke pošte se u današnje vrijeme koriste specijaliziranim programima, mrežama kompromitiranih računala (engl. *botnet*) tako da je pronalazak originalnih pošiljatelja otežan budući da poruke ne dolaze od njih. No s više informacija o tome s kojeg autonomnog sustava dolazi neželjena pošta, možemo poduzeti određene radnje što u konačnici može dovesti do smanjenja dolazne neželjene elektroničke pošte i poboljšanja Interneta kao cjeline.

Rad je podijeljen u pet poglavlja. U drugom poglavlju općenito se opisuju sustavi elektroničke pošte. Ukratko je opisan protokol *SMTP*, koji služi za slanje poruka elektroničke pošte. Prikazani su i dijelovi poruke elektroničke pošte, s posebnim naglaskom na dijelove koji se mogu lažirati. Popisane su i ukratko objašnjene postojeće zaštite od neželjene elektroničke pošte. Posebno je opisana neželjena elektronička pošta, vrste i načini na koji se distribuira. Na kraju je dan i prikaz neželjene elektroničke pošte s obzirom na količinu poslanu po državama i s obzirom na tip oglašavanog materijala. Budući da su mreže kompromitiranih računala danas glavni izvor neželjene elektroničke pošte pobrojano je i detaljno opisano deset najvećih svjetskih kompromiranih mreža, njihova veličina, vrijeme nastanka, količina neželjene elektroničke pošte koje su u mogućnosti poslati, kao i tip oglašavanja kojim se bave.

U trećem poglavlju opisuju se autonomni sustavi. Dan je pregled i ukratko su objašnjeni tipovi postojećih autonomnih sustava. Budući da se ovaj rad temelji na vezi između IP adresa i njemu pripadajućih autonomnih sustava, posebno je objašnjen način na koji se dolazi do tih informacija. U nastavku su opisana i dva autonomna sustava, McColo koji je ugašen i Russian Business Network koji je još uvijek aktivan, najpoznatija dva sustava vezana uz mreže kompromitiranih računala.

Četvrto poglavlje bavi se crnim listama kao i postojećim sustavima i uslugama na Internetu temeljenim na njima i vezanim uz borbu protiv neželjene elektroničke pošte. Na početku se općenito opisuju crne liste, način na koji rade i što smo u mogućnosti napraviti sa traženim podacima. U nastavku su detaljno opisani vodeći Internetski sustavi i usluga, komercijalni i nekomercijalni, informacije koje su na njima dostupne, načine na koji sakupljaju podatke i načine na koje ih možemo koristiti.

Peto poglavlje vezano je u praktični dio rada. U njemu je prikazana shema reputacijskog sustava napravljenog za potrebe rada i opisana formula po kojoj se računa reputacija određenog autonomnog sustava. U nastavku su prikazani podaci za 22 sustava koji su u razdoblju od 15. srpnja do 15. prosinca poslali najviše neželjene elektroničke pošte na poslužitelj FER-a zajedno sa izračunom njihove reputacije.

2. Poruke elektroničke pošte

Elektronička pošta je sustav za razmjenu digitalnih poruka. Sustavi elektroničke pošte su bazirani na modelu "spremi i proslijedi", u kojem jedan poslužitelj primi i proslijedi poruku drugom poslužitelju, dok krajnji poslužitelj dostavljenu poruku sprema u ime korisnika, koji se samo treba spojiti na poslužitelj i preuzeti poruku. Ispočetka su se poruke elektroničke pošte direktno s računala pošiljatelja na primateljevo, bez posredstva specijaliziranih poslužitelja, dok je to danas vrlo rijedak slučaj. Također, u originalu su poruke bile samo tekstualnog tipa, no kasnije su nadograđene multimedijalnim dodacima, definiranim u RFC 2045 – 2049 po nazivom *Multipurpose Internet Mail Extensions* (MIME).

Korijeni elektroničke pošte sežu još iz doba *ARPANET*-a, a standard za poruke je predložen već 1973. godine u RFC-u 561. Poruke elektroničke pošte koje su slane u 1970-im godinama vrlo su slične današnjim. U početku su poruke bile prenošene putem protokola *FTP*, no danas se to obavlja putem protokola *SMTP* (Simple Mail Transfer Protocol, RFC 5321)

2.1. Dijelovi poruke elektroničke pošte

Poruka elektroničke pošte sastoji se od dva glavna dijela:

- Zaglavlje – Strukturirano u polja koja sadrže informacije poput pošiljatelja, primatelja i sl.
- Tijelo – Sadrži tekst poruke. Može sadržavati i potpis ili tekst koji je ubačen od strane pošiljateljevog sustava elektroničke pošte.

Zaglavlje je od tijela poruke odvojeno praznom linijom. Privitci, koji su opcionalni, nalaze se u tijelu poruke, a omogućeni su putem proširenja *MIME*.

Zaglavlje treba sadržavati slijedeća obavezna polja:

- *From*: Pošiljateljeva adresa elektroničke pošte. Smatra se da je ista kao i povratna adresa ako nije drugačije specificirano. Ispis 1, redak 11.
- *To*: Adresa elektroničke pošte, i opcionalno ime i prezime primatelja. Označuje primarnog primatelja poruke. Ispis 1, redak 12.
- *Subject*: Naslov poruke. Ispis 1, redak 10.
- *Date*: Lokalno vrijeme i datum pisanja poruke. Mnogi klijenti elektroničke pošte automatski ispunjavaju ovo polje pri slanju poruke. Ispis 1, redak 8.

Također, zaglavlje može sadržavati sljedeća opcionalna polja:

- *Received*: Prateća informacija dodana od strane svakog poslužitelja koji je obradio poruku. Pogodno za praćenje "puta" poruke. Ispis 1, redak 1, 2, 4, 5.
- *Content-Type*: Informacije o tipu tijela poruke u obliku tip/podtip. Ispis 1, redak 13.
- *References*: Identifikator poruke na koju je ova poruka odgovor. Sadrži sve identifikatore razmjenjenih povezanih poruka. Ispis 1, redak 7.

- *Message-id*: Informacija o izvorištu poruke. Sastoji se od identifikatora nakon kojeg slijedi znak "@" i ime poslužitelja. Ispis 1, redak 9.
- *MIME-Version*: Verzija formata tijela poruke koji se trenutno koristi. Ispis 1, redak 3.
- *Return-Path:* Adresa na koju se šalje odgovor na poruku. Ispis 1, redak 14.
- *In-Reply-To*: Identifikator poruke kojoj je ova poruka odgovor. Služi za spajanje povezanih poruka. Ispis 1, redak 6.

Primjer valjane poruke elektroničke pošte dan je u ispisu 1, svaki element zaglavlja nalazi se u zasebnom retku radi preglednosti. Iz primjera je izbačeno tijelo poruke radi preglednosti kao i dodatna polja u zaglavlju koja dodaju poslužitelji, a nisu bitna u ovom trenutku.

Ispis 1. Primjer zaglavlja poruke elektroničke pošte

```
01: Received: by 10.35.108.5 with SMTP id k5cs149489pym;
        Thu, 6 Jul 2006 08:06:22 -0700 (PDT)
02: Received: by 10.54.84.1 with SMTP id h1mr619007wrb;
        Thu, 06 Jul 2006 08:06:22 -0700 (PDT)
03: Return-Path: <korisnik@yahoo.de>
04: Received: from web52605.mail.yahoo.com (web52605.mail.yahoo.com
[206.190.48.208])
        by mx.gmail.com with SMTP id 14si2109403wrl.2006.07.06.08.06.21;
        Thu, 06 Jul 2006 08:06:22 -0700 (PDT)
05: Received: (qmail 82310 invoked by uid 60001); 6 Jul 2006 15:06:19
-0000
06: Message-ID: <20060706150619.82308.qmail@web52605.mail.yahoo.com>
07: Received: from [83.131.175.14] by web52605.mail.yahoo.com via HTTP;
        Thu,06 Jul 2006 17:06:19 CEST
08: In-Reply-To:
AANLkTi=iQsx_2G8s7FVXLWqq8po=5qDYXhR83oD7+Bnk@mail.gmail.com
09: References:
<AANLkTik0M_sBkfoDNevj68B7+fRG1uQJWZUAtdTKudaY@mail.gmail.com>
        <869292.25888.qm@web52607.mail.re2.yahoo.com>
        <AANLkTi=iQsx_2G8s7FVXLWqq8po=5qDYXhR83oD7+Bnk@mail.gmail.com
10: Date: Thu, 6 Jul 2006 17:06:19 +0200 (CEST)
11: From: "Yahoo korisnik" <korisnik@yahoo.de>
12: Subject: Test
13: To: tomislav@gmail.com
14: MIME-Version: 1.0
15: Content-Type: TEXT/PLAIN; charset=US-ASCII
```

U polju *From* u retku 11 nalazi se adresa pošiljatelja poruke koja je u ovom slučaju korisnik*@yahoo.de*, dok polje *To* (redak 13) predstavlja adresu na koju je poruka poslana i ona je *tomislav@gmail.com*. U retku 12 nalazi se polje *Subject* u kojem je naslov poruke, dok se u polju *DATE* (redak 10) nalazi oznaka datuma i vremena kad je poruka poslana, četvrtak 06. lipnja 2006 u 17:06:19.

Da je stvarno riječ o valjanoj poruci vidimo po identičnosti *Return-Path* i *From* polja (ispis 1, retci 3 i 11) u kojima se nalazi adresa izvornog pošiljatelja poruke.

Praćenjem *Received* polja možemo vidjeti put kojim je poruka prošla od izvora do odredišta. Polja su tako organizirana da je izvorište poruke zapisano u najnižem polju, tj. kako poruka prolazi više računala nova polja se dodaju na vrh. U ispisu 1, retcima 1 i 2

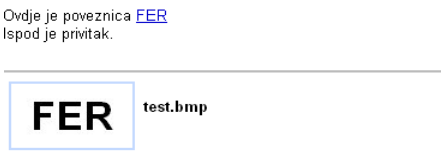
nalaze se lokalne IP adrese računala u ovom slučaju poslužitelja Google koji predstavljaju lokalna mrežu na samom poslužitelju kao i datum obrade poruke. IP adresa poslužitelja s kojeg je poruka stigla nalazi se u retku 4, ona je 206.190.48.208. Provjerom te IP adrese dolazimo do informacije da se zaista radi o poslužitelju s imenom *web52605.mail.yahoo.com*. Ono što je nama bitno nalazi se u retku 07, to je IP adresa pošiljatelja poruke koja je 83.131.175.14. Provjerom te IP adrese dolazimo do informacije da se pošiljatelj poruke nalazi na hrvatskom telekomu (T-Com).

U ispisu 1, retku 6 nalazi se identifikator poruke koji nam je bitan ukoliko imamo razmjenu poruka budući da se putem tog identifikatora one spajaju. U *References* polju koje se nalazi u retku 9 nalazi se lista u kojoj su zapisani svi identifikatori dosad razmjenjenih povezanih poruka. Identifikator poruke kojoj je trenutna poruka odgovor nalazi se u polju *In-Reply-To* u retku 8 i on se mora nalaziti i u *References* polju. To je u ovom slučaju identifikator koji se osim u polju *In-Reply-To* nalazi i na dnu liste u polju *References* a on je:

```
AANLkTi=iQsx_2G8s7FVXLWqq8po=5qDYXhR83oD7+Bnk@mail.gmail.com
```

Verzija formata tijela poruke zapisana je u polju *MIME-Version* u ispisu 1, redak 14 i u ovom slučaju je 1.0. Polje Content-Type u retku 15 je vezano uz proširenje *MIME* budući da opisuje način na koji se tekst u tijelu poruke interpretira. U ovom slučaju to je *TEXT/PLAIN* što označava običan tekst bez ikakvih dodataka, dok *charset=US-ASCII* ukazuje na kodnu shemu.

Tijelo poruke je običan tekst no putem proširenja *MIME* možemo koristiti npr. *HTML* kod koji ima prednosti ubacivanja poveznica i slika, formatiranja teksta. Nedostatak je u povećanoj veličini poruke, privatnosti i zloupotrebi. Primjer koji u poruci prikazuje html poveznicu i sliku kao dodatak prikazan je na slici 2.1.



Slika 2.1. Primjer kodiranja

U ispisu 2 nalazi se detaljan prikaz poruke sa slike 2.1.

Ispis 2. Primjer kodiranja poruke koja se sastoji od više tipova

```
01: Content-Type: multipart/mixed; boundary=00504502bf1c123f6a048e71a648
02:
03: --00504502bf1c123f6a048e71a648
04: Content-Type: multipart/alternative;
    boundary=00504502bf1c123f65048e71a646
05:
06: --00504502bf1c123f65048e71a646
07: Content-Type: text/plain; charset=ISO-8859-1
08:
09: Ovdje je poveznica FER <http://www.FER.hr>
10: Ispod je privitak.
11:
12: --00504502bf1c123f65048e71a646
13: Content-Type: text/html; charset=ISO-8859-1
14:
15: <div class=3D"gmail_quote"><div>Ovdje je poveznica=A0<a
    href=3D"http://www.=FER.hr"target=3D"_blank">FER</a></div></div>Ispo
    d je privitak.
17:
18: --00504502bf1c123f65048e71a646--
19: --00504502bf1c123f6a048e71a648
20: Content-Type: image/bmp; name="test.bmp"
21:
22:
23:
24:Qk12AQAAAAAADYAAAAoAAAACgAAAAoAAAABABgAAAAAAEABAAAAAAAAAAAAAAAAAAAAA
    AA////////////////////////////////AAD/////////////////////
    ///////////////8AAP///////////wAAAAAAAAAAP///////////////wAA///////
    /AAAAAAAA////AAAAAAAA///////////AAD///////8AAAD///////8AAAAAAAAAAA
25: --00504502bf1c123f6a048e71a648--
```

Dijelovi poruke elektroničke pošte koji se prikazuju na različit način naznačuju se upotrebom polja *Content-Type*, a nalaze se unutar granica koje se označava sa delimiterom *boundary*. U ispisu 2, retku 1 polje *Content-Type*: *multipart/mixed* označava poruku koja se sastoji od više dijelova s privitcima. U retku 3 nalazi se polje *Content-Type*: *multipart/alternative* koje označava da je svaki dio unutar granica delimitera alternativna verzija nekog sadržaja. Uglavnom se koristi kada se u tijelu želi prikazati *HTML* kod. Dio sa sadržajem označenim text/plain koristi se u slučaju da preglednik ne može prikazati taj *HTML* kod. Polje boundary=00504502bf1c123f6a048e71a648 u retku 1 koristi se za označavanje početka i kraja tipa sadržaja. Sadržaj s tipom iz retka 1 počinje u retku 2, a završava s retkom 25. U retku 3 nalazi se oznaka tipa *multipart/alternative* koja označuje da je dio koji se nalazi unutar granica 00504502bf1c123f65048e71a646 u poruci dio identičnog (ili sličnog) sadržaja. U retku 13 polje *Content-Type* iznosi *text/html*. To je instrukcija pregledniku da tekst ispod polja prikaže u html formatu. U retku 15 i 16 nalazi se kôd poveznice na www.fer.hr koji se u pregledniku prikaže samo sa FER. U retku 9 i 10 nalazi se alternativni prikaz sadržaja retka 15 i 16 koji se prikazuje ako preglednik ne može prikazati *HTML* kod.

U ispisu 2, retku 20 nalazi se polje polje *Content-Type* koje iznosi image/bmp. To je instrukcija pregledniku da je tekst ispod polja slika formata *BMP*. U *name* dijelu polja nalazi se ime privitka: test.bmp. Sami kod slike nalazi se u retku 24.

2.2. Protokol za razmjenu poruka elektroničke pošte

Simple Mail Transfer Protocol (SMTP) je Internet standard za prijenos poruka elektroničke pošte, prvi puta definiran u RFC 821, a ažuriran u RFC 5321. Taj protokol se koristi za prijenos poruka od klijenta do poslužitelja kao i između poslužitelja elektroničke pošte.

Protokol je baziran na tekstualnim naredbama, u kojima pošiljatelj poruke komunicira s poslužiteljem elektroničke pošte putem *TCP* spoja na pristupima 25 i 587. SMTP sjednica sastoji se od zahtjeva koje klijent šalje poslužitelju i odgovarajućih odgovora od strane poslužitelja elektroničke pošte. SMTP prijenos sastoji se od minimalno tri niza zahtjev/odgovor:

- *MAIL FROM* naredba, definira adresu pošiljatelja, odgovor na poruku će biti poslan na tu adresu.
- *RCPT TO* naredba, definira primatelja poruke, može se pozvati više puta, za svakog primatelja po jednom.
- *DATA* naredba obavještava poslužitelj da slijedi niz podataka, tj. tijelo poruke. Niz se prekida slanjem znaka "." u samostalnoj liniji.

Odgovori poslužitelja elektroničke pošte mogu biti pozitivni, kodovi oblika 2XX, ili negativni, kodovi oblika 5XX i 4XX. Dodatno se koristi i kod 354 koji označava početak slanja tijela poruke. Popis kodova nalazi se u tablici 2.1.

Primjer jednostavne *SMTP* transakcije dan je u ispisu 3. Nakon što se korisnik koji želi poslati poruku elektroničke pošte spoji na poslužitelj elektroničke pošte otvara se sjednica sa pozdravnom porukom od strane poslužitelja u kojoj se nalazi apsolutno ime domene. Korisnik pokreće dijalog odgovarajući sa *EHLO* naredbom koja uključuje njegovo apsolutno ime domene. U ispisu 3, retku 1 nalazi se pozdravna poruka poslužitelja na koji smo se spojili.Kod 220 označava da je usluga spremna, a tu se još nalazi i ime domene. U retku 2 korisnik obavlja *EHLO* naredbu s svojim apsolutnim imenom domene i na taj način pokreće dijalog s poslužiteljom koji u ovom slučaju odgovara kodom 250 naznačujući da je zahtjev prošao u redu.U retku 4 korisnik obavještava poslužitelj o pošiljatelju elektroničke pošte sa *MAIL FROM* naredbom u ovom slučaju *posiljatelj@primjer.org*, a poslužitelj odgovara potvrdnim kodom 250. Adrese na koje se želi poslati poruka predaju se poslužitelju putem *RCPT TO* naredbe u retku 6. U ovom primjeru poruka se šalje samo na adresu *primatelj@primjer.org*. U slučaju slanja poruke na više adresa, svaku adresu postavljamo zasebnom *RCPT* naredbom. Odgovor poslužitelja je 250 što označava da je odredišna adresa uspješno upisana.Prijenos tijela poruke obavlja se putem DATA naredbe. U retku 8 nakon poslanog zahtjeva poslužitelj nas obavještava da je spreman za unos tijela poruke kodom 354. Tijelo poruke se šalje liniju po liniju. Kraj poruke označava se tako da se upiše točka u novom redu nakon koje slijedi novi red. U retcima 10 do 18 nalazi se tijelo poruke. U ovom odjeljku definiraju polja *Subject*, *From* i *To*. Važno je napomenuti da protokol *SMTP* određuje samo omotnicu poruke, dok se u tijelo poruke ne dira, tako da *From* polje ne mora nužno odgovarati *MAIL FROM* stavci, kao ni *To* polje *MAIL TO* stavci. Nakon kraja poruke poslužitelj obavještava korisnika da je sve prošlo u redu kodom 250. Putem QUIT naredbe u retku 7 šalje se zahtjev za prekidom prijenosnog kanala sa poslužiteljem. Odgovorom koji sadrži kod 221 poslužitelj prekida prijenosni kanal. Poruka se ne šalje odmah već ovisi o tome kako je poslužitelj podešen.

Tablica 2.1. Popis povratnih kodova u SMTP dijalogu

Kod	Značenje
200	(nestandardni potvrdni odgovor, više u rfc876)
211	Sustavski status, ili sustavski pomoć odgovor
214	Poruka za pomoć
220	<domena> spremna usluga
221	<domena> usluga zatvara prijenosni kanal
250	Zahtjev prošao u redu
251	Korisnik nije lokalan; proslijediti će se na <forward-path>
354	Početak unosa poruke; završava sa <CRLF>.<CRLF>
421	<domena> Usluga nije dostupna, zatvara se prijenosni kanal
450	Zahtjev pošte nije proveden: sandučić nedostupan
451	Zahtjev prekinut: lokalna pogreška u obradi
452	Zahtjev nije proveden: nedovoljno mjesta za pohranu u sustavu
500	Sintaksna pogreška, neprepoznata naredba
501	Sintaksna pogreška u parametrima, ili argumentima
502	Naredba nije ugrađena
503	Krivi niz naredbi
504	Parametar naredbi nije ugrađen
521	<domena> ne prihvaća poruke (više u rfc1846)
530	Pritup odbijen
550	Zahtjev nije proveden: sandučić nedostupan
551	Korisnik nije lokalan; pokušati <forward-path>
552	Zahtjev pošte prekinut: prekoračen dodjela resursa
553	Zahtjev nije proveden: ime sandučića nije dozvoljeno
554	Neizvršen prijenos

Tijekom vremena, originalni *SMTP* protokol se nadograđivao, danas poznat pod *ESMTP* (extended SMTP). Glavna razlika je u korištenju *EHLO* naredbe umjesto *HELO* za identifikaciju na poslužitelju. Neke od poznatijih naredbi koje su dio proširenja su 8BITMIME – označava podršku za sadržaj poruke koji je kodiran sa 8 bita, *SMTP-AUTH* – označuje autentifikacijski mehanizam, *CHUNKING* – označuje podršku za *BDAT* naredbu koja je proširenje *DATA* naredbe, *DSN* – označuje podršku za obavijesti statusa isporuke dodavanjem opcionalnih parametara *MAIL* i *RCPT* naredbama, *ETRN* – označuje podršku za zahtjeve kojima lokalni *SMTP* poslužitelj pokreće isporuku pošte prema vanjskom *SMTP* poslužitelju putem zasebne veze, *HELP* – vraća poruku pomoći, *PIPELINING* – označuje podršku za zahtjev u kojem se šalje niz naredbi bez da se čeka na odgovor poslužitelja, *SIZE* – označuje maksimalnu veličinu poruke koja će se prihvatiti i označuje podršku za veličinu poruke koja se uključuje kao parametar u *MAIL* naredbi, *STARTTLS* – pokreće se sigurna *SMTP* veza preko zaštićenog sloja *TLS*, *UTF8SMTP* – dopušta korištenje kodiranja *UTF8* za imena sandučića i polja zaglavlja. *ENHANCEDCODES* –

povratni kodovi za *SMTP* proširenja. Podrška za *EHLO* naredbu postala je obavezna, no ukoliko poslužitelj na nju ne odgovori pokušava se sa *HELO*.

Ispis 3. Primjer SMTP dijaloga

```
01: 220 smtp.primjer.org SMTP service ready
02: EHLO klijent.primjer.org
03: 250 Hello klijent.primjer.org, dobrodosli
04: MAIL FROM:<posiljatelj@primjer.org>
05: 250 Ok
06: RCPT TO:<primatelj@primjer.org>
07: 250 Ok
08: DATA
09: 354 End data with <CR><LF>.<CR><LF>
10: From: " Posiljatelj Primjer" <posiljatelj@primjer.org>
11: To: "Primatelj Primjer" <primatelj@primjer.org>
12: Date: Tue, 15 Jan 2008 16:02:43 -0500
13: Subject: Testna poruka
14:
15: Pozdrav,
16: Ovo je testna poruka.
17: Tvoj prijatelj,
18: Posiljatelj
19: .
20: 250 Ok: queued as 12345
21: QUIT
22: 221 Bye
```

SMTP-AUTH je proširenje za *SMTP* putem kojeg se od korisnika traži prijava koristeći autentifikacijske mehanizme koji su podržani od strane poslužitelja elektroničke pošte. Nekorištenje tog proširenja pretvara poslužitelje u otvorene posredničke poslužitelje, olakšavajući rad pošiljateljima neželjene elektroničke pošte. Poslužitelji koji podržavaju *SMTP-AUTH* podeđeni su da odbijaju *RCPT TO* zahtjeve korisnika ukoliko oni nisu autentificirani. Korištenje autentifikacije obavezno je na pristupu 587, a može se koristiti i na pristupu 25. Kao i sva *SMTP* proširenja, *SMTP-AUTH* se objavljuje poslužitelj u EHLO odgovoru. Primjer autentifikacije dan je u ispisu 4.

Ispis 4. Primjer autentifikacije sa SMTP-AUTH

```
01: 220-smtp.example.com ESMTP Server
02: EHLO client.example.com
03: 250-smtp.example.com Hello client.example.com
04: 250-ENHANCEDSTATUSCODES
05: 250 STARTTLS
06: 250-AUTH GSSAPI DIGEST-MD5
07: STARTTLS
08: 220 Ready to start TLS
09:    ... TLS negotiation proceeds, further commands protected by TLS
    layer …
10: EHLO client.example.com
11: 250-smtp.example.com Hello client.example.com
12: 250 AUTH GSSAPI DIGEST-MD5 PLAIN
13: AUTH PLAIN dGVzdAB0ZXN0ADEyMzQ=
14: 235 2.7.0 Authentication successful
```

U ispisu 4 retku 1 imamo standardu poruku poslužitelja na kojeg smo spojeni. Slanjem *EHLO* zahtjeva u retku 2 dobijamo u retku 4 odgovore kojima nas poslužitelj obavještava o proširenjima koje podržava. U ovom primjeru to su *AUTH*, *STARTTLS* i

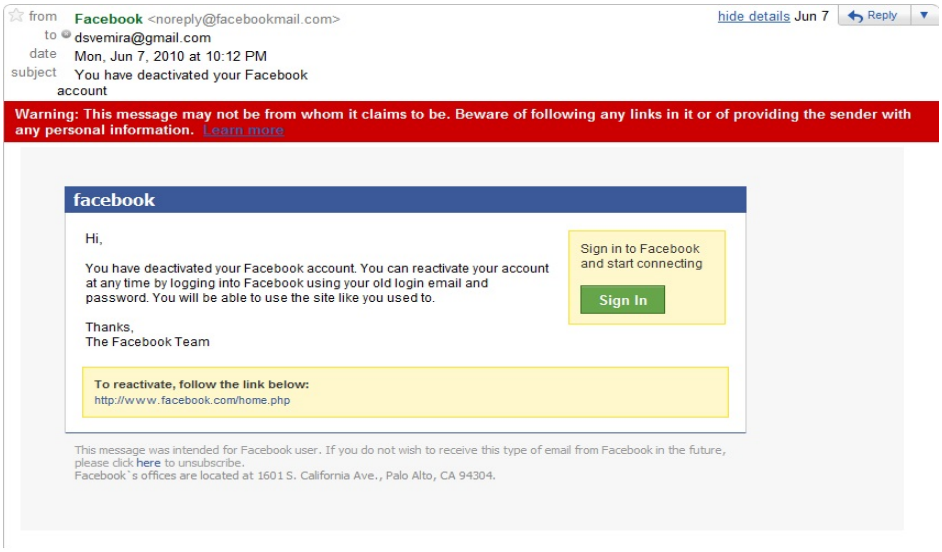
ENHANCEDSTATUSCODES proširenja koja omogućuju autentifikaciju, komunikaciju preko sigurnog sloja i dodatne statusne kodove. Korisnik u retku 7 zahtjevom *STARTLS* želi omogućiti sigurnu komunikaciju sa poslužiteljem. U retku 8 poslužitelj odgovara potvrdno kodom 200 i pokreće sigurnu komunikaciju. Nakon pokretanja uspostave sigurnog kanala nužno je ponovno slanje *EHLO* zahtjeva (redak 10). Poslužitelj u retku 12 ponovno obavještava korisnika o proširenjima koja se na sigurnom kanalu mogu koristiti. U retku 13 korisnik šalje zahtjev za autentifikacijom koja se sastoji od metode autentifikacije *PLAIN* koja označava da se prijava sastoji od jedne poruke. Poruka koja se šalje poslužitelju sastoji se korisničkog imena i zaporke kodiranih *BASE64* shemom. Korisničko ime i zaporka se kodiraju zajedno, u ovom slučaju testtest1234 daje *dGVzdAB0ZXN0ADEyMzQ=*. Znak "=" označava kraj niza koji se šalje.
SMTP-AUTH je samo mehanizam kojim se na poslužitelju zabranjuje slanje elektroničke pošte neautoriziranim korisnicima. Zlonamjerni korisnici, makar autentificirani, mogu lažirati polja zaglavlja. Dodatan je problem ako je korisnikovo računalo dio mreže kompromitiranih računala budući da su ta računala redovito autentificirana.

2.3. Lažiranje poruke elektroničke pošte

Lažiranje je postupak u kojem se u određena polja zaglavlja, npr. adresu pošiljatelja, adresu primatelja, namjerno upisuju lažni podaci. Taj postupak se koristi pri slanju neželjene elektroničke pošte u smislu da se sakrije porijeklo poruke, najčešće tako da izgleda kao da je poruka došla s nekog drugog izvorišta. Protokol *SMTP* propisuje samo razmjenu naredbi za poruke, ali ne i sadržaj, tj. definira se omotnica poruke i njeni parametri, dok se u polja zaglavlja i tijelo poruke ne dira. Poslužitelji elektroničke pošte ne provjeravaju identičnost adresa pošiljatelja u omotnici i poruci što pošiljatelji neželjene elektroničke pošte iskorištavaju da bi sakrili, ili lažirali svoj identitet. Odgovaranje na takve poruke nema efekta jer osobe čija je adresa lažirana nemaju veze s originalnom porukom. Polje *To* u zaglavlju ne odnosi se nužno na adresu na koju se šalje poruka. Također, polje *From* nužno ne mora biti adresa pošiljatelj poruke. Razlog tome je što je vrlo lako lažirati polje *From* tako da izgleda da je stiglo ne neke druge adrese.

Put svake poruke elektroničke pošte sastoji se od izvorišnog i odredišnog poslužitelja, no poruka može proći kroz nekoliko računala ovisno o topologiji lokalne mreže. Taj put se može detaljno pratiti u zaglavlju poruke budući da svako računalo zapiše svoju IP adresu u polje *Received* u zaglavlju. Zadnje polje *Received* sadrži IP adresu izvornog pošiljatelja. Primjer poruke elektroničke pošte koja ima lažirana zaglavlja prikazana je na slici 2.2, a poslužit će i kao primjer pokušaja krađe osobnih podataka s jedne popularne društvene mreže. Iako poruka izgleda legitimno što bi se na temelju *From* adrese moglo zaključiti, tek detaljnim pregledom zaglavlja možemo zapravo ustvrditi da se radi o lažnoj poruci.

U ispisu 5 nalazi se detaljan prikaz poruke sa slike 2.2 iz koje su izostavljeni dijelovi koji za ovaj primjer nisu važni.



Slika 2.2. Lažirana poruka s pokušajem krađe osobnih podataka

Ispis 5. Zaglavlja lažirane poruke

```
01 Delivered-To: tomislav@gmail.com
02 Received: by 10.229.81.5 with SMTP id v5cs48408qck;
     Mon, 7 Jun 2010 13:26:39 -0700 (PDT)
03 Received: by 10.140.180.6 with SMTP id
     c6mr12365341rvf.154.1275942397922;
     Mon, 07 Jun 2010 13:26:37 -0700 (PDT)
04 Return-Path: <claude11377@yahoo.com>
05 Received: from agl14.internetdsl.tpnet.pl (agl14.internetdsl.tpnet.pl
     83.16.167.14])
     by mx.google.com with SMTP id
     c16si7279389rvn.88.2010.06.07.13.26.34;
     Mon, 07 Jun 2010 13:26:37 -0700 (PDT)
06 X-Facebook: from zuckmail ([q8364Fa03CZ2]) by www.facebook.com with
     HTTP (ZuckMail);
07 Date: Mon, 7 Jun 2010 21:12:47 +0100
08 To: <tomislav@gmail.com>
09 From: Facebook <noreply@facebookmail.com>
10 Subject: You have deactivated your Facebook account
11 Message-ID: <fcee49b4012538c744c94c0dfafb21c3@www.facebook.com>
12 X-Priority: 3
13 X-Mailer: ZuckMail [version 1.00]
14 X-Facebook-Notify: deactivation_email; mailid=
15 X-FACEBOOK-PRIORITY: 0
16 MIME-Version: 1.0
17 Content-Type: text/html; charset = "UTF-8"
18 Content-Transfer-Encoding: 7bit
```

Prvo što možemo uočiti je nepodudaranje *Return-Path* polja u retku 4 i *From* polja u retku 9. Napadač je lažirao *From* polje zaglavlja tako da izgleda da je poruka u stvarnosti došla sa *noreply@facebookmail.com*, dok je u stvarnosti došla sa *claude11377@yahoo.com*. IP adresu računala s kojeg je poslana poruka možemo potražiti pregledom zadnjeg *Received* polja koje se nalazi u retku 5. Ona je 83.16.167.14. Provjerom IP adrese dolazimo do informacije da se radi o Poljskom telekomu, a ne *Facebook* poslužitelju. U zaglavlja poruke dodavana su i nova polja koja se nalaze u retcima 6, 12, 13, 14 i 15, sve s razlogom povećanja autentičnosti, tako da imamo polje *X-Mailer*: ZuckMail [version 1.00], ili *X-*

Facebook-Notify: deactivation_email; mailid kojima se aludiranjem na vlasnika servisa i postojeću metodu pokušava zavarati korisnika.

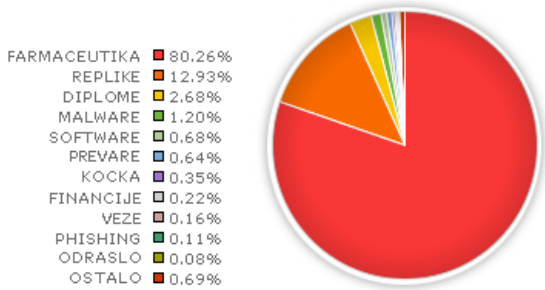
2.4. Neželjena elektronička pošta

Neželjena elektronička pošta je sinonim za *neželjenu masovnu elektroničku poštu* (engl. *Unsolicited Bulk E-mail, UBE*). To je pošta jednakog sadržaja koja se šalje velikom broju primatelja bez da su ju oni prethodno zatražili. Većina današnje neželjene elektroničke pošte je neželjena komercijalna elektronička pošta (engl. *Unsolicited Commercial E-mail, UCE*). To je pošta komercijalnog sadržaja koju primatelj nije zatražio, u kojoj nepoznati pošiljatelj nudi svoje usluge.

Pošiljatelji neželjene elektroničke pošte za rad trebaju ažuriranu bazu podataka s adresama. Kada se šalju poruke na Usenet, jednostavni, automatizirani programi pregledavaju zaglavlje poruke. Spremanjem pojedinih polja (*From, Return-Path*) može se izraditi lista potencijalnih primatelja. Postoje i loše podešene distribucijske liste (engl. *mailing list*) koje odaju listu pretplatnika. Jednostavni automatizirani programi mogu tražiti adrese i po Web stranicama. Za svaku pronađenu Web stranicu, program će tražiti *mailto:* poveznice.

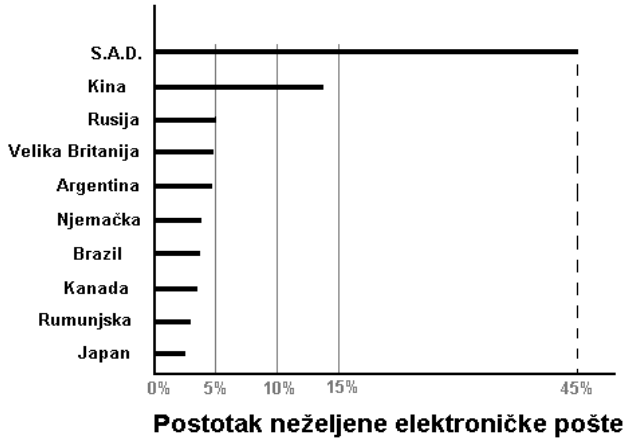
Pošiljatelji neželjene elektroničke pošte se za slanje neželjene elektroničke pošte raznim metodama od kojih se izdvajaju mreže kompromitiranih računala kao najveći izvor. Od ostalih tu su otvoreni posrednički poslužitelji (engl. *open proxy*) i otvoreni poslužitelj (engl. *open relay*). Otvoreni posrednički poslužitelj usluga koja je otvorena za bilo kakve zahtjeve i koja omogućuje pošiljateljima neželjene elektroničke pošte anonimnost. Pošiljatelji neželjene elektroničke pošte koriste više otvorenih posredničkih poslužitelja jer tako povećavaju šansu da je jedan od njih loše podešen i da neće zapisati njegovu IP adresu. Otvoreni poslužitelj je poslužitelj koji dopušta prijenos poruka elektroničke pošte s treće strane, makar nisu namijenjene za njegovu domenu. Te poslužitelje često koriste pošiljatelji neželjene elektroničke pošte za slanje velikog broja neželjene elektroničke pošte, ali se često i nalaze na crnim listama.

Većina današnje neželjene elektroničke pošte svodi se na farmaceutske proizvode, i skupa s reklamama za replike čine preko 90% sveukupne neželjene elektroničke pošte [3]. Na slici 2.3 prikazana je raspodjela svjetske neželjene pošte po tipovima, a osim farmaceutskih proizvoda i replika oglašavaju se diplome, razni sadržaji za odrasle, financijske prijevare i poslovi vezani uz kocku. Jedan dio neželjene pošte otpada i na maliciozne programe kojima se pokušava kompromitirati računala.



Slika 2.3. Postotak neželjene elektroničke pošte po tipovima

Većina ukupne svjetske neželjene elektroničke pošte konstantno dolazi iz istih država [3]. Deset država iz kojih dolazi najviše neželjene elektroničke pošte prikazano je na slici 2.4.



Slika 2.4. Obujam neželjene elektroničke pošte po državama

Ova lista u većini slučajeva kroz vrijeme ostaje ista, Sjedinjene Američke Države uvjerljivo vode sa skoro 45 posto ukupne svjetske neželjene elektroničke pošte, a Kina prati sa 13 posto. Osim njih dvije, u svjetskom slanju neželjene elektroničke pošte nalaze se Rusija, Velika Britanija, Argentina, Njemačka, Brazil, Kanada, Rumunjska i Japan, koje se postotkom malo razlikuju (3 – 5 posto). Te države većinom izmjenjuju mjesta na ljestvici ovisno o mjesecu praćenja, a osim njih se na listi znaju naći i države poput Indije, Sjeverne Koreje, Francuske, Vijetnama.[1, 4]

2.5. Mreže kompromitiranih računala

Najveći izvor neželjenih elektroničkih poruka danas su mreže kompromitiranih računala. To je skup međusobno povezanih računala koja su zaražena malicioznim programima. Vlasnik mreže kompromitiranih računala kontrolira mrežu s udaljene lokacije, npr. putem IRC-a, za ilegalne radnje. Shema mreže kompromitiranih računala dana je na slici 2.5. Mreže kompromitiranih računala sačinjavaju velik dio ukupnih računala na Internetu, tj. smatra se da je danas jedna četvrtina svih osobnih računala na Internetu dio neke mreže kompromitiranih računala [16]. U današnje vrijeme većim i dugotrajnijim mrežama kompromitiranih računala dodjeljena su imena, od kojih je napoznatiji Rustok koji je odvoran za 50% neželjene elektroničke pošte [3].

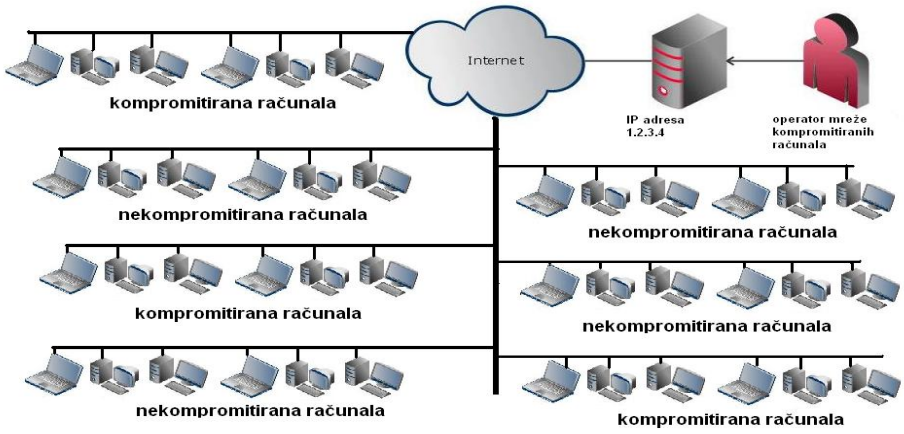
Mreže kompromitiranih računala izgrađuju se upotrebom rootkit-ova. *Rootkit* je zlonamjerni program koji je napravljen s ciljem preuzimanja kontrole nad operacijskim sustavom tako da nadomjesti sustavske procese i podatke bez dopuštenja korisnika. Tipično, napadač ugrađuje rootkit na udaljeno računalo iskorištavanjem neke slabosti u operacijskog sustava. Naziv rootkit dolazi od riječi *root* koji označava najveću razinu kontrole nad operacijskim sustavom i *kit* koji se odnosi na programsku komponentu.

Zombie računalo je računalo spojeno na Internet, a kompromitirano je od strane napadača, računalnog virusa, ili trojanskog konja te se s njime može upravljati s udaljene lokacije. Općenito gledajući, ta računala su dio mreže kompromitiranih računala i koriste se za

izvršavanje malicioznih zadataka. Većina vlasnika zombi računala nije svjesna da se njihovi sistemi koriste na taj način, odakle i dolazi ime.

Mreže kompromitiranih računala mogu se koristiti u razne svrhe:

- Raspodjeljeni napadi uskraćivanja resursa (engl. *distibuted denial of service*) – višestruki sustavi pristupaju nekoj Internet usluzi, ali u većem broju nego je to uobičajeno, što dovodi do zagušenja tog sustava.
- Oglašivački programi (engl. *adware*) – posebni programi koji oglašavaju neke komercijalne stavke na korisnikovom računalu bez prethodnog korisnikovog dopuštenja.
- Špijunski programi (engl. *spyware*) – programi koji šalju informacije napadačima o korisnikovom djelovanju
- Neželjena elektronička pošta – poruke elektroničke pošte kojima se maskira pošiljatelj u svrhu oglašavanja, smetanja ili zlih namjera.
- Prijevara klikanjem (engl. *Click fraud*) – računala posjećuju razne Web stranice u svrhu komercijalne i osobne koristi.



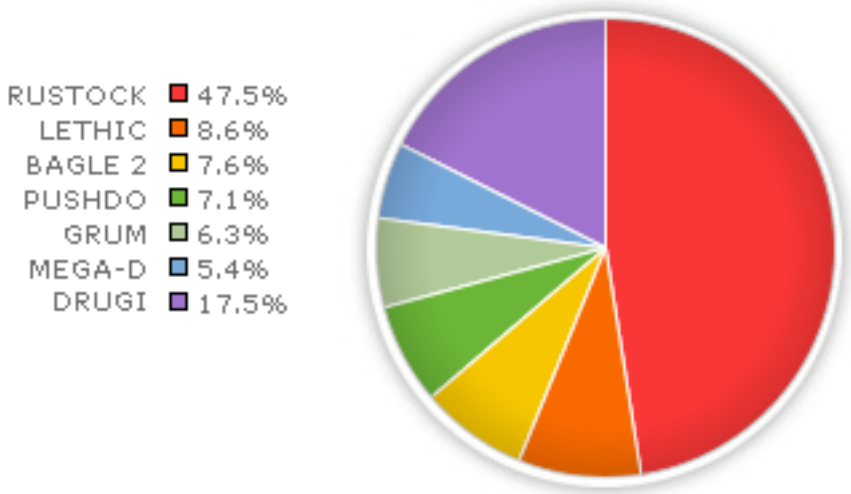
Slika 2.5. Shema mreže kompromitiranih računala na Internetu

U novije vrijeme mreže kompromitiranih računala upravljaju se putem partnerskih (engl. *p2p*) mreža, a upravljački mehanizmi za kontrolu mreže su ugrađeni u svakom kompromitiranom računalu. Takve mreže su dinamički ažurirane i varijabilne pa mogu izbjeći razne kvarove. Operatori najnovijih mreža kompromitiranih računala imaju mogućnost detektiranja i reagiranja na pokušaje otkrivanja njihovog načina rada, a mreže kompromitiranih računala imaju i mogućnost raspodjeljenog napada uskraćivanjem resursa prema korisniku koji ga proučava [17].

Pošiljatelji neželjene elektroničke pošte kupuju pristup mreži kompromitiranih računala od operatora, uglavnom na određeno vrijeme te zatim šalju naredbe zaraženim računalima za slanje neželjene elektroničke pošte.

Većina današnje neželjene elektroničke pošte dolazi s nekolicine mreža kompromitiranih računala [3, 6]. Tipično, mali broj mreža kompromitiranih računala zaslužno je za većinu neželjene elektroničke pošte. Ukupni obujam poslane neželjene elektroničke pošte putem

mreža kompromitiranih računala prikazan je na slici 2.6. Rustock mreža kompromitiranih računala zaslužna je za polovinu sveukupne neželjene elektroničke pošte. Ostale mreže poput Lethica, Bagle2, Pushdo, Grum i Mega-D drže isti postotak koji iznosi od 5 do 9 posto.[5]



Slika 2.6. Neželjena elektronička pošta po mrežama kompromitiranih računala

Osnovne informacije o vodećim mrežama kompromitiranih računala poput veličine, mogućnostima slanja neželjene elektroničke pošte i tipu oglašavanja kojim se bave dane su u nastavku:

- *Rustock* (alias: Costrat) – Sveprisutan u raznim oblicima već oko dvije godine, vrlo vjerojatno i duže. Sofisticiran i profiliran stroj za slanje neželjene elektroničke pošte. Vodeći u slanju neželjene elektroničke pošte. Koristi *rootkit* da se sakrije na domaćinu. Pri oglašavanju se često mijenjaju predlošci oglašavanih proizvoda, a fokus je većinom na farmaceutskim lijekovima. Većina Rustockovih varijanti se ne mogu identificirati putem antivirusnih programa kao Rustock, već putem generičkih imena. Ima sposobnost slanja 25.000 poruka po satu po svakom kompromitiranom računalu. Procjenjuje se da se sastoji od 1.3 milijuna do 2 milijuna kompromitiranih računala [6, 7].
- *Lethic* – Iako tek nedavno otkriven, smatra se da je postoji već duže vrijeme. To je mreža kompromitiranih računala koja koristi zombije kao posredničke poslužitelje, koji prenose neželjenu elektroničku poštu sa centralnog kontrolnog poslužitelja prema odredištu. Fokusiran je na slanje elektroničkih poruka u kojima se reklamiraju farmaceutske kompanije i replike satova. Ima sposobnost slanja od 12.000 do 60.000 poruka po satu po svakom kompromitiranom računalu, dok mu se veličina procjenjuje na 1 milijun kompromitiranih računala [6, 7].
- *Bagle 2* (alias: Beagle, Mitglieder, Lodeight) – Prvi put se pojavio u 2004. godini kao masovni crv za slanje poruka. Od onda, skupio je stotinjak varijanti i njegovo ponašanje evoluira. Danas služi kao posrednički poslužitelj te prenosi neželjenu

elektroničku poštu ka krajnjim odredištima. Neželjena elektronička pošta razlikuje se ovisno o kontrolnom poslužitelju koji ju prenosi. Veličina mu se procjenjuje na 600.000 do 800.000 kompromitiranih računala [6, 7].

- *Pushdo* (alias: Cutwail, Pushu, Pandex) – Počeo sa djelovanjem sredinom 2007.g. Zaslužan je za slanje širokog spektra komercijalne elektroničke pošte promovirajući primjerice farmaceutske tvrtke, lažnu dizajnersku odjeću ili programsku podršku. Vrlo je aktivan u slanju malicioznih programa i u distribuciji *phishing* elektroničke pošte u kojima cilja na širok spektar financijskih institucija. Brzina slanja neželjene elektroničke pošte mu je nešto niža od novijih mreža kompromitiranih računala i ona iznosi 4500 poruka na sat po kompromitiranom računalu. Sastoji se od 1 milijun do 1.5 milijuna kompromitiranih računala [6, 7].
- *Grum* (alias: Tedroo) – Ima tendenciju inficirati datoteke vezane za pokretanje računala. Budući da koristi rootkit njegovo otkrivanje i uklanjanje je teško. Uglavnom je koncentriran na promoviranje farmaceutskih tvrtki. Širok spektar predložaka za slanje neželjene elektroničke pošte mijenja se često, pod nadzorom više poslužitelja. Ima sposobnost slanja neželjene elektroničke pošte od 4000 poruka po satu po kompromitiranom računalu, a procjenjuje se da se sastoji od 600.000 do 800.000 kompromitiranih računala [6, 7].
- *Mega-D* (alias: Ozdok) – Postoji od 2007. godine, i u jednom trenutku je bio odgovoran za trećinu sveukupne svjetske neželjene pošte. Većinom je vezan za farmaceutsku industriju, ponajviše za Canadian Pharmacy. Učinak mu je bio kratko poremećen uklanjanjem McColo mreže u studenom 2008. Ima mogućnost slanja 15.000 poruka na sat po kompromitiranom računalu. Veličina mu se procjenjuje na 300.000 do 500.000 kompromitiranih računala [6, 7].
- *Bobax* (alias: Kraken, Oderoor, Hacktool.spammer) – Privukao je veliku medijsku pažnju u 2008. godini unatoč činjenici da se za njegovo postojanje zna od 2006. godine, a postoji i od prije. Bio je zaslužan za 5-10% ukupne svjetske neželjene elektroničke pošte pred kraj 2008. godine. Ima sposobnost slanja 7200 poruka na sat po kompromitiranom računalu. Procjenjuje se da se sastoji od 185.000 kompromitiranih računala [6, 7].
- *Xarvester* (alias: Risloup, Pixoliz) – Počeo je masovno slanje neželjene elektroničke pošte ubrzo nakon ukidanja McColo mreže u studenom 2008. Koncentrira se na oglašavanje replika satova i farmaceutskih proizvoda. Može slati 25,000 poruka na sat po kompromitiranom računalu. Procjenjuje se da se sastoji od 500.000 do 800.000 kompromitiranih računala [6, 7].
- *Srizbi* (alias: CbePlay, Exchanger) – Tijekom cijele 2008. godine vodeći u slanju neželjene elektroničke pošte, zaslužan za 50% sveukupne neželjene elektroničke pošte. Bio je sastavljen od oko 450.000 kompromitiranih računala i bio u stanju slati 60-80 milijardi poruka na dan. Ukidanjem McColo mreže poremećen je rad kontrolnih servera od kojih se Srizbi nije nikad oporavio. Sam automatizirani program je ekstremno skriven jer koristi napredni *rootkit* što čini teškim njegovo detektiranje i uklanjanje. Danas ima mogućnost slanja 8000 poruka na sat po kompromitiranom računalu [6, 7].

- *Waledac* (alias: Waled, Waledpak) – Pojavio se pred kraj 2008. godine i smatra se nasljednikom Storm mreže kompromitiranih računala budući da ima dosta sličnosti u ponašanju. Predlošci neželjene elektroničke pošte su identični onima koje je koristila Storm mreža. U odnosu na vodeće spam botnete, broj Waledacovih poruka ostaje mali. Unatoč tome, Waledac je visoko profilna mreža kompromitiranih računala koji vodi kampanje točno određenog karaktera vezanih uz maliciozni softver i socijalne mreže. Tipične teme vezane su uz elektroničke razglednice, lažne kupone i trenutne događaje. Koristi se i za slanje poruka vezanih uz Canadian Pharmacy i druge proizvode. Ima mogućnost slanja 7000 poruka na sat po kompromitiranom računalu. Procjenjuje se da se sastoji od oko 400.000 kompromitiranih računala [6, 7].

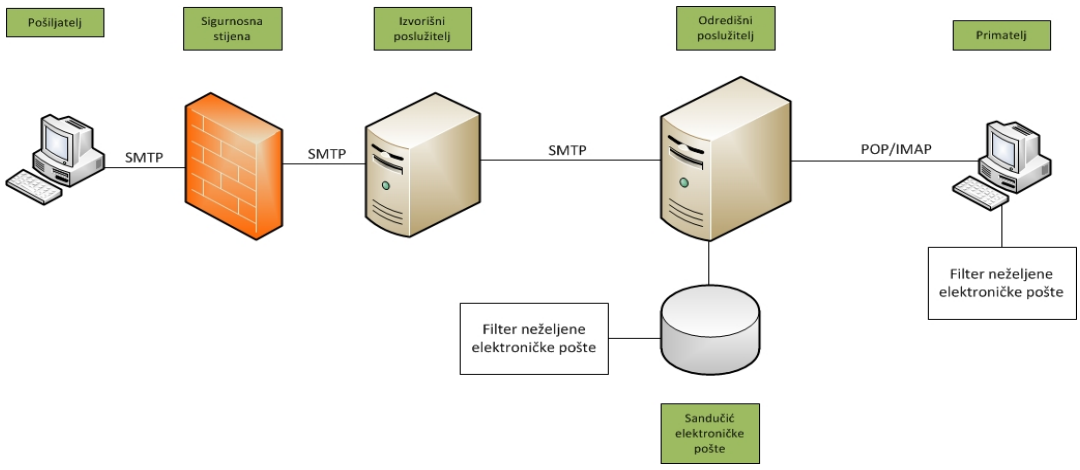
2.6. Tehnike zaustavljanja neželjene elektroničke pošte

Da bi spriječili neželjenu elektroničku poštu, korisnici i administratori sustava elektroničke pošte koriste razne tehnike koje su ugrađene u proizvode, usluge i programe no nijedna ne pruža kompletno rješenje, svaka ima svojih prednosti i mana i koriste se zajedno radi povećanja efikasnosti. Veliki problem tehnika je razina agresivnosti prema elektroničkoj pošti. Ako su tehnike postavljene agresivno postoji mogućnost odbijanja jednog dijela legitimne elektroničke pošte, a ako se razina agresivnosti smanji moguća je situacija da se neće blokirati sva neželjena elektronička pošta.

Lažni pozitiv (engl. *false positive*) je naziv za valjanu elektroničku poštu koja je na neki način označena kao neželjena elektronička pošta. Cilj je svakog sustava svesti broj lažnih pozitiva na minimum budući da se takve poruke nepotrebno odbacuju.

Tehnike zaustavljanja neželjene elektroničke pošte mogu se podijeliti na četiri grupe: (I) tehnike koje se koriste na izvorišnom poslužitelju, (II) tehnike koje se koriste na odredišnom poslužitelju, (III) tehnike koje se koriste na računalu klijenta odredišta, (IV) mjere koje mogu primijeniti istraživači i zakonske udruge.

Shema mreže na kojoj se odvija slanje elektroničke pošte prikazana je na slici 2.7.



Slika 2.7. Shema slanja poruke elektroničke pošte

Tehnike koje se koriste na izvorišnom poslužitelju:

- Informiranje korisnika o ilegalnim radnjama – Svaki pružatelj Internetskih usluga ima uvjete korištenja i slanjem upozorenja može korisnika upozoriti na ilegalne radnje. Nastavkom ponašanja korisniku se može ukinuti usluga.
- Provjera izlazne pošte – Specijalizirani programi na poslužiteljima provjeravaju izlaznu poštu u potrazi za virusima i ostalim malicioznim programima. Na taj način štite i sebe od zapisa u crnim listama.
- Provjera *HELO*/*EHLO* naredbe - *SMTP* poslužitelj može provjeriti da li korisnik daje pravilni odgovor *HELO*/*EHLO* pri spajanju na poslužitelj, ali samo temeljem te činjenice ne može mu odbiti poruku. Poslužitelji imaju mogućnost odbijanja spoja u slučaju da korisnik preda nevaljanu *HELO* naredbu, npr. da je ime domene krivo napisana, u slučaju da se preda lažna naredba, u slučaju da se korisnik spaja sa domene koja nije autentificirana i za domene koje ne nalaze u *DNS* zapisima.
- Blokiranje i presretanje pristupa 25 – Sigurnosne stijene i usmjerivač se mogu podesiti da blokiraju promet na pristupu 25 za računala na mreži koja nemaju dozvolu rada kao poslužitelji elektroničke pošte. Promet sa pristupa 25 može se i proslijediti prema poslužiteljima koji ima postavljene izlazne filtere.
- Autentifikacija pošiljatelja – Prije slanja elektroničke pošte korisnik se mora identificirati na poslužitelju. Mehanizmi kojima se identifikacija omogućuje su *SMTP AUTH* proširenje za protokol *SMTP* kojim se omogućuje prijava korisnika na poslužitelj, *SMTP TLS* kojim se korisnik autentificira certifikatima i pruža sigurni protok podataka, *POP before SMTP* kojim se korisniku dopušta *SMTP* promet ukoliko se uspješno prijavio na poslužitelj putem *POP* usluge.

Tehnike koje se koriste na odredišnom poslužitelju:

- Baza poruka neželjene elektroničke pošte – Ova tehnika se oslanja na povratne informacije koje pružaju korisnici kada prime neželjenu elektroničku poštu. Ukoliko dovoljno velik broj korisnika označi neku poruku kao neželjenu, u bazu se zapisuju podaci o poruci i tako sprečava njeno daljnje širenje.
- Korištenje crnih lista – Crne liste još su poznate i kao blokirajuće liste budući da im je namjena blokiranje korisnika koji žele slati poruke elektroničke pošte. Te liste se sastoje od IP adresa, imena ljudi, domena, ili tvrtki kojima se zabranjuje komunikacija prema legitimnim korisnicima.
- Korištenje bijelih lista – Bijele liste su suprotnost crnim listama u kojima se korisnici odobre za slanje i primanje elektroničke pošte. Ukoliko npr. dvije tvrtke žele međusobno razmjenjivati elektroničku poštu bez smetnji drugih korisnika mogu koristiti bijele liste. Na taj način štedi se na resursima i osigurava od napada izvana.
- Sive liste – Metoda kojom se privremeno odbija poruka, no u listu se npr. zapisuje IP adresa i adresa pošiljatelja i adresa primatelja. Izvorišnom poslužitelju se pošalje odgovor da je poruka odbijena, a ako se poruka pošalje ponovno s istim podacima prihvatit će se. Razlog tomu je što pošiljatelji neželjenih elektroničkih poruka ne

pokušavaju ponovno poslati poruke s istim podacima već kreću na nove koje polaze istu proceduru.

- Detekcija vršnog prometa – Metoda kojom se promet nadgleda u realnom vremenu i pruža administratorima mogućnost brze reakcije u slučaju povećanog prometa i blokiranja pošiljatelja neželjene elektroničke pošte .
- Detekcija anomalija u prometu – Kao i u slučaju detekcije vršnog prometa, promet nad mrežom se nadgleda, samo što se u ovom slučaju administratori traže anomalije koje bi ukazale na slanje neželjene elektroničke pošte.
- Zamke – Skup lažnih adresa i poslužitelja kroz koje se može uloviti pošiljatelje neželjene elektroničke pošte. Adrese koje se koriste za zamke ne koriste normalni korisnici tako da se sva pošta koja stigne na njih može smatrati neželjenom elektroničkom poštom.
- sigurnosne stijene – Koriste se u tvrtkama, a svrha im je identifikacija neželjene elektroničke pošte i njeno nedopuštanje ulaska u lokalnu mrežu.
- Tehnika upit/odgovor (engl. challenge/response) – Kada se koristi ova tehnika svaka adresa elektroničke pošta mora imati dopuštenje dostave poruke. Dopuštenje izdaje primatelj, a ako nam netko želi poslati poruku sa nepoznate adrese dobije natrag upit formuliran na način da ga samo osoba može odgovoriti. Ako je odgovor potvrdan poruka se propušta, inače se adresa stavlja u crnu listu. Primjer takve tehnike je *CAPTCHA*.
- Reputacijski sustavi – Sustavi koji se se bave ocjenjivanjem pouzdanosti nekog sustava na temelju skupa činjenica. Ocjena služi korisnicima za procjenu vjerovanja određenom sustavu.
- Autentifikacija pošiljatelja – Poslužitelj koji je primio poruku ima mogućnost provjere identiteta pošiljatelja poruke, a na raspolaganju mu je nekoliko metoda: *Reverse-MX* metoda kojom se provjerava da li je poruka stigla s poslužitelja s poznatom IP adresom, *DKIM* metoda kojom se poruka veže uz domenu i kriptira radi očuvanja integriteta, *SPF* metoda kojom se provjerava da li je poruka stigla sa poslužitelja koji ima dopuštenje slanja elektroničke pošte i da li je stigla od korisnika koji se nalazi na istoj domeni kao i poslužitelj.
- Filtriranje poruka – Filtriranje se obavlja putem specijaliziranih programa, npr. SpammAassassin, Mailwasher, koji koriste heurističke algoritme, ili Bayesian filtriranje. Heurističko filtriranje radi na principu usporedbe zaglavlja, tijela i omotnice poruke sa tisućama predefiniranih pravila. Svakom pravilu dodjeljen je numerički ekvivalent vjerojatnosti da je poruka neželjena. Krajnji rezultat je broj koji ovisi o predefiniranom broju kojeg odredi administrator poslužitelja. Ako se prag postavi visoko može se desiti situacija propuštanja velike količine neželjene elektroničke pošte, a ako se prag postavi nisko može se desiti odbijanje određenog broja legitimnih poruka. Nedostatak filtera je što se pošiljatelji neželjenih elektroničkih poruka prilagođavaju pravilima tako da se ona stalno moraju ažurirati. Za razliku od heurističkih pravila koja su statička bayesian filter radi na principu usporedbe dva seta informacija. U jednom setu imamo valjane poruke pomoću

kojih se izračunava vrijednost koja se koristi za filter. Vrijednost koju izračuna filter putem legitimnih poruka koristi se pri usporedbi dolaznih poruka.

Tehnike koje se koriste na odredišnom računalu:

- Filtriranje poruka – Kao i slučaju kod poslužitelja, na lokalnom računalo možemo imati specijalizirani program za filtriranje. Koristi se ako želimo dodatnu sigurnost, ili nam jednostavno filter na poslužitelju ne odgovara.
- Ne odgovaranje na poruke neželjene elektroničke pošte – Ukoliko odgovorimo na poruku neželjene elektroničke pošte jasno dajemo njenom pošiljatelju do znanja da se adresa koristi.
- Maskiranje adrese elektroničke pošte – Ako smo primorani ostaviti adresu elektroničke pošte na nekom vidljivom mjestu na Internetu, preporuča se adresu zamaskirati na način da automatizirani sakupljači adresa nemaju od nje koristi, dok je lako čitljiva normalnim korisnicima, npr. korisnikANTI@SPAM.example.com

Tehnike koje koriste istraživači i organi zakona:

- Zakonodavstvo i provedba: Velik utjecaj na smanjenje neželjene elektroničke pošte kaznama i gašenjima sustava koji se bave slanjem neželjene elektroničke pošte. Važno je spomenuti američki CAN-SPAM zakon iz 2003. [22] koji određuje pravila slanja komercijalne pošte: zabranjeno je korištenje lažnih informacija u zaglavlju poruke, zabranjeno je korištenje naslova poruke koji može zavarati primatelja, poruka se mora identificirati kao oglas, poruka mora sadržavati legitimnu adresu tvrtke, pružiti mogućnost brisanja iz distribucijske liste.
- Analiza oglašavanih Internet stranica: Uglavnom vodi do sumnjivih registracija domena koje se pravilnim prijavama mogu ugasiti.

2.6.1. DKIM

Budući da većina neželjene elektroničke pošte ima lažirane dijelove u zaglavlju poruke javila se potreba za načinom autentifikacije poruka elektroničke pošte. *DomainKeys Identified Mail* je metoda za autentifikaciju poruka elektroničke pošte koja omogućuje primatelju poruke provjeru da li je poruka mijenjana na njenom putu od izvorišta do odredišta. Metoda veže ime domene s porukom tako da primatelj može provjeriti ispravnost. Način validacije temelji se na kriptografskim metodama javnog ključa. Potpisnik poruke dodaje digitalni potpis u zaglavlje poruke, polje *DKIM-Signature*. Korisnik koji provjerava poruku preuzima javni ključ potpisnika putem *DNS* upita i zatim provjerava poruku tražeći da li su potpisani dijelovi možda mijenjani.

Metoda osigurava potpisivanje odabranih polja u zaglavlju, npr. polja *From, Subject*, kao i cjelokupnog tijela poruke. Na taj način metoda osigurava poruke elektroničke pošte od neovlaštenog mijenjanja i nudi integritet poruke s potpisnikove strane.

Vodeći pružatelji usluga elektroničke pošte, *Yahoo*, *Gmail* i *FastMail,* imaju *DKIM* implementiran i sve poruke elektroničke pošte koje dolaze s njihovih poslužitelja sadrže *DKIM* potpis.

Poslužitelji elektroničke pošte obavljaju potpisivanje i provjeru poruke elektroničke pošte. Organizacija koja potpisuje poruku može biti izvorni poslužitelj, ili specijalizirani poslužitelj kojem se šalje poruka samo za *DKIM* potpisivanje. Specijalizirani poslužitelj zatim šalje potpisanu poruku dalje prema odredištu. Njegova reputacija važan je faktor i temelj procjene vjerovanja valjanosti poruke. Odgovorna organizacija dodaje digitalni potpis poruci i na taj način veže ime domene s organizacijom. Provjera ispravnosti potpisa vrši se na odredišnom poslužitelju.

DKIM potpis se sastoji od nekoliko polja *oznaka=vrijednost*. Oznake se uobičajeno sastoje od jednog do dva slova. Najvažnije oznake su *b* za digitalni potpis zaglavlja i tijela poruke, *bh* za sažetak tijela poruke, *d* za domenu koja potpisuje poruku, *s* za odabir potpisnika (svaka domena može imati više potpisnika). Pretpostavljeni algoritmi autentifikacijskog mehanizma su *SHA-256* za kriptografski sažetak poruke, *RSA* kao metoda kriptiranja javnim ključem dok se za kodiranje sažetka koristi *Base64*. Primjer konkretnog *DKIM* potpisa dan je u ispisu 6.

Ispis 6. Primjer DKIM potpisa u zaglavlju poruke

```
01: DKIM-Signature: v=1; a=rsa-sha256; d=example.net; s=brisbane;
02: c=relaxed/simple; q=dns/txt; l=1234; t=1117574938; x=1118006938;
03: h=from:to:subject:date;
04: bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
05: b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZVoG4ZHRNiYzR
```

SMTP poslužitelj koji prima poruku elektroničke pošte koristi ime domene i ime potpisnika za dohvat ključa u *DNS* zapisu. U ispisu 6, retku 1 nalazi se polje u zaglavlju kojim počinje *DKIM* potpis. Oznaka *v* predstavlja verziju potpisa koja iznosi 1, *a* su algoritmi koji se koriste za kriptiranje (*RSA*) i izračun sažetka poruke potpisa (*SHA-256*) u našem slučaju. Svi se *DKIM* ključevi spremaju u *_domainkey* poddomenu. Spajanjem oznake *d* i *s* dolazi se do informacije da će *DNS* upit ići na *brisbaine._domainkey.example.net*. U retku 2 nalazi se oznaka *c* koja ukazuje na tip kanonizacije zaglavlja i tijela poruke, u ovom primjeru *relaxed* označuje da se razmaci u poljima zaglavlja brišu, a sva slova u imenima polja zaglavlja se pretvaraju u mala slova, dok se za tijelo poruke koristi *simple* jednostavni, podrazumjevani tip koji ne dopušta nikakvu modifikaciju tijela poruke, *q* je metoda upita, *dns/txt* označuje metodu za dohvat javnog ključa, putem *DNS*-a, *l* je duljina kanoniziranog dijela tijela u bajtovima potpisane poruke koji je u primjeru 1234, *t* je vremenska oznaka kad je poruka potpisana, a *x* je vrijeme isteka potpisa. U našem slučaju poruka je potpisana u utorak, 31. 5. 2005. godine u 21:28:58, dok potpis ističe nedjelju, 5. 6. 2005. godine u 21:28:58. U retku 3 nalazi se oznaka *h* koja je u biti lista polja zaglavlja koja se potpisuju. U ovom primjeru potpisuju se *From*, *To*, *Subject* i *Date*. U retku 4 nalazi se sažetak tijela poruke, a u retku 5 digitalni potpis zaglavlja i tijela poruke.

Kada se na odredištu želi provjeriti potpis šalje se *DNS* upit temeljen na oznakama *d* i *s* u *DKIM* potpisu. Podaci koji se dobiju upitom uključuju javni ključ domene, i oznake i zastavice vezane uz korištenje ključa. Primatelj poruke elektroničke pošte može na taj način izračunom sažetka potvrditi da li je poruka valjano potpisana od strane neke organizacije i da li je možda mijenjana po putu.

Primarna prednost korištenja *DKIM*-a je ta što dopušta korisnicima da sa sigurnošću identificiraju putove na kojima poruka elektroničke pošte nije mijenjana. Te informacije mogu se koristiti kao jedna od stavki pri evaluaciji reputacije nekog sustava.

Najveći nedostatak metode je što ne sprečava pošiljatelja neželjene elektroničke pošte da sastavi poruku na nekoj domeni kojoj se vjeruje i na taj način ju digitalno potpiše. Na taj način, npr. putem mreže kompromitiranih računala, može se slati neželjena elektronička pošta koju primatelj smatra vjerodostojnom budući da je digitalno potpisana od strane organizacije kojoj se vjeruje. Poslužitelji elektroničke pošte imaju mogućnost prihvaćanja potpisanih poruka bez daljnjih filtriranja, što u slučaju kompromitiranog korisnika, ili domene, pomaže pošiljateljima neželjene elektroničke pošte.

2.6.2. SPF

Sender Policy Framework (SPF) je proširenje protokola *SMTP* koje dopušta programima identifikaciju i odbijanje poruka elektroničke pošte kojima su lažirane adrese u *Return-Path* polju zaglavlja poruke elektroničke pošte, tipičnom za neželjenu elektroničku poštu.

SPF dopušta vlasniku Internet domene specificiranje računala unutar domene koja autorizirana za slanje poruka elektroničke pošte. To specificiranje obavlja se upotrebom *DNS* zapisa.

Glavna prednost *SPF*-a je za korisnike čije se adrese elektroničke pošte lažiraju u povratnoj adresi. Takvi korisnici primaju velike količine poruka o grešci i automatiziranih odgovora, otežavajući korištenje elektroničke pošte. Ukoliko se koristi *SPF*, primatelji poruka elektroničke pošte mogu jendnostavno provjeriti i odbiti one lažirane.

Mnogi poslužiteljski programi podržavaju SPF dok je ostalima to dostupno kroz dodatke. Poslužitelji koji podržavaju *SPF* su Courier, CommuniGate Pro, Wildcat i Microsoft Exchange, dok ga putem dodataka podržavaju Exim, Postfix, Qmail, Sendmail, . U anketi provedenoj 2007. godine, 5% .com i .net domena sadržavalo je nekakav *SPF* zapis, dok ga veće domene koriste već od 2004 godine [7]. Domene koje su objavile *SPF* zapise već na kraju 2004. godine su Amazon.com, AOL.com, Ebay.com, Google.com, Hotmail.com, Microsoft.com, W3C.org, AltaVista.com, Perl.org, DynDNS.org.

Implementacija *SPF*-a sastoji se od mehanizama, kvantifikatora i modifikatora. Definirano je osam mehanizama: *ALL* – mehanizam se uvijek prihvaća, koristi za predefiniranu akciju nad za sve IP adrese koje se nisu prihvatile tijekom prijašnjih provjera, *A* - ako ime domene ima *A* zapis koji odgovara pošiljateljevoj adresi, prihvatit će se, tj. ako poruka dođe direktno s imena domene, *IP4* - ako je pošiljatelj u danom rasponu IP adresa verzije 4, mehanizam se prihvaća, *IP6* - ako je pošiljatelj u danom rasponu IP adresa verzije 6, mehanizam se prihvaća, *MX* - ako ime domene ima MX zapis koji se podudara sa pošiljateljovom adresom, mehanizam se prihvaća, *PTR* - prihvaća se ako IP završava s imenom domene koji je potvrđen sa adresom primatelja, *EXISTS* – izvodi se upit kojim se traži A zapis dane domene, ako postoji mehanizam se prihvaća, *INCLUDE* – domena koja se želi dodati pretražuje se da li ima vlastiti SPF zapis. Kvantifikatori su **"~"** - koristi se za oznaku odbijanja poruke, pomoć između neutralnog odabira i odbijanja poruke, **"-"** - koristi se za se odbijanje poruke, **"+"** - koristi se za poruke koje prolaze, može se i ispustiti, +mx je jednako s mx, **"?"** - koristi se za neutralan rezultat. Modifikatori dopuštaju ektenzije u budućnosti, a do sad, samo 2 definirana u RFC 4408 su u širokoj

upotrebi: *exp* - služi za objašnjenje zašto se poruka odbila, sadrži adresu domene na kojoj se nalazi objašnjenje i *redirect* - može se koristiti umjesto ALL mehanizma, a služi za ukazivanje na SPF zapise drugih domena.

U nastavku je dan primjer SPF zapisa. Ako smo vlasnik domene example.com, a uz to šaljemo ponekad elektroničku poštu putem korisničkog računa na GMailu, DNS zapis će izgledati ispis 7:

Ispis 7. Primjer SPF zapisa u DNS bazi

```
example.net IN TXT  "v=spf1 mx a:pluto.example.net include:aspmx.googlemail.com
-all"
```

v=spf1 označuje verziju *SPF*-a koja se koristi, to je verzija 1. MX u zapisu označuje da svi poslužitelji sa example.net domene koji imaju MX zapis smiju slati elektroničku poštu za tu domenu. Oznaka *a:pluto.example.net* označuje da pluto također smije slati elektroničku poštu za danu domenu. Oznaka *include:aspmx.googlemail.com* ukazuje na to da sva pošta koja stiže example.net domene može doći od *example.net* ili *aspmx.googlemail.com*. Oznaka -all označava da sva druga računala na domeni nemaju dopuštenje slanja elektroničke pošte.

Poslužitelji koji vrše *SPF* provjeru upisuju rezultate u zaglavlje poruke. To su polja *Received-SPF* i *Authentication-Results*. Primjer rezultata dan je u ispisu 8. U primjeru se osim navedena dva polja nalazi i *Received* polje koje sadrži IP adresu poslužitelja s kojeg je poruka stigla, adresa elektroničke pošte za koju se vrši provjera IP adresa pošiljatelja poruke.

Ispis 8. Primjer polja SPF u zaglavlju poruke

```
01: Return-Path: <bitbucket@valvesoftware.com>
02: Received: from wcmx2.valvesoftware.com (wcmx2.valvesoftware.com
       [72.165.61.135]) by mx.google.com with ESMTP id
       s16si787823vcf.121.2010.08.11.11.01.37; Wed, 11 Aug 2010 11:01:37
       -0700 (PDT)
03: Received-SPF: pass (google.com: best guess record for domain of
       bitbucket@valvesoftware.com designates 72.165.61.135 as permitted
       sender) client-ip=72.165.61.135;
04: Authentication-Results: mx.google.com; spf=pass (google.com: best
       guess record for domain of bitbucket@valvesoftware.com designates
       72.165.61.135 as permitted sender)
       smtp.mail=bitbucket@valvesoftware.com
05: Received: from 72-165-61-174.dia.static.qwest.net
       ([72.165.61.174]:1798 helo=valvesoftware.com)by
       wcmx2.valvesoftware.com with smtp (Exim 4.69)
       (envelope-from <bitbucket@valvesoftware.com>)id 1OjFcO-0002rj-Rh
       for tomislav@gmail.com; Wed, 11 Aug 2010 11:01:36 -0700
```

U ispisu 8, retku 1 nalazi se adresa pošiljatelja poruke koja je *bitbucket@valvesoftware.com,* dok se u retku 5 nalazi *Received* polje koje sadrži IP adresu pošiljatelja poruke, a ona je 72.165.61.147. U retku 2 nalazi se IP adresa poslužitelja s kojeg je poruka stigla, ona je 72.165.61.135. Putem *SPF*-a se vrši provjera kojom se pokušava potvrditi pripadnost adrese pošiljatelja i domene poslužitelja. U retku 3 nalazi se *Received-SPF* polje koje putem stavke *pass* potvrđuje da domena adrese s adrese *bitbucket@valvesoftware.com* s koje je stigla poruka pripada poslužitelju s IP adresom 72.165.61.135 i da je on valjani poslužitelj za slanje poruka. Polje *Authentication-Results*

u retku 4 u stvari je lista u koju se zapisuju rezultati autentifikacije koje podržava dani poslužitelj. Tu se mogu naći zapisi koji se dobiju vršenjem *SPF*, *DKIM* provjera.

Prednosti *SPF*-a ima nekoliko, posebice kod otkrivanja i onemogućavanja pošiljatelja neželjene elektroničke pošte, budući da sprječava lažiranje *Return-Path* adrese elektroničke pošte. Također, neželjena elektronička pošta se odbija na početku, prije nego se primi tijelo poruke, tako se štede procesorski resursi na poslužitelju kao i propusna raspoloživost (engl. *bandwidth)*. Protokol je proširiv, a u budućnosti se planira spajanje sa autentifikacijskim mehanizmima. *SPF DNS* zapisi mogu se koristiti kao zasebne stavke pri ocjenjivanju reputacije nekog sustava.

No sam *SPF* ima i nekoliko nedostataka. SPF ne dopušta poslužiteljsko prosljeđivanje (engl. *redirection*). Alternative su zamjena originalnog pošiljatelja s onim koji pripada lokalnoj domeni, odbijanje slanja, zapisivanje u bijelu listu na ciljnom poslužitelju, tako da ne odbija proslijeđene poruke i automatsko prepisivanje adrese (engl. *sender rewriting sheme*). Također, korištenjem *SPF*-a se ne dopušta "legitimna prijevara", kada želimo poslati poruku preko "treće osobe", npr. elektroničke razglednice. SPF ne sprečava se slanje neželjene elektroničke pošte ukoliko osoba ima valjani korisnički račun na domeni, ali u tom slučaju lako ga se može otkriti. Također, jedan od nedostaka SPF-a je i u tome što postavljanje *DNS* zapisa traje određeno vrijeme. Općenito gledajući SPF ne sprečava neželjenu elektroničku poštu.

3. Autonomni sustavi

Na Internetu, autonomni sustav (*engl. Autonomus System*) je administrativna cjelina, tj. jedna ili više mreža koje se nalaze pod jedinstvenim administrativnim upravljanjem. Svaki autonomni sustav ima dodijeljen globalno jedinstven broj, broj autonomnog sustava (engl. *Autonomus System Number ASN*).

Mreže unutar autonomnog sustava razmjenjuju usmjerivačke informacije putem nekog *IGP*-a (engl. *Interior Gateway Protocol*). Autonomni sustavi razmjenjuju usmjerivačke informacije s drugim autonomnim sustavima putem *BGP*-a (engl. *Border Gateway Protocol*).

Autonomni sustavi mogu se podijeliti u dvije kategorije, ovisno o tome kako su povezani s drugim autonomnim sustavima i o njihovim usmjerivačkim pravilima:

- Višepristupni (*engl. Multihomed*): Autonomni sustav koji je povezan sa više drugih autonomnih sustava i dopušta da promet drugih autonomnim sustavima prolazi preko sebe. Većina velikih pružatelja Internetskih usluga su višepristupni autonomni sustavi. Takvi autonomni sustavi mogu biti spojeni s jednim, ili više drugih autonomnih sustava. Na taj način, autonomni sustavi ostaju spojeni na Internet u slučaju ispada neke od njihovih veza.
- Krajnji (*engl. Stub*): Autonomni sustav koji je spojen na samo jedan autonomni sustav. S obzirom na usmjeravanje, može ga se smatrati proširenjem drugog autonomnog sustava. U većini slučajeva, mreže s jednom vezom na Internet nemaju dodijeljen jedinstven broj autonomnog sustava, već se njihove adrese tretiraju kao dio roditeljskog autonomnog sustava.

Broj autonomnog sustava je 16-bitni cijeli broj, dakle moguće je dodijeliti 65536 vrijednosti. AS0 je rezerviran i može se koristiti za mreže koje se ne usmjeruju. Najveća vrijednost, AS65536 je također rezervirana. Blok brojeva od 64512 do 65534 je predviđen za privatnu upotrebu. AS23456 je rezerviran za tranziciju. Ostatak vrijednosti, od 1 do 64511 (osim 23456), dostupan je za korištenje u usmjeravanju putem Interneta. Brojevi su nestrukturirani, niti postoji mogućnost agregacije ili sažimanja. U novije vrijeme, uvedeni su 32-bitni cijeli brojevi kao brojevi autonomnih sustava. Ti brojevi su ili cijeli brojevi, ili brojevi tipa x.y, gdje su i x i y 16-bitni cijeli brojevi. Brojevi tipa 0.y su identični starim 16-bitnim brojevima, 1.y i 65535.65535 su rezervirani, a ostatak je slobodan za upotrebu.

Organizacija koja je, između ostalog, zaslužna za globalnu koordinaciju brojeva autonomnih sustava zove se *IANA* (Internet Assigned Number Authority). *IANA* alocira IP adrese i brojeve autonomnih sustava iz popisa nealociranih brojeva i predaje ih određenim regionalnim Internet registrarima (engl. *Regional Internet Registry RIR*) prema potrebi, a može i sama alocirati broj nekom autonomnom sustavu. Valja napomenuti da je svijet podjeljen na pet registrara kao što je prikazano na slici 3.1. To su *ARIN* koji je vezan za područje Sjeverne Amerike, *LACNIC* koji je vezan za Latinsku Ameriku i neke Karipske otoke, *AfriNIC* koji je vezan za Afričku regiju, *RIPE NCC* koji je vezan za Europu, Bliski istok i centralnu Aziju i *APNIC* koji je vezan uz Azijsko pacifičku regiju. Detaljne informacije za određenu IP adresu možemo dobiti samo ispitivanjem poslužitelja koji je vezan za regiju na kojoj se IP adresa nalazi.

Slika 3.1. Svjetski Internet registri

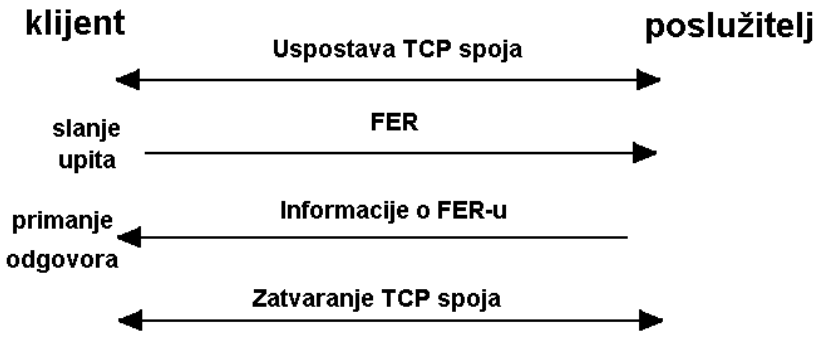
Cilj ovog rada je određivanje reputacije autonomnih sustava. Na raspolaganju imamo poruke neželjene pošte iz kojih možemo iščitati IP adrese njihovih pošiljatelja. Ono što je nama potrebno jest odrediti autonomni sustav na temelju IP adrese pošiljatelja neželjene elektroničke pošte. To se radi upotrebom *Whois* naredbe koja za danu IP adresu vraća informacije o sustavu kojem pripada.

3.1. Protokol Whois

Whois je protokol koji koristi *TCP* za prijenos, a putem niza zahtjev/odgovor pruža korisnicima Interneta informacije o imenima domena, autonomnim sustavima, IP adresama.

Whois poslužitelj čeka zahtjeve na pristupu 43. Kada klijent pošalje zahtjev prema poslužitelju, poslužitelj odgovara tekstualnim nizom. Odgovor može sadržavati više linija, a poslužitelj zatvara spoj kad završi s informacijom i tako signalizira klijentu kraj.

Primjer zahtjeva dan je na slici 3.2.



Slika 3.2. Primjer Whois upita

Kada korisnik želi saznati više informacija o nekoj domeni ili IP adresi uspostavlja TCP spoj sa whois poslužiteljem. Nakon uspješne uspostave spoja, korisnik šalje ključnu riječ pretrage (ime domene, IP adresu), a poslužitelj vraća informacije o danom zapisu. Nakon što je poslužitelj poslao sve informacije prekida se TCP spoj s klijentom.

Sam protokol Whois ne pruža integritet traženih podataka budući da neki registrari ne provjeravaju striktno informacije koje zapisuju ili ih rijetko ažuriraju.

Primjer informacija dobivenih Whois naredbom IP adresu FER-a [161.53.72.23] dan je u ispisu 9.

Ispis 9. Primjer Whois odgovora za neki IP

```
01 OrgName:    RIPE Network Coordination Centre
02 OrgID:      RIPE
03 Address:    P.O. Box 10096
04 City:       Amsterdam
05 StateProv:
06 PostalCode: 1001EB
07 Country:    NL
08 ReferralServer: whois://whois.ripe.net:43
09 NetRange:   161.52.0.0 - 161.54.255.255
10 CIDR:       161.52.0.0/15, 161.54.0.0/16
11 NetName:    RIPE-ERX-161-52-0-0
12 NetHandle:  NET-161-52-0-0-1
13 Parent:     NET-161-0-0-0-0
14 NetType:    Early Registrations, Transferred to RIPE NCC
15 Comment:    These addresses have been further assigned to users in
16 Comment:    the RIPE NCC region.  Contact information can be found in
17 Comment:    the RIPE database at http://www.ripe.net/whois
18 RegDate:    2004-02-18
19 Updated:    2004-02-18,
20 % Information related to '161.53.64.0 - 161.53.79.255'
21
22 inetnum:        161.53.64.0 - 161.53.79.255
23 netname:        CARNET-FER
24 descr:          Fakultet elektrotehnike i racunarstva
25 descr:          Unska 3
26 descr:          10000 Zagreb
27 country:        HR
28 admin-c:        CIa22-RIPE
29 tech-c:         CIa22-RIPE
30 status:         ASSIGNED PA
31 mnt-by:         AS2108-MNT
32 source:         RIPE # Filtered
33
34 role:           CARNet IP administrator
35 address:        CARNet
36 address:        J.Marohnica 5
37 address:        10000 Zagreb
38 address:        Croatia
39 abuse-mailbox:  abuse@carnet.hr
40 admin-c:        IV762-RIPE
41 admin-c:        DK2798-RIPE
42 tech-c:         IV762-RIPE
43 tech-c:         DK2798-RIPE
44 nic-hdl:        CIa22-RIPE
45 mnt-by:         AS2108-MNT
46 source:         RIPE # Filtered
```

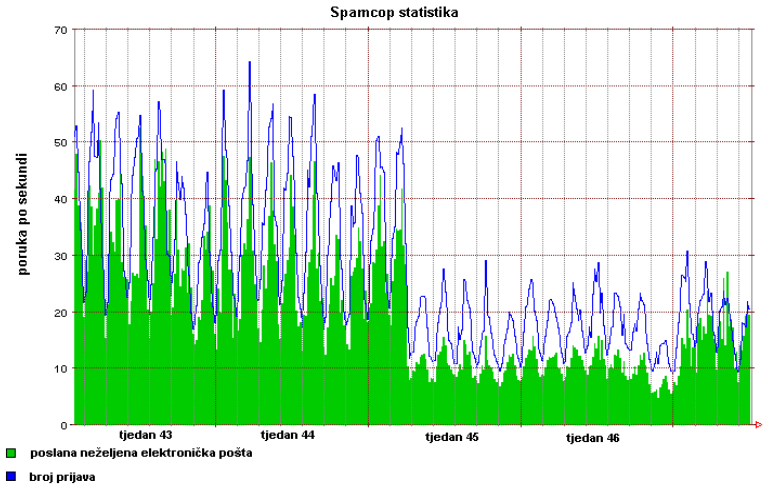
U ispisu 9, retcima 1 do 9 nalaze se informacije o registraru koji je zadužen za alokaciju Internet resursa tražene IP adrese. U primjeru je to *RIPE* registar što znači da se tražena IP adresa nalazi u Europi, Bliskom istoku, ili centralnoj Aziji. Registrar se nalazi u gradu Amsterdamu u Nizozemskoj, a adresa referentnog whois poslužitelja je whois.ripe.net. U retcima 9 do 19 nalaze se informacije o rasponu IP adresa organizacije kojoj pripada tražena IP adresa. Iz identifikatora se isčitava da je riječ o CARNet-u, a dana je i

informacija o njegovom nadređenom sustavu, datum registracije i ažuriranja tog zapisa. U retcima 20 do 46 nalaze se informacije za autonomni sustav u kojem se nalazi tražena IP adresa. To su raspon IP adresa kojima se autonomni sustav služi, ime sustava i adresa. Tu se nalazi i broj autonomnog sustava Carnet koji je 2108.

3.2. Primjeri malicioznih sustava

3.2.1. McColo mreža

McColo je bio pružatelj Internetskih usluga lociran u San Joseu. Krajem 2008. godine kompanija je ukinuta od strane dva viša poslužitelja, Global Crossing i Hurricane Electric, budući da se značajan dio svjetskih malicioznih programa i upravljačkih poslužitelja mreža kompromitiranih računala nalazio upravo na McColo mreži [10, 13]. Na slici 3.3 vidljivo je da su do vremena kad je kompanija ukinuta, korisnici McColo mreže bili odgovorni za velik dio u slanju neželjene elektroničke pošte, dok se nakon ukidanja mreže ukupni obujam svjetske neželjene pošte smanjio za dvije trećine [11, 12].



Slika 3.3. Pad udjela neželjene elektroničke pošte nakon ukidanja McColo tvrtke

McColo je bio jedna od vodećih kompanija u pružanju usluga bilo kome, bez obzira na pritužbe. Na njegovim poslužiteljima nalazili su se upravljački poslužitelji nekoliko velikih mreža kompromitiranih računala, Mega-D, Srizbi, Pushdo, Rustock i Warezov. U jednom tjednu, oko 1.5 milijuna različitih računala, slalo je putem Srizbija ili Rustocka neželjenu elektroničku poštu [9, 12].

Ukidanje McColo poslužitelja najviše je pogodilo Srizbi mrežu kompromitiranih računala, koja je u tom trenutku bila najveća svjetska mreža kompromitiranih računala i uključivala je 500.000 čvorova. U to vrijeme, mreža je bila u mogućnosti slati 60 milijardi poruka neželjene elektroničke pošte na dan, što je više od pola sveukupnog svjetskog udjela koji je iznosio 100 milijardi poruka [12].

Već u travnju 2009. godine, slanje neželjene elektroničke pošte vratilo se na razmjere kakve je imalo prije ukidanja McColo tvrtke [11]. Razlog tome bilo je stvaranje novih mreža kompromitiranih računala, kao i uključivanje starih.

3.2.2. Russian Business Network

Russian Business Network (RBN) [13] je organizacija koja se bavi ilegalnim aktivnostima na Internetu vezanim uz krađu i preprodaju osobnih podataka. Organizacija je registrirana u St. Petersburgu 2006. godine i ispočetka se bavila legalnim radnjama no ubrzo joj se posao sveo na dječju pornografiju, slanje neželjenih elektroničkih poruka, prijevare, maliciozne programe i pružanje Internetskih usluga bez obzira na pritužbe drugih korisnika.

Russian Business Network je vrlo teško pratiti, budući da sama organizacija nije registrirana, a domene su registrirane na anonimne adrese. Organizacija se ne oglašava, dok sve transakcije obavlja elektroničkim putem. Organizacije koje se bore protiv RBN-a često su meta distribuiranog napada uskraćivanjem resursa.

Russian Business Network krade osobne podatke korištenjem lažnih programa za borbu protiv zloćudnih i špijunskih programa. Najpoznatiji program je *MalwareAlarm* koji korisniku nudi opciju besplatnog testa računala, nakon kojeg prijavi probleme na računalu i nagovori korisnika da plati za punu verziju programa.

RBN je poznat pod više imena, za neke se dijelove smatra da djeluju samostalno, a neki dijelovi su bazirani u raznim državama. Imena su RBNet, RBNetwork, RbusinessNetwork, iFrame Cash, SBT Telecom Network lociran u Sejšelima, Aki Mon Telecom, 4Stat, Eexhost, DefconHost, Rusouvenirs Ltd., Tcs Network lociran u Panami, Nevcon Ltd. Lociran u Panami, Micronnet Ltd., Too coin Software lociran u Velikoj Britaniji, 76Sservice, MalwareAlarm lociran u Češkoj, InstallsCash, Jiangsu Network Co., LTD, Heihachi LTD.

Uz RBN se veže Zeus mreža kompromitiranih računala. Zeus je trojanski konj koji na kompromitiranom računalu krade bankovne podatke i većinom se nalazi na računalima u vlasništvu velikih tvrtki. Prava veličina kompromitirane mreže nije poznata, a u Americi je zabilježeno 3.6 milijuna zaraženih računala [13, 14]. U novije vrijeme kompromitirana računala šalju poruke koje sadrže trojanski konj ili poveznice za preuzimanje, putem elektroničke pošte ili društvenih mreža. Na taj način povećavaju svoju mrežu. Zeus je još poznat pod imenima Zbot, PRG, Wsnpoem, Gorhax i Kneber.

4. Liste pošiljatelja neželjene elektroničke pošte

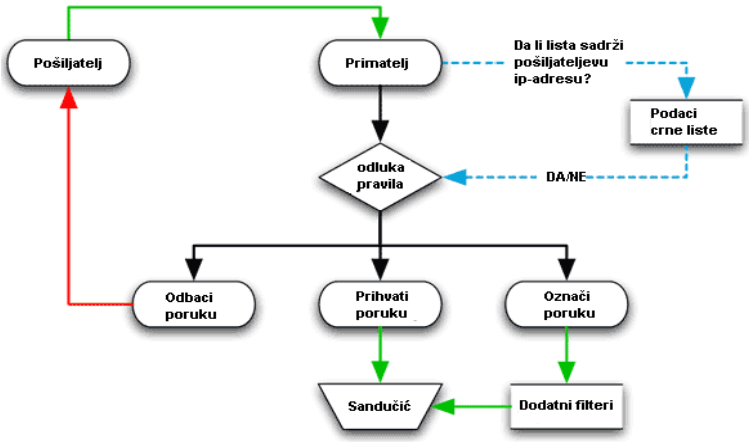
Crne liste (engl. *Domain Name System Blacklist – DNSBL*) su liste koje služe za blokiranje neželjene elektroničke pošte. Većina poslužitelja elektroničke pošte može se podesiti da odbace ili označe elektroničku poštu koja dolazi s nekog izvorišta sadržanog u crnoj listi. Liste koriste *DNS* da bi pretvorili IP adrese npr. 140.15.84.2 u imena domena npr. *example.net*. Prilikom provjere
IP adrese poruke elektroničke pošte, ako je korisnik crne liste u prošlosti već primio neželjenu elektroničku poštu s te domene, poslužitelj se dodaje u crnu listu i sve poruke primljene od njega se odbacuju ili označuju. Dijagram provjere IP adrese prikazan je na slici 4.1.

Slika 4.1. Provjera IP adrese u crnoj listi

Kada poruka elektroničke pošte stigne na odredišni poslužitelj, vrši se provjera u nekoj od crnih listi koje mogu biti dostupne lokalno ili kao usluga na nekim od specijaliziranih poslužitelja. Odgovor koji stigne od crne liste može biti jednostavan tipa da/ne ukazujući samo na postojanje IP adrese u listi, ili u složen ovisno o složenosti same liste u kojem svaki dio liste vraća svoju ocjenu.

Odluka o tome da li će se poruka elektroničke pošte primiti, odbaciti ili označiti ostaje isključivo na primatelju, što je prikazano na slici 4.2. Ako se IP adresa pošiljatelja ne nalazi u crnoj listi poruka se prihvaća, a ako se nalazi ne mora se nužno odbiti već se može označiti za daljnju obradu. Propuštanjem označene poruke kroz dodatne filtre možemo donijeti konačnu odluku od prihvaćanju ili odbijanju dospjele poruke. Crne liste, kao i ostali filtri neželjene elektroničke pošte, samo odgovaraju na pitanje da li se određeni uvjet ispunio ili ne.

Na Dnsbl Web stranici [18] nalazi se popis 81 najkorištenijih aktivnih crnih lista, na kojoj se nudi i mogućnost provjere da li se neka IP adresa nalazi u nekoj od crnih lista.



Slika 4.2. Odluka nakon provjere IP adrese

Na Internetu postoji mnoštvo sustava koji prate pošiljatelje neželjene elektroničke pošte, a temelje se na crnim listama koje se popunjavaju na razne načine, postavljanjem zamki (engl. *honeypot*) i složenim algoritmima za detekciju neželjene elektroničke pošte. Podaci su dostupni na Internetu, putem upita na bazu ili putem specijaliziranih klijenata na lokalnom računalu.

Sustavi se dijele na aktivne i pasivne. Aktivni sustavi baziraju se na pronalasku originalnog pošiljatelja neželjene pošte, blokiranju njegovog daljnjeg rada i proslijeđivanju podataka zakonskim udrugama. Pasivni sustavi se bave razvijanjem algoritama za detekciju neželjene elektroničke pošte i putem određenih pravila štite korisnike. Poduzimanje daljnjih koraka pasivnih sustava nije u opisu posla.

Nijedan od ovih servisa ne nudi ono što nama treba, budući da ciljaju direktno na pošiljatelje neželjene elektroničke pošte, a nama je bitno otkrivanje autonomnih sustava s kojih ti pošiljatelji rade. U nastavku je navedeno par najpoznatijih servisa od kojih se izdvaja Spamhaus kao najveći aktivni servis s detaljnim podacima o pošiljateljima neželjene elektroničke pošte. Za svaki sustav su navedeni načini na koji prikupljaju informacije i kako se do njih može doći.

4.1. Spamhaus

Spamhaus je sustav koji prati pošiljatelje neželjene elektroničke pošte, njihove skupine i servise, pruža zaštitu od neželjene elektroničke pošte u realnom vremenu i sudjeluje s organima zakona u identifikaciji i progonjenju pošiljatelja neželjene elektroničke pošte u čitavom svijetu.

Upiti se prema Spamhaus-ovim crnim listama mogu slati na dva načina. Poslužitelj elektroničke pošte može slati upite Spamhausovim besplatnim poslužiteljima, ili slati upite lokalno, privatnim poslužiteljima na lokalnoj mreži koji imaju kopiju Spamhaus podataka. Također, na Spamhaus Web stranici postoji forma za pojedinačne upite, no automatizacija upita je zabranjena.

Spamhaus usluge možemo koristiti na dva načina, besplatni i profesionalni. Da bi mogli besplatno koristiti uslugu, naše korištenje usluge mora biti nekomercijalno, promet elektroničkih poruka mora biti manji od 100.000 *SMTP* konekcija na dan i upiti prema

listama moraju biti ispod 300.000 na dan. Ukoliko upotreba premašuje te kriterije, moramo prijeći na profesionalnu upotrebu.

Servis sadrži nekoliko crnih listi: SBL, XBL, PBL, DBL, DROP i ROKSO.

ROKSO (Register Of Known Spam Operations) je baza s informacijama i dokazima o profesionalnim pošiljateljima neželjene elektroničke pošte.

Osamdeset posto neželjene elektroničke pošte primljene u Sjevernoj Americi i Europi može se povezati, putem aliasa, adresa, lokacija, domena s grupom od oko 100 poznatih organizacija koje se većinom nalaze u ovoj listi. Svaka organizacija neželjene elektroničke pošte sastoji se od jednog do pet pošiljatelja, što u globalu daje 300-400 pošiljatelja neželjene elektroničke pošte. Isječak *ROKSO* liste prikazan je na slici 4.3.

Većina pošiljatelja neželjene elektroničke pošte djeluje ilegalno, seleći se s jedne mreže na drugu i jedne države u drugu, u potrazi za pružateljima Internet usluga sa slabom sigurnošću, ili onih koji ne primjenjuju politiku protiv neželjene elektroničke pošte. Velik dio njih pretvara se da svoje operacije vrše van države u kojoj se nalaze, dok se ostali sakrivaju iza anonimnosti i prave se da su mali pružatelji Internet usluga, i da neželjena elektronička pošta pristiže od strane nepostojećih korisnika. Nakon što ih se ukloni s određenog pružatelja Internet usluga, jednostavno prelaze na novi, već podešen. Jednom sadržan u ROKSO listi, sve IP adrese pod vlasništvom pošiljatelja neželjene elektroničke pošte se automatski i preventivno ubacuju u listu.

The ROKSO List	5/23/10
Known Spam Operation	Country
Alan Alvarez - DMG	United States
Alan Ralsky	United States
Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov	Ukraine
Andria Petito / Tranzact Media	United States
Anton Gorodov / Gorodetsk - srx / s-rx	Russia
AWG aka youngjoo aka qline	Japan
Bill Waggoner	United States
Bison Delivery Systems	United States
Brendan Battles / IMG Online / World-Services	United States
Brian Kramer / Expedite Media Group	United States
Caliber One / caliberone.net - Kurt Lemmings	United States
Canadian Pharmacy	Ukraine
Christopher Alesich / Vividstream	United States
Chuck An / iomega	United States
Dan Abramovich	United States
Darrin Wohl	United States
Data Champions / Sloan Marketing	India
Earthstore	United States
elogic.cc	United States
emailspidereasy.com	China

Slika 4.3. Rokso popis

Za svakog pošiljatelja neželjene elektroničke pošte postoji detaljan opis što je prikazano sa slici 4.4, a sadrži glavne informacije o pošiljatelju, domene kojima se koristi, informacije o poslovima kojima se bavi, primjeri poruka neželjene elektroničke pošte i razne druge informacije. Zapisi u *SBL* listi koje se tiču *ROKSO* pošiljatelja neželjene elektroničke pošte posebno su označene u svrhu obraćanja posebne pažnje od strane pružatelja Internet usluga. Zakonske udruge određenih zemalja imaju pristup povjerljivim podacima o organizacijama sadržanim u *ROKSO* listi uz čiju pomoć lakše procesiraju pošiljatelje neželjene elektroničke pošte koji krše zakon. Mnogi pružatelji Internet usluga koriste listu mogućih korisnika da bi provjerili sumnjive korisnike prije nego što im pruže usluge i IP prostor.

Slika 4.4: Detaljne informacije o pošiljatelju neželjene elektroničke pošte

Podaci u listi nisu trajni, ako se ne pronađe nikakva aktivnost pošiljatelja neželjene elektroničke pošte tijekom šest mjeseci, podaci se privremeno brišu, no ako se nastavi sa slanjem podaci se vraćaju u listu.

SBL (Spamhaus Block List) je lista IP adresa s kojih se ne preporuča primanje elektroničke pošte. Ona sadrži zapise o raznim izvorima neželjene elektroničke pošte poput poznatih pošiljatelja neželjene elektroničke pošte, bilo da rade sami ili u skupinama, organizacijama i sustavima koji pomažu u slanju neželjene elektroničke pošte. Sustavi elektroničke pošte na cijelom Internetu šalju listi SBL upite koja omogućuje administratoru poslužitelja elektroničke pošte da identificira, označi ili blokira dolazeće spojeve sa IP adresa za koje Spamhaus smatra da su umiješani u slanje poruka neželjene elektroničke pošte. Lista se koristi za blokiranje pošiljateljeve IP adrese, kao i za blokiranje Web stranica oglašavanih u porukama.

Lista se provjerava tako što poslužitelj elektroničke pošte šalje upite na adresu *sbl.spamhaus.org*

Trenutno lista u prosjeku sprečava 5-10% neželjene elektroničke pošte u trenutku *SMTP* spajanja, i od 60-90% neželjene elektroničke pošte provjeravajući tijelo poruke za poveznicama na Internet stranice [19]. Lista je namijenjena da se koristi sa drugim listama, budući da ona cilja samo na pošiljatelje neželjene elektroničke pošte koji šalju sa fiksnih lokacija, a ažurira se svakih 10 minuta [19]. Postavljanje zapisa u listu je trenutno, a u nekim slučajevima i preventivno, i ne zahtjeva slanje upozorenja. Kriteriji za upis u listu su slijedeći:

- Izvori neželjene elektroničke pošte: Izvori neželjene elektroničke pošte koji su slali na Spamhausove zamke ili podaci koje šalje povjerljiva treća strana.

- Usluge slanja neželjene elektroničke pošte: Poslužitelji elektroničke pošte koji su identificirani kao sastavni dio operacija slanja neželjene elektroničke pošte ili koji su pod direktnom kontrolom pošiljatelja neželjene elektroničke pošte.
- Organizacije slanja neželjene elektroničke pošte: Poznate grupe i organizacije vezane uz slanje neželjene elektroničke pošte koje su sadržane u ROKSO registru, uključujući i preventivno uključivanje novih IP adresa ukoliko se pošiljatelj neželjene elektroničke pošte prebaci na novi poslužitelj.
- Usluge pomaganja pošiljateljima neželjene elektroničke pošte: Usluge i sustavi koji pomažu organizacijama sadržanim u *ROKSO* registru, u što ulazi pružanje Internetskih usluga bez obzira na žalbe, pružanje usluga anonimnog slanja elektroničke pošte, prodavanje liste adresa elektroničke pošte, namjerno posluživanje pošiljatelja neželjene elektroničke pošte.

XBL (Exploits Block List) je baza IP adresa računala koja su zaražena virusom, crvom, ili trojanskim konjem, a uključuje kompromitirana računala i otvorene posredničke poslužitelje.
Lista se ažurira svakih 15 minuta, a podatke popunjavaju dva povjerljiva izvora:

- *CBL* (Composite Black List)
- *NJABL* lista otvorenih posredničkih poslužitelja

Trenutni podaci pokazuju da *XBL* lista može zaustaviti u prosjeku 50-70% neželjene elektroničke pošte [20].

Lista sadrži popis dinamičkih IP adresa, što znači da je u jednom trenutku IP adresa bila povezana s kompromitiranim računalom.

PBL (Policy Block List) je baza IP adresa računala koja ne bi smjela dostavljati neautoriziranu elektroničku poštu.

Svaka mreža koja sudjeluje u *PBL* projektu dodaje raspon IP adresa u *PBL* listu. Dodatne blokove IP adresa dodaju i održavaju Spamhaus administratori, posebno mreže koje ne sudjeluju aktivno u projektu, i za raspon IP adresa koje tipično sadrže veliku koncentraciju kompromitiranih računala, koji su velik izvor neželjene elektroničke pošte. Lista sadrži i dinamičke i statičke IP adrese, tj. bilo koju IP adresu s koje nebi smjela direktno pristizati elektronička pošta.

Odlika ove liste je što omogućuje krajnjim korisnicima sa statičkom IP adresom unutar većeg raspona IP adresa i administratorima valjanih poslužitelja elektroničke pošte ubacivanje svojih mišljenja o tome da je njihova IP adresa povjerljivo izvorište elektroničke pošte. Iz liste je moguće obrisati zapise no zaštite su uključene da bi se spriječila zloupotreba od strane pošiljatelja neželjene elektroničke pošte.

PBL lista nije crna lista, već lista IP adresa koje se korisnicima dodjeljuju dinamički, normalno za korisnicima širokopojasnog interneta. Normalna stvar je da se dinamičke IP adrese nalaze u listi, dok bi se u najboljem slučaju, sve svjetske dinamičke IP adrese trebale tamo nalaziti. U listi bi se također trebale i nalaziti statičke IP adrese koje se ne bave slanjem elektroničke pošte.

PBL i *XBL* liste se koriste za blokiranje pošiljatelja neželjene elektroničke pošte koji vrše kriminalne radnje s ciljem slanja neželjene elektroničke pošte. Te liste su napravljene s ciljem sprečavanja neželjene elektroničke pošte koja pristiže s mreža kompromitiranih računala ili posredničke poslužitelje.

DBL (Domain Block List) je baza domena pronađenih u neželjenim porukama elektroničke pošte. Poslužitelji elektroničke pošte koji imaju sposobnost provjeravati tijelo poruke za imenima i IP adresama domena mogu koristiti listu za identificiranje, klasificiranje i odbijanje neželjene elektroničke pošte koja se nalazi u *DBL* listi. Lista uz imena domena Internet stranica koja se nalaze u tijelu poruke elektroničke pošte također sadrži i listu imena domena koja se nalaze u *From, Reply-To* i *Message-ID* stavkama u zaglavlju poruke.

Lista koristi kodove koje vraća na *DNS* upit u formatu 127.0.1.0/24 koji su dani u tablici 4.1.

Tablica 4.1. Povratni kodovi DNS upita

Kod	Izvor podataka
127.0.1.2	Domene pošiljatelja neželjene elektroničke pošte
127.0.1.3-.19	Domene pošiljatelja neželjene elektroničke pošte (rezervirano za buduću upotrebu)
127.0.1.20-.39	*Phishing* domene (rezervirano za buduću upotrebu)
127.0.1.40-.59	Domene zloćudnih programa (rezervirano za buduću upotrebu)
127.0.1.255	Zabranjeni IP upiti

DBL je strogo lista imena domena i ne sadrži IP adrese.

Trenutni testovi pokazuju da ako se koristi samo ta lista, u mogućnosti je zaustaviti od 60 do 90 posto dolazne neželjene elektroničke pošte provjeravajući tijelo poruke [21]. Dodatno se taj postotak može povećati ukoliko se testira pošiljateljeva domena u tijekom *SMTP* prijenosa.

Lista se ažurira svake dvije minute [21] kako bi se osiguralo da su nove domene pošiljatelja neželjene elektroničke pošte blokirane, a one krivo izlistane brzo maknute.

DROP (Don't Route Or Peer List): je lista blokova IP adresa koji pod kontrolom profesionalnih pošiljatelja neželjene elektroničke pošte i blokova IP adresa kompromitiranih računala. Lista je manji dio SBL liste predviđen za korištenje u sigurnosnim stijenama i usmjerivačkim komponentama.

U listi se nikad ne nalaze IP adrese koje su u vlasništvu valjanih mreža, čak i ako se koriste za slanje neželjene elektroničke pošte. Lista samo sadrži blokove IP adresa koje su alocirane direktno putem Regionalnog Internet Registra (RIR) ili Nacionalnog Internet Registra (NIR) kao što su *ARIN*, RIPE, *AFRINIC*, *APNIC*, *LACNIC*, *KRNIC*, a nezakonito su uzeti od originalnih vlasnika. To su ukradeni blokovi IP adresa, uzeti od kompanija koje su prestale s radom, a sad su pod kontrolom pošiljatelja neželjene elektroničke pošte.

Kad se lista implementira u usmjerivače na pružatelju Internet usluga, pomaže u štićenju mreže od pošiljatelja neželjene elektroničke pošte, sakupljanja adresa elektroničke pošte, otimanja domena i raspodjeljenih napada uskraćivanjem resursa.

ZEN je kombinacija crnih lista temeljenih na bazama IP adresa, a sadrži *SBL*, *XBL* i *PBL* crne liste zajedno. Ako se u poslužitelju elektroničke pošte koristi filtriranje putem crnih lista, Spamhaus preporuča korištenje samo *ZEN* liste.

Crne liste Spamhausa namjenjene su za korištenje tijekom *SMTP* dijaloga, omogućujući tako da se neželjena elektronička pošta odbaci rano u prijenosu, prije nego što dalje optereti poslužitelje. Preporuča se upotreba upita na *SBL*, *XBL* i *PBL* liste, budući da svaka blokira različite izvore neželjene elektroničke pošte. Sve tri liste skupa su dostupne preko Zen zone i prikazane u tablici 4.2.

Tablica 4.2. Spamhaus zone

Lista	Zona upita	Odgovor	Sadržaj
SBL	sbl.spamhaus.org	127.0.0.2-3	Statički izvori neželjene elektroničke pošte, provjereni servisi i ROKSO registar
XBL	xbl.spamhaus.org	127.0.0.4-7	Ilegalni posrednički poslužitelji, crvi i trojanski konji
PBL	pbl.spamhaus.org	127.0.0.10-11	Raspon IP adresa koje ne bi smjele slati neautentificiranu elektroničku poštu
ZEN	zen.spamhaus.org	127.0.0.2-11	Kombinirana zona, uključuje SBL, XBL i PBL

Značenje pojedinih povratnih kodova pri upitu crne liste IP adresa prikazano je u tablici 4.3.

Tablica 4.3. Povratni kodovi Spamhaus zona

Povratni kod	Zona	Opis
127.0.0.2	SBL	Spamhaus SBL podaci
127.0.0.3	SBL	Spamhaus SBL CSS podaci
127.0.0.4	XBL	CBL podaci
127.0.0.5	XBL	NJABL podaci
127.0.0.10	PBL	Podaci pružatelja Internet usluga
127.0.0.11	PBL	Spamhaus PBL podaci

Spamhaus koristi predefinirane povratne kodove ovisno o korištenoj listi. Tablica tih kodova prikazana je u tablici 4.4.

Tablica 4.4. Općenita konvencija povratnih kodova

Povratni kod	Opis
127.0.0.0/24	Crna lista IP adresa
127.0.1.0/24	Crna lista domena
127.0.2.0/24	Bijele liste

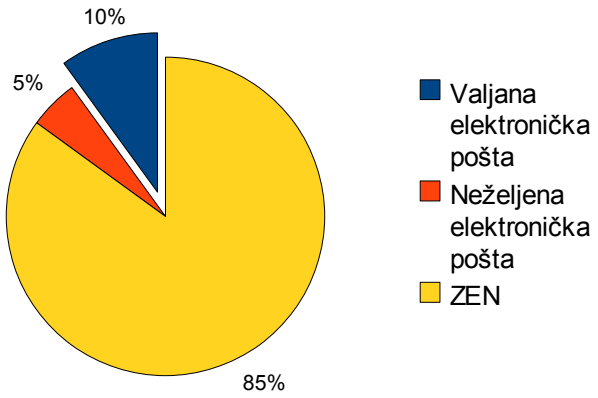
Primjer upita na Spamhaus crne dan je u nastavku, kao primjer je korištena IP adresa 116.25.63.23.

```
upit: korisnik:~$ host 23.63.25.116.pbl.spamhaus.org
odgovor: 23.63.25.116.pbl.spamhaus.org has address 127.0.0.11
upit: korisnik:~$ host 23.63.25.116.xbl.spamhaus.org
odgovor: 23.63.25.116.xbl.spamhaus.org has address 127.0.0.4
upit: korisnik:~$ host 23.63.25.116.dbl.spamhaus.org
odgovor: 23.63.25.116.dbl.spamhaus.org has address 127.0.1.255
upit: korisnik:~$ host 23.63.25.116.zen.spamhaus.org
odgovor: 23.63.25.116.zen.spamhaus.org has address 127.0.0.11
odgovor: 23.63.25.116.zen.spamhaus.org has address 127.0.0.4
```

Odgovor 127.0.0.11 PBL liste potvrđuje da se ispitivana adresa nalazi u njoj, tj. da dana IP adresa nije autorizirana za dostavljanje elektroničke pošte, dok odgovor 127.0.0.4 označava da je dana IP adresa pridružena kompromitiranom računalu (CBL lista). Odgovor 127.0.0.255 DBL liste označava zabranjeni upit, budući da DBL lista sadrži imena domena. Upitom skupne ZEN liste potvrđuju se odgovori pojedinačnih listi.

Efektivno filtriranje neželjene elektroničke pošte putem Spamhausa treba se gledati kao proces od dva koraka, pri čemu se najbrži i najjeftiniji proces odvija na početku u cilju smanjivanja velike količine neželjene elektroničke pošte na manji dio, pogodniji za daljnje filtriranje. Koristeći Spamhausovu crnu listu *ZEN* (*PBL*, *XBL* i *SBL*), Internetske mreže mogu s velikom sigurnošću odbaciti 85% dolazne elektroničke pošte tijekom *SMTP* dijaloga, prije nego se poslužitelji opterete s daljnjim procesiranjem. Ostatak neželjene elektroničke pošte filtrira se u drugom koraku putem *DBL* crne liste. Ovaj način filtriranja ima učinkovitost od 99% uz nula lažnih pozitiva.

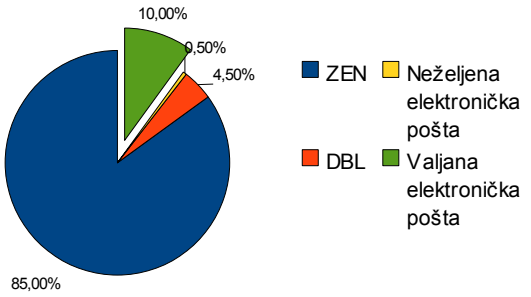
Prvi korak procesa je postavljanje *ZEN* crne liste na poslužitelj elektroničke pošte. Ta lista je u mogućnosti identificirati i odbaciti oko 85% dolazne elektroničke pošte što je prikazano na slici 4.5 uz jako nizak postotak lažnih pozitiva [12]. Ako elektronička pošta stiže sa poslužitelja koji se nalazi u jednoj od *ZEN* crnih listi, *SMTP* dijalog se mora se prekinuti tijekom *RCPT TO* naredbe. Na taj način tijelo poruke se ne prenosi na poslužitelj pa se štede resursi. Ovaj način je vrlo učinkovit, budući da sa sigurnošću rješava tri



Slika 4.5: Prvi korak filtera

četvrtine dolaznog prometa. U slučaju da se greškom blokira legitimni pošiljatelj on je o tome odmah obaviješten putem svojeg poslužitelja elektroničke pošte.

Drugi korak je propuštanje preostale elektroničke pošte kroz dublje filtere koji provjeravaju tijelo poruke specifično tražeći domene i IP adrese Internet stranica koje se u njima spominju. To se radi korištenjem programa specijaliziranih za brzo provjeravanje tijela poruka u kojima se traže domene i nakon toga provjeravaju u *DBL* crnoj listi. Velika većina neželjene elektroničke pošte sadrži poveznice na Web stranice, a tim putem i na domene. Pronalazak i blokiranje tih domena je upravo ono za što je *DBL* crna lista napravljena. Dodatak svemu je i pretraživanje domena u *SBL* listi, budući da se u 60% neželjene elektroničke pošte nalaze poveznice koje se nalaze u *SBL* crnoj listi. Preostala neželjena elektronička pošta je nakon dva koraka svedena na 0.5% [12] što se vidi na slici 4.6, koja se zatim može lako provjeriti putem aplikacija poput SpamAssassin-a.



Slika 4.6. Drugi korak filtera

4.2. Spamcop

Spamcop je besplatni sustav usluga koji pronalazi izvor neželjene poruke elektroničke pošte i prijavi ga njegovom pružatelju Internetskih usluga, a također sadrži i crnu listu pošiljatelja neželjene elektroničke pošte. Sastoji se od tri dijela, servisa za prijavu, servisa za elektroničku poštu i crne liste. Prijave generiraju statistiku koja se ukomponira u crnu listu koju koristi servis pošte kao filter. Sustav se temelji na principu parsiranja zaglavlja poruke elektroničke pošte koje šalju korisnici.

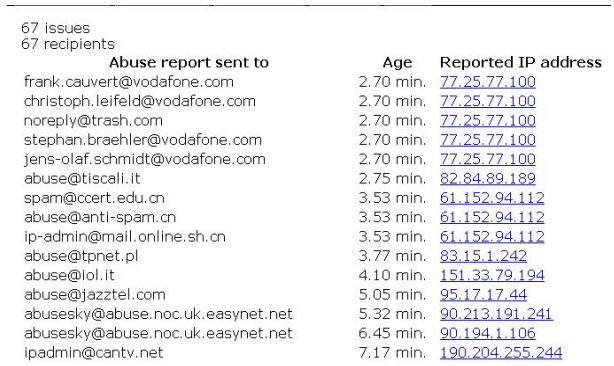
Na sustavu su dostupne liste o izvorima neželjene elektroničke pošte kao i oglašavanim stranicama u njima. Također su dostupni i godišnji, mjesečni, tjedni i dnevni izvještaj o poslanoj neželjenoj elektroničkoj pošti. Crne liste možemo pregledavati putem forme na na Web stranici tako da ispitujemo svaku IP adresu posebno, dok se crna lista koristi u poslužiteljima elektroničke pošte tako da se u filter postavi adresa: *bl.spamcop.net*, npr za IP adresu 116.25.63.23:

```
upit: wraith@fly:~$ host 23.63.25.116.bl.spamcop.net
odgovor: 23.63.25.116.bl.spamcop.net has address 127.0.0.2
```

Za danu IP adresu odgovor 127.0.0.2 označuje da se tražena adresa nalazi u *SpamCop* crnoj listi.

Na *Web* stranici su dostupni podaci o slanju neželjene elektroničke pošte koje se trenutno dešava, podaci o vodećim pošiljateljima neželjene elektroničke pošte, statistički izvještaji o svim blokovima IP adresa u svijetu i izvještaji o ukupnoj količini poslane neželjene elektroničke pošte u proteklom danu, zadnjem tjednu, mjesecu i godini.

Podaci o slanju neželjene elektroničke pošte koje se trenutno dešava nalaze se u dvije liste. To su lista IP adresa i lista količine prijavljene neželjene elektroničke pošte u zadnjih 30 minuta. Prva lista pokazuje IP adresu s koje je pristigla neželjena elektronička pošta, adresu na koju je poslana prijava za tu IP adresu i vrijeme proteklo od prijave kao i što je prikazano na slici 4.7. Prije 4min i 10 sekundi prijavljena je adresa 83.15.1.242 sa slike 4.7, a *Spamcop* je poslao pritužbu na adresu korisničke službe abuse@iol.it.



67 issues
67 recipients

Abuse report sent to	Age	Reported IP address
frank.cauvert@vodafone.com	2.70 min.	77.25.77.100
christoph.leifeld@vodafone.com	2.70 min.	77.25.77.100
noreply@trash.com	2.70 min.	77.25.77.100
stephan.braehler@vodafone.com	2.70 min.	77.25.77.100
jens-olaf.schmidt@vodafone.com	2.70 min.	77.25.77.100
abuse@tiscali.it	2.75 min.	82.84.89.189
spam@ccert.edu.cn	3.53 min.	61.152.94.112
abuse@anti-spam.cn	3.53 min.	61.152.94.112
ip-admin@mail.online.sh.cn	3.53 min.	61.152.94.112
abuse@tpnet.pl	3.77 min.	83.15.1.242
abuse@iol.it	4.10 min.	151.33.79.194
abuse@jazztel.com	5.05 min.	95.17.17.44
abusesky@abuse.noc.uk.easynet.net	5.32 min.	90.213.191.241
abusesky@abuse.noc.uk.easynet.net	6.45 min.	90.194.1.106
ipadmin@cantv.net	7.17 min.	190.204.255.244

Slika 4.7. Izvor neželjene elektroničke pošte

Slika 4.8 prikazuje drugu listu koja sadrži Internet stranice koje se oglašavaju u porukama neželjene elektroničke pošte, vrijeme od prijave i adresa elektroničke pošte na koju je prijava poslana.

19 issues
27 recipients

Abuse report sent to	Age	Reported web site
spam@ms1.hinet.net	7.57 min.	http://linda-michelle.com.tw/nationaliB¢¯¢¸¢´¢·...
mehmet@omnis.com.tr	9.90 min.	http://www.samsunnuf.gov.tr/matrix26.html
abuse@ntt.net	12.08 min.	http://onlinegame.kojyuro.com/slangy68.html
noc@noc.kddnet.ad.jp	12.08 min.	http://onlinegame.kojyuro.com/slangy68.html
abuse@ucom.ne.jp	12.08 min.	http://onlinegame.kojyuro.com/slangy68.html
postmaster@ucom.ne.jp	12.08 min.	http://onlinegame.kojyuro.com/slangy68.html
abuse@kddnet.ad.jp	12.08 min.	http://onlinegame.kojyuro.com/slangy68.html
mehmet@omnis.com.tr	12.28 min.	http://www.samsunnuf.gov.tr/matrix26.html
abuse@ip.datagroup.ua	14.83 min.	http://goldstraight.ru/
abuse@server.ua	14.83 min.	http://goldstraight.ru/
postmaster#ans.mk.ua@devnull.spamcop.net	14.83 min.	http://goldstraight.ru/
abuse@ans.mk.ua	14.83 min.	http://goldstraight.ru/
abuse@cyso.net	16.32 min.	http://www.tuningsystems.nl/duffer34.html
pny0118@empal.com	16.52 min.	http://bluecourt.ru/
sjkim11@tbroad.com	16.52 min.	http://bluecourt.ru/
nypark@tbroad.com	16.52 min.	http://bluecourt.ru/

Slika 4.8. Oglašavane Internet stranice

Vodeći ciljevi pošiljatelja neželjene elektroničke pošte prikazani su na slici 4.9. Prikazana e lista koja prikazuje ciljeve pošiljatelja neželjene elektroničke pošte, njihov reverzni *DNS* zapis, broj poslane neželjene elektroničke pošte, postotak ukupnog udjela, starost zapisa i vrijeme kroz koje je sustav promatran.

Top 200 targets of spam reports
For the week ending Sun May 23 2010 09:05:27 GMT+0200 (Central European Daylight Time) +0200 with share of total 200.

Skip to domain summary

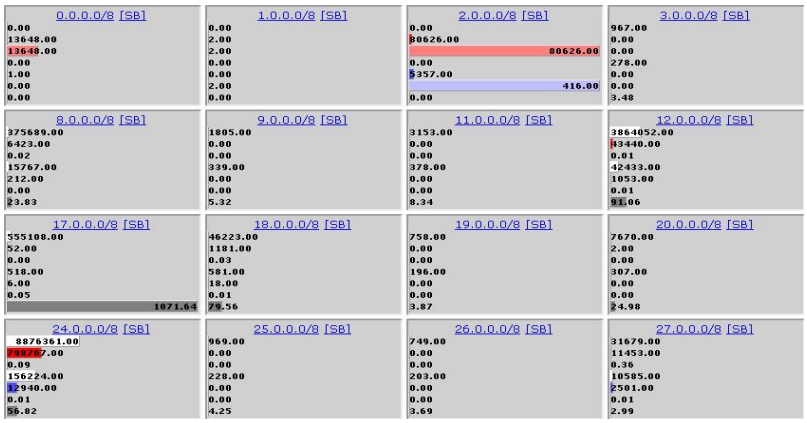
#	IP (reverse dns)	Qty.	Share	Age	Duration
1	72.21.7.79 (mailing.publicwire.com)	85361	0.089%	40 hours	9.3 days
2	187.45.193.223 (hm2814.locaweb.com.br)	74797	0.078%	2.6 days	68.3 days
3	111.224.250.131	55057	0.057%	2.1 days	42.4 days
4	111.224.250.133	49104	0.051%	2 hours	85.9 days
5	111.224.250.129	46307	0.048%	4.1 days	42.9 days
6	74.208.166.151 (www.bagcrafters.com)	45918	0.048%	16 hours	29.8 days
7	111.224.250.130 (ip-187-91-97-250.user.vivozap.com.br.)	45705	0.048%	3.1 days	85.9 days
8	111.224.250.132	41799	0.043%	26 hours	85.7 days
9	111.224.250.134	39751	0.041%	0 hours	114.0 days
10	83.16.167.14 (agl14.internetdsl.tpnet.pl)	35777	0.037%	0 hours	15.8 days
11	211.191.174.141	26093	0.027%	0 hours	206.3 days
12	67.217.50.44	24270	0.025%	0 hours	45.4 days
13	221.143.46.33	23733	0.025%	0 hours	152.1 days
14	209.239.47.205 (host.twpfsecure.com)	22619	0.024%	34 hours	29.4 days
15	94.212.16.61 (5ED4103D.cable.ziggo.nl)	22454	0.023%	0 hours	17.9 days

Slika 4.9. Ciljevi pošiljatelja neželjene elektroničke pošte

Na slici 4.9 za IP adresu 72.21.7.79 poslano je 85.361 poruka neželjene elektroničke pošte tijekom 9 dana što čini 0.089% ukupne pošte koju sustav nadgleda.

Izvještaji o blokovima IP adresa su izvještaji bazirani na omjerima valjane i neželjene elektroničke pošte, sastoji se pretraživačke mape prostora IP adresa, najgoreg /24 bloka baziranog na ukupnoj neželjenoj elektroničkoj pošti, najgoreg /16 bloka baziranog na ukupnoj neželjenoj elektroničkoj pošti, najgoreg /24 i /16 bloka baziranog na omjeru valjane i neželjene elektroničke pošte.

Slika 4.10 prikazuje mapu prostora IP adresa na kojoj je za svaki blok prikazana statistika koja se sastoji od ukupnog broja elektroničke pošte, ukupnog broja prijava neželjene elektroničke pošte, broj prijava u odnosu na ukupan broj poruka, broj poslužitelja koji šalju elektroničku poštu, broj poslužitelja koji šalju neželjenu elektroničku poštu, omjer prijavljenih poslužitelja u odnosu na ukupne i prosječan broj poslanih poruka po poslužitelju.

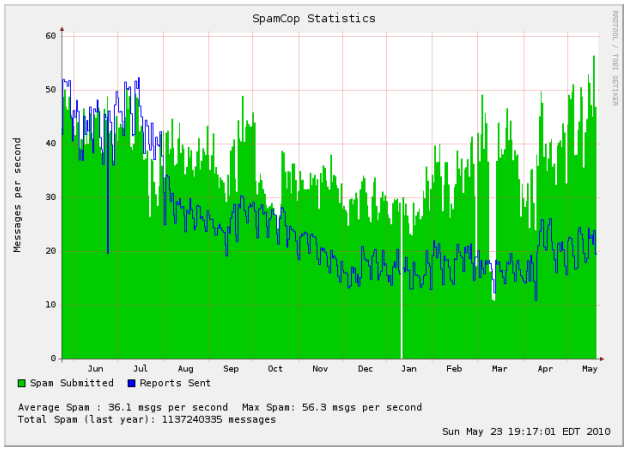


Slika 4.10. Mapa IPv4 prostora

Za svaki blok postoji detaljan prikaz za blok IP adresa u rasponu /16 i /24.

Ukupni broj poruka neželjene elektroničke pošte prikazan je grafovima na kojima se prikazuje broj poruka koje su poslane kao neželjena elektronička pošta u omjeru na sveukupni broj prijava koje šalju korisnici sustava. Ti grafovi više prikazuju Spamcopov

uzorak nego informacije o neželjenoj elektroničkoj pošti. Brojevi prikazuju mali dio ukupne neželjene elektroničke pošte. Slika 4.11 prikazuje dostupne su grafove koji prikazuju podatke u zadnja 24 sata, zadnji tjedan, zadnji mjesec i zadnjih godinu dana.



Slika 4.11. Godišnji prikaz prijava i ukupne neželjene elektroničke pošte

4.3. Project HoneyPot

Project HoneyPot je sustav koji kroz distribuiranu mrežu lažnih Web stranica sakuplja informacije o napadačima na te stranice, pošiljateljima neželjene elektroničke pošte i skupljačima adresa elektroničke pošte. Korisnici koji sudjeluju u projektu ustvari postavljaju zamke na poslužitelje kojima upravljaju.

Sustav se popunjava podacima putem posebnih adresa elektroničke koje su postavljene kao zamka na Web stranicama poslužitelja koji sudjeluje u projektu. Takve adrese elektroničke pošte su jedinstvene ne samo za određenu stranicu, već i za svakog posjetitelja. Na taj način se točno može odrediti IP adresa i vrijeme kada je napadač posjetio stranicu.

Sustav koristi jedinstvenu metriku kako bi opisao procjenu opasnosti neke IP adrese s obzirom na njenu aktivnosti. Te aktivnosti uključuju slanje neželjene elektroničke pošte, napade putem rječnika, sakupljanje adresa elektroničke pošte, slanje neželjenih komentara, držanje zloćudnih Web stranica i povredu pravila o automatiziranim programima. Broj koji opisuje razinu opasnosti je logaritamski rezultat, a ovisi o broju zabilježenih počinjenih napada. Npr. za slanje neželjene elektroničke pošte rezultat od 25 ekvivalentan je 100 poslanih poruka, rezultat 50 je 10.000 poruka, rezultat 75 je ekvivalent 1.000.000 poslanih poruka neželjene elektroničke pošte.

Na sustavu je dostupno nekoliko listi: crna lista koja sadrži podatke o sakupljačima adresa elektroničke pošte (engl. *Harvester*), lista računala koji šalju neželjenu elektroničku poštu (engl. *Spam Server*), lista napadača putem rječnika (engl. *Dictionary Attacker*) i lista pošiljatelja neželjenih komentara (engl. *Comment Spammer*).

Sakupljači adresa elektroničke pošte su programi koji na Internetu traže adrese elektroničke pošte s kojima pošiljatelji neželjene elektroničke pošte grade svoje liste. Lista sakupljača

adresa elektroničke pošte sadrži IP adresu sakupljača, ukupni broj sakupljanja i datum prvog i zadnjeg sakupljanja što je prikazano na slici 4.12.

Harvester IP	Event	Total	First	Last
200.226.134.53 | HC	Harvest	145,629	2007-10-19	2007-12-07
64.27.5.162 | HC	Harvest	100,631	2007-03-06	2008-08-14
64.233.166.136 | Se	Harvest	72,138	2005-04-21	2008-08-08
195.229.242.154 | HC	Harvest	60,531	2008-01-23	2008-03-31
64.233.178.136 | Se	Harvest	58,536	2005-04-21	2008-11-16
66.249.90.136 | Se	Harvest	51,156	2006-12-27	2008-08-14
203.144.144.164 | HC	Harvest	40,505	2006-03-22	2008-07-04
72.14.220.136 | Se	Harvest	39,429	2006-11-23	2008-12-24
165.228.133.11 | HC	Harvest	33,147	2006-07-30	2008-04-09
62.163.80.205 | H	Harvest	29,332	2007-02-06	2007-09-12
200.65.127.161 | HC	Harvest	28,880	2007-10-24	2009-06-13
208.223.208.181 | H	Harvest	27,911	2005-02-03	2008-08-14
165.228.130.12 | HC	Harvest	27,363	2005-06-01	2008-04-09
209.85.138.136 | Se	Harvest	27,033	2007-03-27	2008-12-04
72.14.252.136 | Se	Harvest	23,955	2006-11-19	2008-08-14
216.239.50.136 | HC	Harvest	22,800	2007-04-19	2009-01-10
165.228.131.12 | HC	Harvest	21,208	2005-05-10	2008-04-10
62.163.37.157 | H	Harvest	20,082	2007-03-29	2007-08-02
195.175.37.71 | HC	Harvest	18,867	2006-03-28	2007-12-14
64.34.255.239 | HC	Harvest	18,688	2007-08-18	2008-12-07

Slika 4.12. Lista sakupljača adresa elektroničke pošte

Za svaku IP adresu sakupljača postoje detaljni podaci u kojima se nalazi zemljopisna lokacija IP adrese sakupljača adresa elektroničke pošte, podatak o prvom viđenju, zadnjem viđenju, broju viđenja u ovisnosti o zamkama, broj sakupljenih adresa elektroničke pošte, ukupni broj poslanih poruka, podatci o vremenu od sakupljanja adrese elektroničke pošte do prve poslane poruke na tu adresu elektroničke pošte, procjenu opasnosti, IP adrese poslužitelja elektroničke pošte koji koriste sakupljene adrese elektroničke pošte sakupljača i podatke o programima kojima se sakupljač koristi za sakupljanje.

Na slici 4.13 prikazani su detaljni podaci jednog sakupljača adresa elektroničke pošte.

Geographic Location	Romania
Harvester First Seen	approximately 2 years, 4 months, 4 weeks ago
Harvester Last Seen	within 1 week
Harvester Sightings	8,178 visit(s) to 324 honey pot(s)
Harvester Results	96.60599999999999 messages per visit 790,042 message(s) resulting from harvests - First: approximately 2 years, 4 months, 4 weeks ago - Last: approximately 1 week ago 10,483 email address(es) harvested - First: approximately 2 years, 4 months, 4 weeks ago - Last: Wed, 18 Nov 2009 13:09:42 -0500
Time From Harvest To First Spam	**Fastest:** 3 hours, 55 mins, 26 secs **Slowest:** 1 month, 2 weeks, 2 days, 17 hours, 48 mins, 43 secs **Average:** 2 days, 11 hours, 33 mins, 28 secs **Std Dev:** 2 days, 13 hours, 32 mins, 41 secs
Threat Rating	**75** (Read More)

Associated Mail Servers
41.189.3.86 | S
58.244.204.66 | S
58.244.217.35 | S
58.244.217.36 | S
58.244.217.40 | S
58.244.217.47 | S
59.90.200.16 | S
59.151.100.220 | SD
59.175.187.36 | SD
60.172.190.178 | S
60.173.9.37 | SD
60.234.241.129 | SC
60.251.66.206 | SD
61.53.150.195 | SD
61.53.150.199 | SD
61.53.150.200 | SD

89.122.29.32's User Agent Strings
Java/1.6.0_04
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727; MEGAUPLOAD 2.0)
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC1; .NET CLR 2.0.50727)

Slika 4.13. Detaljan prikaz sakupljača adresa elektroničke pošte

IP adresa sakupljača prikazanog na slici 4.13 adresa elektroničke pošte je 89.122.29.32 i dolazi iz Rumunjske. Kroz 324 postavljene zamke sakupljač je ulovljen 8178 puta. Sakupljač je prvu adresu prikupio otprilike prije 2 godine i 4 mjeseca dok je zadnji put viđen otprilike prije tjedan dana. Najbrže vrijeme otkad je sakupio adresu elektroničke pošte do kad je neželjena pošta stigla na nju je 3 sata 55 minuta, dok je najduže trebalo 1 mjesec i 2 tjedna. U prosjeku vrijeme od sakupljanja adrese elektroničke pošte do kad neželjena pošta na nju stigne je 2 dana i 11 sati. Procjena opasnosti ovog sakupljača je 75. Tijekom svoga rada sakupljač je sakupio 10.483 adresa elektroničke pošte na koje je pristiglo 790.042 poruke neželjene elektroničke pošte. S desne strane vidimo IP adrese s kojih je pristigla neželjena elektronička pošta, mahom iz Kine.

Računala koja šalju neželjenu elektroničku poštu kontoliraju pošiljatelji neželjene elektroničke pošte i u većini slučajeva ne pripadaju njima, već su dio mreže kompromitiranih računala. Ta lista sadrži IP adresu računala, ukupni broj poslanih poruka neželjene elektroničke pošte, kao i datum prvog i zadnjeg slanja što je prikazano na slici 4.14.

Spam Server IP	Event	Total	First	Last
94.41.90.174 | SC	Bad Event	5	2009-10-30	2010-05-17
189.56.100.42 | SDC	Bad Event	104	2008-05-15	2010-05-17
122.169.210.164 | SC	Bad Event	5	2009-04-27	2010-05-17
94.125.162.113 | SC	Bad Event	6	2010-04-29	2010-05-17
222.255.239.135 | SDC	Bad Event	38	2010-05-13	2010-05-17
91.193.35.199 | SDC	Bad Event	45	2009-06-17	2010-05-17
212.178.17.45 | SC	Bad Event	16	2009-02-17	2010-05-17
190.144.53.138 | SDC	Bad Event	45	2008-04-15	2010-05-17
82.193.140.165 | SDC	Bad Event	2,312	2009-01-20	2010-05-17
88.245.1.124 | SC	Bad Event	13	2007-12-29	2010-05-17
92.47.36.52 | SC	Bad Event	5	2008-11-05	2010-05-17
122.156.184.80 | SC	Bad Event	14	2008-12-26	2010-05-17
196.12.243.181 | SDC	Bad Event	583	2009-01-25	2010-05-17
193.231.17.37 | SDC	Bad Event	453	2007-08-06	2010-05-17
85.105.141.39 | SC	Bad Event	20	2006-10-10	2010-05-17
85.17.254.135 | SDC	Bad Event	159	2009-04-05	2010-05-17
82.207.66.114 | SC	Bad Event	6	2007-12-21	2010-05-17
117.102.91.6 | SDC	Bad Event	148	2009-06-11	2010-05-17
222.124.192.156 | SDC	Bad Event	330	2009-06-26	2010-05-17
222.73.219.207 | SDC	Bad Event	37	2010-04-26	2010-05-17

Slika 4.14. Lista računala koji šalju neželjenu elektroničku poštu

Za svaku IP adresu postoje detaljni podaci prikazani na slici 4.15 u kojima se nalazi zamljopisna lokacija računala koje šalje neželjenu elektroničku poštu, procjena opasnosti, datum prvog i zadnjeg slanja neželjene elektroničke pošte, kao i ukupan broj poslanih poruka. Također je dostupan popis sakupljača adresa elektroničke pošte vezanih uz IP adresu računala, IP adrese računala koje se nalaze na istom sustavu kao IP adresa koja se provjerava i primjer poslane poruke neželjene elektroničke pošte.

Geographic Location	Morocco
Threat Rating	10 (Read More)
First Received From	approximately 1 week ago
Last Received From	within 1 week
Number Received	6 email(s) sent from this IP

Associated Harvesters
207.150.196.52 | HS
75.125.52.146 | H
216.40.220.34 | H
74.86.249.98 | H
74.53.249.34 | H

IPs In The Neighborhood
41.140.0.155 | SD
41.140.0.156 | SD
41.140.0.171
41.140.0.178 | SD
41.140.0.189
41.140.0.198
41.140.0.202 | D
41.140.0.207
41.140.0.208 | SD
41.140.0.229

Example Messages Sent From 41.140.1.110
From: "Herrell Jerimiah" <scott@scott4realestate.com>
Subject: thanks
From: "Garafola Nawkishu" <resumes@micro.ti.com>
Subject: very much
From: "Grimsley Jarita" <rhsre@br.ibm.com>
Subject: No description
From: "Breeding Nadeana" <tnemyren@cablespeed.com>
Subject: waiting for reply
From: "Bridgeman Wissam" <kristin@aqueouschurch.com>
Subject: waiting for an answer

Slika 4.15. Detaljan opis računala koje šalje neželjenu elektroničku poštu

IP adresa pošiljatelja neželjene elektroničke pošte prikazanog na slici 4.15 iznosi 41.140.1.110 i dolazi iz Maroka. Prva poruka neželjene elektroničke pošte poslana je prije

jednog tjedna, a pošiljatelj je tijekom tjedna poslao 6 poruka neželjene elektroničke pošte. Za pošiljatelja neželjene elektroničke pošte prikazani su i sakupljači adresa elektroničke pošte sa kojih je pošiljatelj pribavio adrese elektroničke pošte. Procjena opasnosti ovog pošiljatelja neželjene elektroničke pošte je 10.

Napad korištenjem rječnika je metoda kojom se služe pošiljatelji neželjene elektroničke pošte kako bi pronašli nove adrese. Korištenjem rječnika se stvori niz novih adresa, na koje se zatim šalju poruke elektroničke pošte i provjerava da li su dostavljene. Na slici 4.16 prikazana je lista koja sadrži IP adresu napadača, ukupan broj napada, kao i datum prvog i zadnjeg napada.

Dictionary Attacker IP	Event	Total	First	Last
189.56.100.42 | SDC	Bad Event	104	2008-05-15	2010-05-17
222.255.239.135 | SDC	Bad Event	38	2010-05-13	2010-05-17
91.193.35.199 | SDC	Bad Event	45	2009-06-17	2010-05-17
190.144.53.138 | SDC	Bad Event	45	2008-04-15	2010-05-17
82.193.140.165 | SDC	Bad Event	2,312	2009-01-20	2010-05-17
91.121.178.43 | DC	Bad Event	4	2010-05-03	2010-05-17
196.12.243.181 | SDC	Bad Event	583	2009-01-25	2010-05-17
193.231.17.37 | SDC	Bad Event	453	2007-08-06	2010-05-17
94.228.213.107 | DC	Bad Event	5	2010-05-14	2010-05-17
85.17.254.135 | SDC	Bad Event	159	2009-04-05	2010-05-17
117.102.91.6 | SDC	Bad Event	148	2009-06-11	2010-05-17
222.124.192.156 | SDC	Bad Event	330	2009-06-26	2010-05-17
222.73.219.207 | SDC	Bad Event	37	2010-04-26	2010-05-17
220.178.41.50 | SDC	Bad Event	30	2010-04-28	2010-05-17
81.19.34.130 | SDC	Bad Event	65	2005-09-20	2010-05-17
220.189.227.2 | SDC	Bad Event	863	2008-12-05	2010-05-17
91.194.80.1 | SDC	Bad Event	314	2008-01-23	2010-05-17
8.9.209.2 | SDC	Bad Event	657	2009-06-27	2010-05-17
24.151.223.251 | DC	Bad Event	140	2009-11-04	2010-05-17
87.205.230.63 | SDC	Bad Event	22	2008-08-29	2010-05-17

Slika 4.16. Lista IP adresa napadača korištenjem rječnika

Za svaku IP adresu postoje detaljni podaci prikazani na slici 4.17 u kojima se nalazi zemljopisna lokacija računala napadača korištenjem rječnika, procjena opasnosti, ukupan broj napada, datum prvog i zadnjeg zabilježenog napada. Dostupan je i popis IP adresa računala koje se nalaze na istom sustavu kao IP adresa koja se provjerava, kao i primjer korisničkih imena koje napadač koristi.

Geographic Location	Indonesia
Threat Rating	16 (Read More)
Dictionary Attacks	16 email(s) sent from this IP
First Received From	approximately 1 week ago
Last Received From	within 1 week

IPs In The Neighborhood	Example User Names Used By 125.165.101.218
125.165.100.250	User-name: dugat
125.165.101.4 | SD	User-name: fullbright
125.165.101.5 | S	User-name: robertsfaw
125.165.101.14	User-name: uvvz
125.165.101.15 | D	User-name: vapgf
125.165.101.29 | D	User-name: vgbq
125.165.101.31 | S	User-name: vvz
125.165.101.37	User-name: wff
125.165.101.45 | SD	User-name: xpj
125.165.101.47 | S	User-name: zzvalq
125.165.101.48	User-name: jonbcorin
125.165.101.52	User-name: jonniefullbright
125.165.101.55 | S	User-name: regenabdugat
125.165.101.56	User-name: simonebgarmire
	User-name: rupertsauna
	User-name: tanjahhoglan

Slika 4.17. Detaljan opis napadača putem rječnika

IP adresa napadača korištenjem rječnika prikazanog na slici 4.17 je 125.165.101.218 i nalazi se u Indoneziji. Procjena opasnosti ovog napadača je 10. Prvi napad korištenjem rječnika zabilježen je prije tjedan dana dok je napad izveo 16 puta. IP adrese računala koje se nalaze na istoj mreži kao i napadač prikazuju druge napadače korištenjem riječnika kao i pošiljatelje neželjene elektroničke pošte. Da danu IP adresu prikazana su i korisnička imena kojim se napadač služi prilikom napada, npr. *dugat, fullbright, robertsfaw*.

Vrlo često se događa da se s jedne IP adrese izvodi više različitih napada. Sakupljači adresa elektroničke pošte uglavnom su povezani sa pošiljateljima neželjene elektroničke pošte, a ponekad i sa napadima korištenjem rječnika, dok se slanje neželjenih komentara uglavnom vrši samostalno. Sve akcije koje dolaze s određene IP adrese prikazane su u detaljnom opisu.

Pošiljatelji neželjenih komentara šalju poruke na forume i blogove. Te poruke sadrže poveznice na komercijalne stranice. Dodatni cilj je i povećati rangiranje na Internetskim tražilicama budući neke rade na principu povećanja ranga ovisno o broju posjeta. Slika 4.18 prikazuje listu koja sadrži zemljopisnu lokaciju pošiljatelja, ukupan broj poslanih komentara, datum prvog i posljednjeg slanja neželjenog komentara.

Comment Spammer IP	Event	Total	First	Last
212.235.107.5 | C	Bad Event	13	2010-05-17	2010-05-17
212.92.244.146 | C	Bad Event	35	2010-05-15	2010-05-17
94.142.131.20 | C	Bad Event	8,609	2009-10-08	2010-05-17
195.191.54.217 | C	Bad Event	66	2010-05-15	2010-05-17
220.136.24.247 | C	Bad Event	3	2010-05-14	2010-05-17
217.23.8.141 | C	Bad Event	75	2010-05-15	2010-05-17
94.102.49.83 | C	Bad Event	1,760	2010-05-15	2010-05-17
195.191.54.212 | C	Bad Event	50	2010-05-15	2010-05-17
195.191.54.220 | C	Bad Event	57	2010-05-15	2010-05-17
213.5.71.85 | C	Bad Event	20	2010-05-17	2010-05-17
94.142.130.20 | C	Bad Event	1	2010-05-17	2010-05-17
94.142.131.25 | C	Bad Event	8,680	2009-10-08	2010-05-17
195.191.54.213 | C	Bad Event	56	2010-05-15	2010-05-17
195.191.54.219 | C	Bad Event	46	2010-05-15	2010-05-17
94.142.131.23 | C	Bad Event	8,495	2009-10-08	2010-05-17
212.235.107.73 | C	Bad Event	9	2010-05-17	2010-05-17
193.104.110.10 | C	Bad Event	27	2010-05-15	2010-05-17

Slika 4.18. Lista pošiljatelja neželjenih komentara

Za svaku IP adresu postoje detaljni podaci na kojem se nalazi zemljopisna lokacija pošiljatelja, procjena opasnosti, ukupan broj poslanih neželjenih komentara, datum prvog i zadnjeg slanja neželjenog komentara. Također je dostupan popis IP adresa računala koje se nalaze na istom sustavu kao IP adresa koja se provjerava i primjeri poslanih komentara, koji uključuju domenu, poveznicu i ključnu riječ vezanu uz komentar. Može se saznati i program kojim se pošiljatelj služi što je vidljivo sa slike 4.19.

Geographic Location	Netherlands
Spider First Seen	approximately 1 week ago
Spider Last Seen	within 1 week
Spider Sightings	36 visit(s)
User-Agents	seen with 21 user-agent(s)
Threat Rating	33 (Read More)
First Post On	approximately 1 week ago
Last Post On	within 1 week
Form Posts	126 web post submission(s) sent from this IP

IPs In The Neighborhood
217.23.7.173 | S
217.23.7.174
217.23.7.186
217.23.7.208
217.23.8.10
217.23.8.14
217.23.8.40
217.23.8.74
217.23.8.206 | S
217.23.8.251 | S
217.23.9.37
217.23.9.38
217.23.9.39

Sample Spam URLs & Keywords Posted From 217.23.8.141
Domain: 1998jaycofsseagle.blockgooded.in **URL**: http://1998jaycofsseagle.blockgooded.in/ **Keywords**: 1998 jayco fss eagle
Domain: weiderhomegymexercisechart.minegooded.in **URL**: http://weiderhomegymexercisechart.minegooded.in/ **Keywords**: weider home gym exercise chart
Domain: spankherlittleass.minegooded.in **URL**: http://spankherlittleass.minegooded.in/ **Keywords**: spank her little ass
Domain: 67nminpoundsperfoot.doorgooded.in **URL**: http://67nminpoundsperfoot.doorgooded.in/ **Keywords**: 67 nm in pounds per foot
Domain: 5090ammunition.wellgooded.in **URL**: http://5090ammunition.wellgooded.in/ **Keywords**: 50 90ammunition
Domain: articulosparapastaflexible.withgooded.in **URL**: http://articulosparapastaflexible.withgooded.in/ **Keywords**: articulos para pasta flexible
Domain: bideosdemujeresteniendobebesenvivo.withgooded.in **URL**: http://bideosdemujeresteniendobebesenvivo.withgooded.in/ **Keywords**: bideos de mujeres teniendo bebes en vivo

Slika 4.19. Detaljan prikaz pošiljatelja neželjenih komentara

IP adresa pošiljatelja neželjenih komentara prikazanog na slici 4.19 je 217.23.8.141 i nalazi se u Nizozemskoj. Procjena opasnosti ovog pošiljatelja neželjenih komentara je 33, viđen je prvi puta prije tjedan dana dok je za to vrijeme poslao 126 neželjenih komentara. S desne strane slike prikazani su primjeri adrese Web stranice i ključnih riječi koji se koriste u neželjenom komentaru, npr. *http://5090ammunition.wellgooded.in*.

Na sustavu je dostupna Http:BL usluga temeljena na *DNS* upitima preko koje poslužitelji elektroničke pošte mogu efikasno provjeriti klijenta koji se na njih spaja. Korištenje Http:BL usluge je slično korištenju crnih lista, no za razliku od većine crnih listi nije ograničena samo na promet elektroničke pošte, nego i za ukupan promet vezan uz Web stranicu. Na taj način, administratori Web stranice mogu odlučiti koji je promet dopušten na njihovim stranicama. Usluga sadrži podatke o IP adresama sakupljača adresa elektroničke pošte, pošiljatelja neželjenih komentara i raznih automatiziranih programa koji posjećuju Web stranicu. Usluga ne sadrži podatke o IP adresama računala koja šalju neželjenu elektroničku poštu, razlog tomu je što iz administratori Project Honeypota smatraju da se na Internetu mogu pronaći bolje i potpunije liste, npr. Spamhaus, SpamCop. Svaki korisnik koji želi koristiti uslugu mora zatražiti vlastiti ključ.

Upiti na Http:BL imaju određeni format:

abcdefghijl .2.1.9.127.dnsbl.httpbl.org
[pristupni ključ][IP adresa reverznih okteta][domena crne liste]

U *DNS* odgovoru nalaze se detalji o aktivnostima provjeravane IP adrese. Odgovor vraća rezultat u obliku IP adrese sa tri ili četiri okteta, a sadržava informacije o posjetitelju Web stranice. Razlog tome je taj što se želi ponuditi fleksibilnost u načinu na koji se tretiraju posjetitelji, za razliku od samo crne ili bijele liste. Na taj način možemo poduzeti drugačije mjere ovisno o tome da li se radi o sakupljaču adresa elektroničke pošte ili pošiljatelju neželjenih komentara.
Odgovor na upit dan je na primjeru: 127.3.5.1
Svaki oktet, osim prvog ima značenje. Prvi oktet je uvijek predefiniran na 127 i nema veze sa posjetiteljem Web stranice. Ukoliko je prvi oktet različit od 127 znači da je došlo do greške, i da vjerojatno upit nije pravilno definiran.
Drugi oktet predstavlja broj dana od zadnje aktivnosti. U gornjem primjeru, to je 3, što znači da je ispitivana IP adresa viđena na *Project Honeypot* mreži zadnji put prije tri dana. Ta vrijednost ima raspon od 0 – 255 i pomaže u procjeni starosti informacije i da li se na nju može osloniti.

Treći oktet predstavlja procjenu opasnosti. Ocjena je dodjeljena interno, a ovisi o raznim faktorima, npr. broj posjeta zamkama, napravljenoj šteti (broj sakupljenih adresa elektroničke pošte, broj poslanih neželjenih komentara). Ocjena ima raspon od 0 – 255, 0 predstavlja nikakvu dok 255 ekstremnu opasnost.

Četvrti oktet predstavlja tip posjetitelja. Definirani tipovi uključuju: pretraživača, sumnjive, sakupljače, pošiljatelje neželjenih komentara. Budući da posjetitelj može biti sastavljen od više tipova, oktet je reprezentiran kao zbroj određenih vrijednosti ovisno o tipu prikazan u tablici 4.5.

Tablica 4.5. Vrijednosti tipova posjetitelja

Vrijednost	Značenje
0	Pretraživač
1	Sumnjiv
2	Sakupljač adresa elektroničke pošte
4	Pošiljatelj neželjenih komentara
8, 16, 32, 64, 128	Rezervirano za buduće korištenje

Primjer upita nad Http:BL uslugom i odgovara dan je u nastavku. Kao primjer je korištena IP adresa sa slike 4.13.

upit: `korisnik:~$ host etlfsokkkruz.32.29.122.89.dnsbl.httpbl.org`

odgovor:
```
etlfsokkkruz.32.29.122.89.dnsbl.httpbl.org has address
127.54.76.3
```

Ključ za korištenje usluge dobije se registracijom, u ovom slučaju je *etlfsokkkruz*. Upit se predaje na način *etlfsokkkruz.32.29.122.89.dnsbl.httpbl.org*. Odgovor usluge je 127.49.76.3. Prvi oktet je 127 što znači da je sve prošlo u redu, drugi oktet označava da je aktivnost dane IP adrese zadnji put viđena prije 49 dana. Procjena opasnosti, koja se nalazi u trećem oktetu je 76, dok četvrti oktet iznosi 3 što označava sumnjivo ponašanje i sakupljača adresa.

4.4. SORBS

SORBS je besplatni servis koji se bavi blokiranjem neželjene elektroničke pošte i otvorenih posredničkih poslužitelja (engl. *Spam and Open Relay Blocking System*). Temelji se na crnim listama koje se popunjavaju korištenjem zamki.

Putem servisa je dostupno više crnih listi, koje se koriste podešavanjem poslužitelja elektroničke pošte, a one su:

- Lista korisnika i poslužitelja s dinamičkim IP adresama (engl. *Dynamic User and Host List – DUHL*) je lista blokova IP adresa kojima pružatelj Internetskih usluga dodijeljuju adrese dinamički, što u konačnici otežava identifikaciju izvora neželjene elektroničke pošte.
- Lista otvorenih i posredničkih poslužitelja
- Lista "zombie" računala i mreža za koje se smatra da nisu pod potpunom kontrolom svojih pravih vlasnika.

Crne liste su dostupne putem više zona koje su prikazane u tablici 4.6:

Tablica 4.6. Lista SORBS zona

dnsbl.sorbs.net	grupna zona, sadrži sve niže popisane zone, osim spam.dnsbl.sorbs.net
http.dnsbl.sorbs.net	lista otvorenih HTTP posredničkih poslužitelja
socks.dnsbl.sorbs.net	lista otvorenih SOCKS posredničkih poslužitelja
misc.dnsbl.sorbs.net	lista otvorenih posredničkih poslužitelja koji nisu pobrojani u HTTP i SOCKS listi
smtp.dnsbl.sorbs.net	lista otvorenih SMTP posredničkih poslužitelja
web.dnsbl.sorbs.net	lista koji su kompromitiranih Internet (WWW) poslužitelja
new.spam.dnsbl.sorbs.net	lista poslužitelja koji su poslali neželjenu elektroničku poštu u proteklih 48 sati
recent.spam..dnsbl.sorbs.net	lista poslužitelja koji su poslali neželjenu elektroničku poštu u zadnjih 28 dana
old.spam.dnsbl.sorbs.net	lista poslužitelja koji su poslali neželjenu elektroničku poštu tijekom prošle godine
spam.dnsbl.sorbs.net	lista poslužitelja koji šalju neželjenu elektroničku poštu i ne šalju zahtjeve za micanjem iz liste
escalations.dnsbl.sorbs.net	lista koja sadrži raspon IP adresa pružatelja Internet usluga koji podržavaju slanje neželjene elektroničke pošte
block.dnsbl.sorbs.net	lista poslužitelja koji zahtijevaju da ih ne testira putem usluge
zombie.dnsbl.sorbs.net	lista mreža kompromitiranih računala
dul.dnsbl.sorbs.net	lista raspona dinamičkih IP adresa
rhsbl.sorbs.net	grupna zona, sadrži sve RHS zone
badconf.rhsbl.sorbs.net	lista domena kojima A ili MX zapis ukazuje na nepostojeći adresni prostor
nomail.rhsbl.sorbs.net	lista imena domena za koje su njihovi vlasnici garantiraju da nesmije pristizati nikakva elektronička pošta

Usluga vraća kodove u obliku 127.0.0.X da bi ukazala na listu iz koje je testirani podatak izvučen. Ukoliko se koriste grupne zone, povratni kod vraća odgovore od svake zone u kojima se testirani zapis nalazi.

Povratni kodovi nalaze se u tablici 4.7:

Tablica 4.7. Sorbs povratni kodovi

http.dnsbl.sorbs.net	127.0.0.2
socks.dnsbl.sorbs.net	127.0.0.3
misc.dnsbl.sorbs.net	127.0.0.4
smtp.dnsbl.sorbs.net	127.0.0.5
new.spam.dnsbl.sorbs.net	127.0.0.6
recent.spam.dnsbl.sorbs.net	127.0.0.6
old.spam.dnsbl.sorbs.net	127.0.0.6
spam.dnsbl.sorbs.net	127.0.0.6
escalations.dnsbl.sorbs.net	127.0.0.6
web.dnsbl.sorbs.net	127.0.0.7
block.dnsbl.sorbs.net	127.0.0.8
zombie.dnsbl.sorbs.net	127.0.0.9
dul.dnsbl.sorbs.net	127.0.0.10
badconf.rhsbl.sorbs.net	127.0.0.11
nomail.rhsbl.sorbs.net	127.0.0.12

4.5. APEWS

APEWS (Anonymous Postmaster Early Warning System) je usluga koja sadrži listu raspona IP adresa (L2 lista), i listu imena domena (L1 lista) koji pripadaju određenom pružatelju internetskih usluga za koje se smatra da pružaju usluge pošiljateljima neželjene elektroničke pošte, ili ne sprečavaju njihovu zloupotrebu prema drugim mrežnim resursima.

Uslugu je utemeljila grupa koja je uvidjela da je SPEWS (Spam Prevention Early Warning System) postao neaktivan. Izgled i način djelovanja APEWS usluge identičan je SPEWS usluzi, no APEWS koristi jednu listu više. Kontroverze oko samog korištenja usluge postoje budući da liste sadrže imena pružatelja internetskih usluga. Grupa koja održava uslugu je anonimna, uglavnom da bi se izbjegle tužbe pošiljatelja neželjene elektroničke pošte. Neki korisnici smatraju da blokiranje pružatelja internetskih usluga nije rješenje, no time ih se pokušava prisiliti da poprave način na koji rade jer u suprotnom gube velik dio korisnika.

Kao što je navedeno ranije *APEWS* usluga se sastoji od 2 liste:

- L1 lista – lista domena koja su u vlasništvu pošiljatelja neželjene elektroničke pošte ili ljudi koji im pružaju usluge. Ako poznati pošiljatelj neželjene elektroničke pošte kupi novu domenu, a još nije počeo sa slanjem, postoji šansa da se ta domena nađe u listi. Treba obratiti pozornost na činjenicu da se određena poruka može odbiti

koristeći L1 listu, dok kroz L2 prolazi. Zato se preporuča korištenje obje liste. To je i najveća razlika u odnosu na SPEWS usluge, gdje su veze bile hijerarhijske.

- L2 lista – lista IP adresa i blokova IP adresa poznatih pošiljatelja neželjene elektroničke pošte, i organizacija koje im pružaju Internet usluge. Ova lista je "nepažljiva", tj. može se desiti da lista sadrži IP adrese korisnika koje ne šalju neželjenu elektroničku poštu no dio su bloka blokiranih IP adresa, ali ju ipak mogu koristiti manji pružatelji internetskih usluga koji žele striktnije blokiranje ili filtriranje.

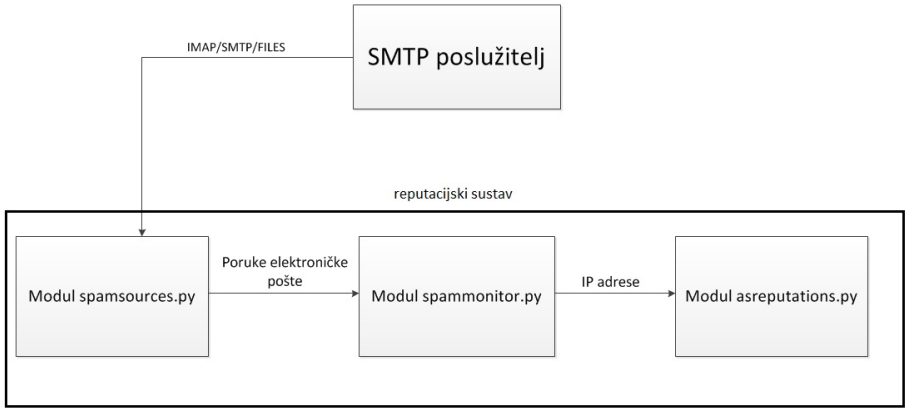
Za korištenje usluge koristi se *DNS* upit tako da se uzme IP adresa, ili ime poslužitelja s kojeg je pristigla poruka elektroničke pošte i provjeri da li se nalazi u nekoj od listi. Ukoliko je IP adresa ili ime poslužitelja pronađena u listi, poslužitelj može poruku odbaciti, ili ju označiti za daljnje provjeravanje.

Provjera IP adrese ili domene moguća je na dva načina:

- Za male tvrtke – za domene: provjera tipa ime-domene.l1.apews.org. U slučaju da se domena nalazi u listi, vratiti će se vrijednost [127.0.0.2]. Za IP adrese koristi se provjera tipa IP-adresa.l2.apews.org. U slučaju da se IP adresa nalazi u listi, vratiti će se vrijednost [127.0.0.2].
- za velike tvrtke: mogu se preuzeti obje liste u tekstualnom obliku i koristiti za provjeru na lokalnom poslužitelju. L1 lista sadrži samo imena domena, dok L2 lista sadrži IP adrese.

5. Reputacijski sustav

Cilj ovog rada bio je izgraditi reputacijski sustav za ocjenjivanje nekog autonomnog sustava. Sustav je napravljen u jeziku *Python*, a sastoji se od tri modula međusobno povezanih prikazanih na slici 5.1.



Slika 5.1. Shema reputacijskog sustava

Modul *spamsources* služi za prikupljanje poruka elektroničke pošte s raznih izvora. Trenutno je modul u mogućnosti primati poruke s dva različita izvora, direktorija na lokalnom disku i sandučića elektroničke pošte putem protokola *IMAP*. Modul prosljeđuje prikupljene poruke elektroničke pošte modulu *spammonitor*.

Modul *spammonitor* je namjenjen traženju IP adresa u zaglavlju poruke elektroničke pošte. Modul prima poruke elektroničke pošte od modula *spamsources* i parsira zaglavlja poruke iz kojih se uzimaju polja Received budući da ona sadrže IP adrese računala po kojima je poruka putovala. Upotrebom regularnog izraza prilagođenog na uzorak IP adrese sakupljaju se IP adrese računala kroz koje je poruka prošla. Sve IP adrese prosljeđuju se modulu *asreputations*.

Modul *asreputations* je modul koji je zaslužan za izračun reputacije nekog sustava. On sadrži bazu kojom se iz IP adrese pronalazi broj autonomnog sustava. Također i sadrži bazu koja za svaku pristiglu IP adresu ima pridruženu vremensku oznaku pomoću koje se kasnije izračunava reputacija nekog autonomnog sustava.

Reputacija nekog sustava računa se svakih sat vremena, a ovisi o dva faktora. Prvi faktor je trenutna reputacija sustava, tj. reputacija koja je izračunata za prethodni sat. Drugi faktor je prag koji se izračunava za trenutni sat, a ovisi o broju pristigle neželjene elektroničke pošte. Važno je napomenuti da veća reputacija zapravo označava sustav s kojeg pristiže više neželjene elektroničke pošte. Inicijalna reputacija svakog novog sustava je 1, tj. ideja je sumnjati malo u svaki sustav, a dopustiti mu mogućnost da dokaže svoju valjanost tijekom vremena. Pri izračunu reputacije moguća su tri ishoda: povećanje reputacije, ostanak iste reputacije i smanjenje reputacije. Povećanje reputacije je trenutno, tj. ako sustav prođe prag određen u tablici 5.1 reputacija mu se diže na dani nivo. Ako je nova reputacija u istom rangu kao i trenutna, ona ostaje ista. Smanjivanje reputacije nije trenutno već se izvodi padajućom eksponencijalnom funkcijom, tako da ako sa sustava počinje

pristizati manje neželjene elektroničke pošte reputacija će se smanjivati na početku polagano, a ako se takvo ponašanje nastavi reputacija pada sve brže.

Tablica 5.1. Pragovi reputacije autonomnih sustava

Broj poruka u jednom satu	Rang
Do 9	1 - slab
Od 10 do 49	2 - umjeren
Od 50 do 199	3 - jak
Od 201	4 - ekstreman

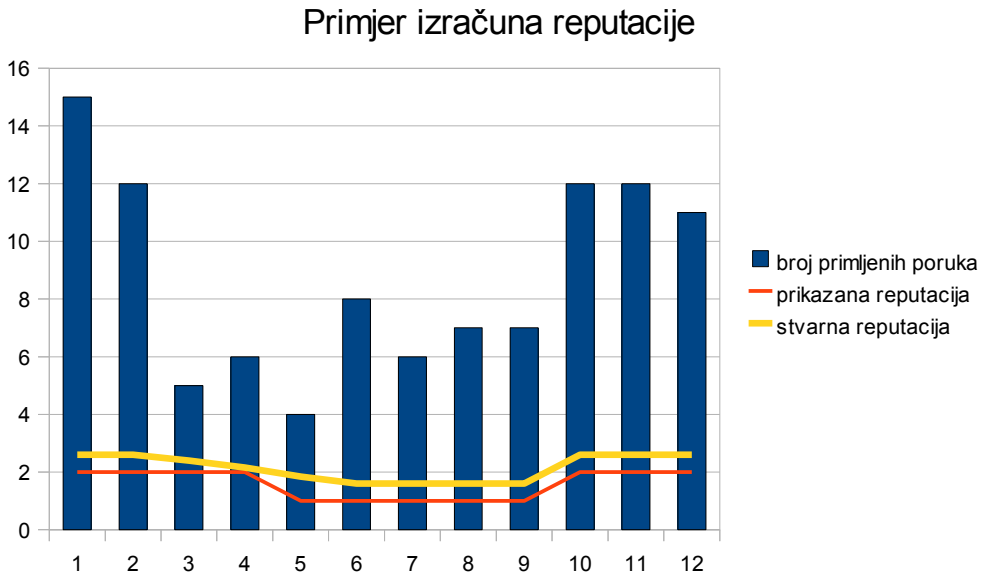
Formula za izračunavanje reputacije za određeni sat n je sljedeća (R – reputacija, r – rang):

Ako je prema broju primljene neželjene elektroničke pošte izračunati rang jednak reputaciji u prethodnom satu: $R_n = R_{n-1}$

Ako je prema broju primljene neželjene elektroničke pošte izračunati rang veći od onog u prethodnom satu $R_n = r$

Ako je prema broju primljene neželjene elektroničke pošte izračunati rang manji od onog u prethodnom satu $R_n = R_{n-1} - e^{-(R_n - r)}$

Da bi dopustili sustavima polagano padanje reputacije pragovi se zapravo izračunavaju na sljedeći način: prag 1 ima ekvivalent 1.6 u bazi, prag 2 ima 2.6, prag 3 ima 3.6, a prag 4 ima 4.6. Primjer izračuna reputacije prikazan je na slici 5.2.



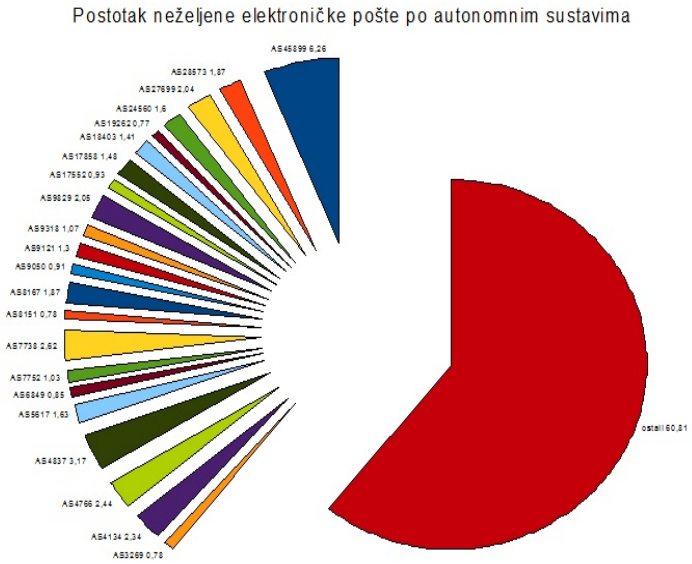
Slika 5.2. Primjer izračuna reputacije za 12 sati

Izvor podataka koji je služio za prikaz jesu poruke neželjene elektroničke pošte koje su stigle na FER poslužitelj elektroničke pošte u razdoblju od 15. srpnja 2009. godine do 15. prosinca 2009. Neki statistički podaci prikazani su u tablici 5.2.

Tablica 5.2. Osnovna statistika

Broj primljenih poruka neželjene elektroničke pošte	263452
Broj autonomnih sustava	6505
Autonomni sustav s najviše poslane pošte	AS14899
Najviše primljenih poruka u jednom danu	417 (AS14899)

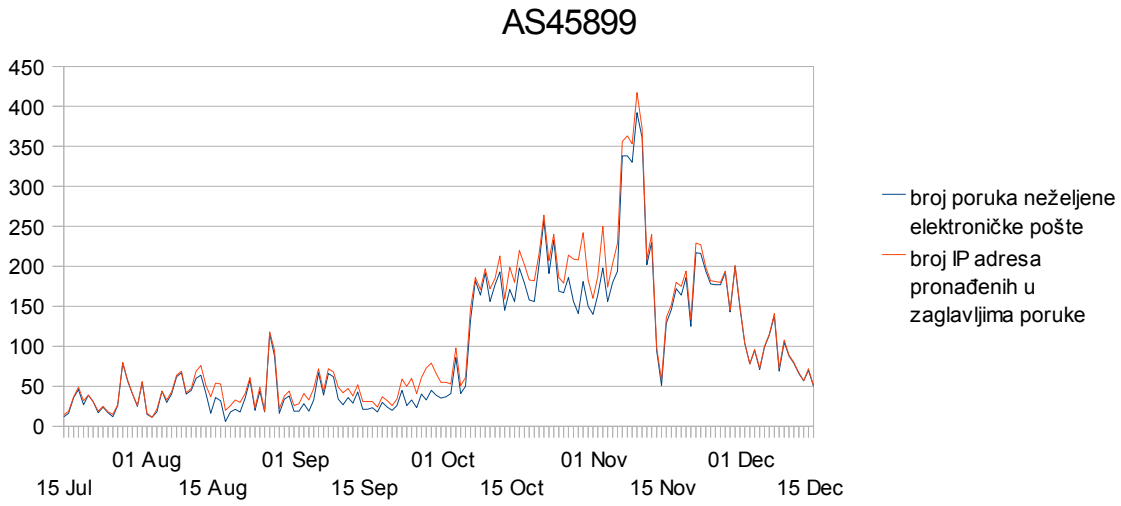
Od sveukupnog broja autonomnih sustava za potrebe statistike uzeto je njih 22, tj. oni sustavi s kojih je pristiglo 2000 i više poruka neželjene elektroničke pošte. Na slici 5.3 prikazana je statistika tih autonomnih sustava u promatranom razdoblju.



Slika 5.3. Postotak neželjene elektroničke pošte po autonomnim sustavima

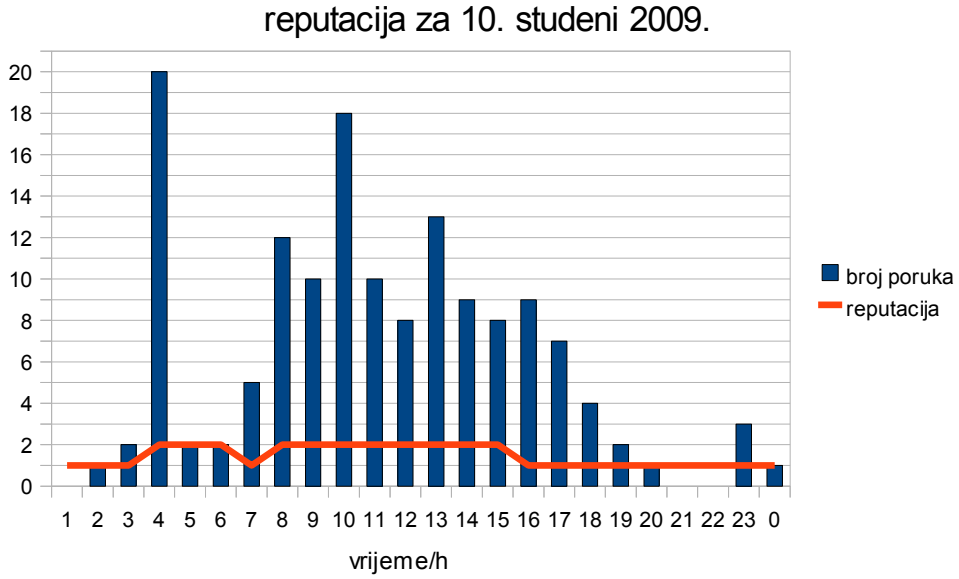
Statistika za sustave je generirana odvojeno od reputacijskog sustava posebnim modulom u jeziku *python*. Modul je uključen u repozitoriju. Za primjer prikaza izračuna reputacije birani su nasumični dani, no uzimali su se oni u kojima je bio povećan priljev neželjene elektroničke pošte da bi reputacijska funkcija bila čim bolje izražena. Kao što će biti prikazano detaljno statistikom, autonomni sustavi imaju tendenciju jednolikog ponašanja, tj. u vremenu im se uzorak slanja neželjene elektoničke pošte sporo mijenja. Uzevši tu činjenicu u obzir, izgrađeni reputacijski sustav je sposoban u realnom vremenu pružiti korisniku korisne informacije o ponašanju određenog autonomnog sustava koji tako može vrlo brzo reagirati čim se pojavi neželjena elektronička pošta. U nastavku su prikazane statistike za 22 autonomna sustava, njihova imena, broj poruka koje su izvorište u danom autonomnom sustavu, broj IP adresa koje su se pojavile u porukama a pripadaju danom sustavu, dok je na grafovima prikazan ukupan broj pronađenih IP adresa u porukama u vremenu od 15 svibnja 2009. godine do 15. prosinca 2009. godine, i reputacija danog sustava za određeni dan.

Autonomni sustav s kojeg je pristiglo najviše neželjene pošte u danom razdoblju je *VNPT Corp 57 Huynh Thuc Khang str, Dong Da Dist, Ha Noi* lociran u Vijetnamu, broj autnomnog sustava mu je 45899. Od ukupnog broja poruka neželjene elektroničke pošte, s ovog autonomnog sustava stiglo je 14.799 poruka. Kako reputacijski sustav radi na principu kažnjavanja svih autonomnih sustava na putu poruke elektroničke pošte, broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 16.482, tj. 6,26% ukupnog obujma. Na slici 5.4 prikazana je statistika za autonomni sustav 45899.



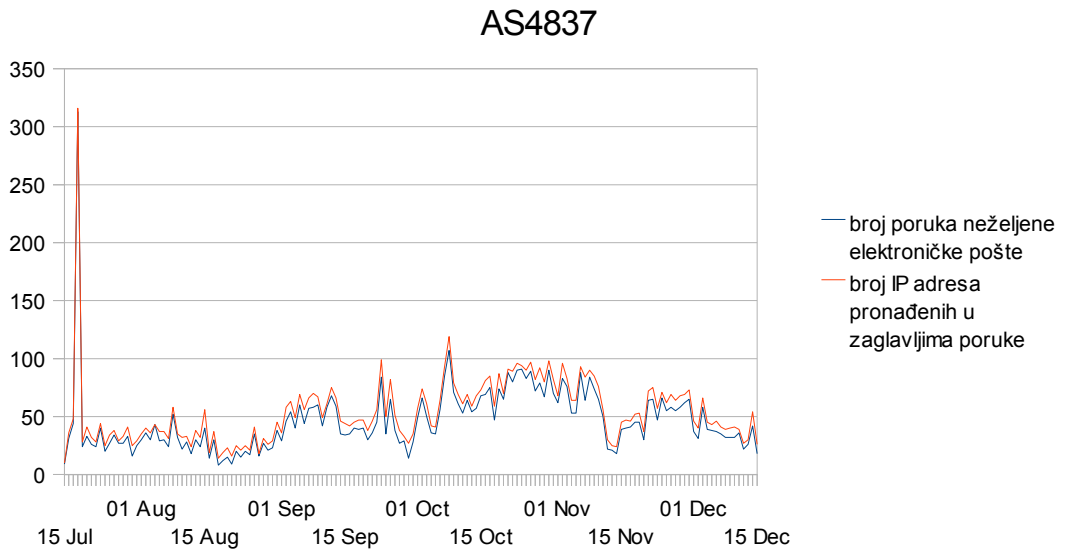
Slika 5.4. Statistika za autonomni sustav 45899

Reputacija sustava za dan 10. studeni 2009. prikazana je na slici 5.5.



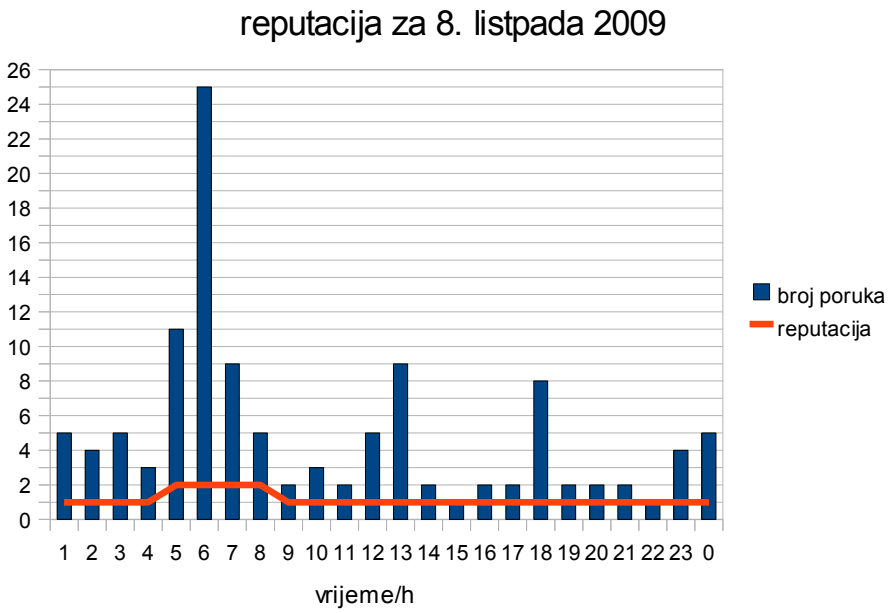
Slika 5.5. Prikaz reputacije sustava

Drugi autonomni sustav po broju poslane neželjene elektroničke pošte je *China169-Backbone* iz Kine, broj autonomnog sustava mu je 4837. S ovog je sustava u promatranom vremenu pristiglo 7174 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 8348 što čini 3,17% ukupnog obujma. Na slici 5.6 prikazana je statistika za autonomni sustav 4837.



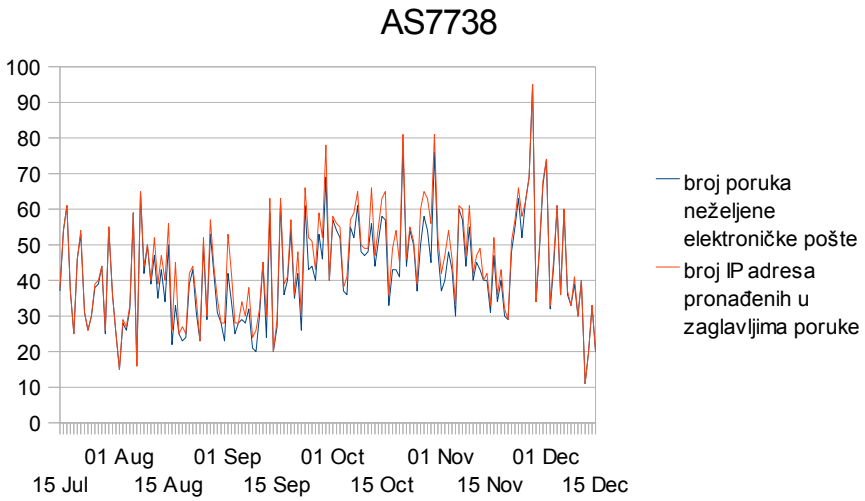
Slika 5.6. Statistika za autonomni sustav 4837

Reputacija sustava za dan 8. studeni prikazana je na slici 5.7.



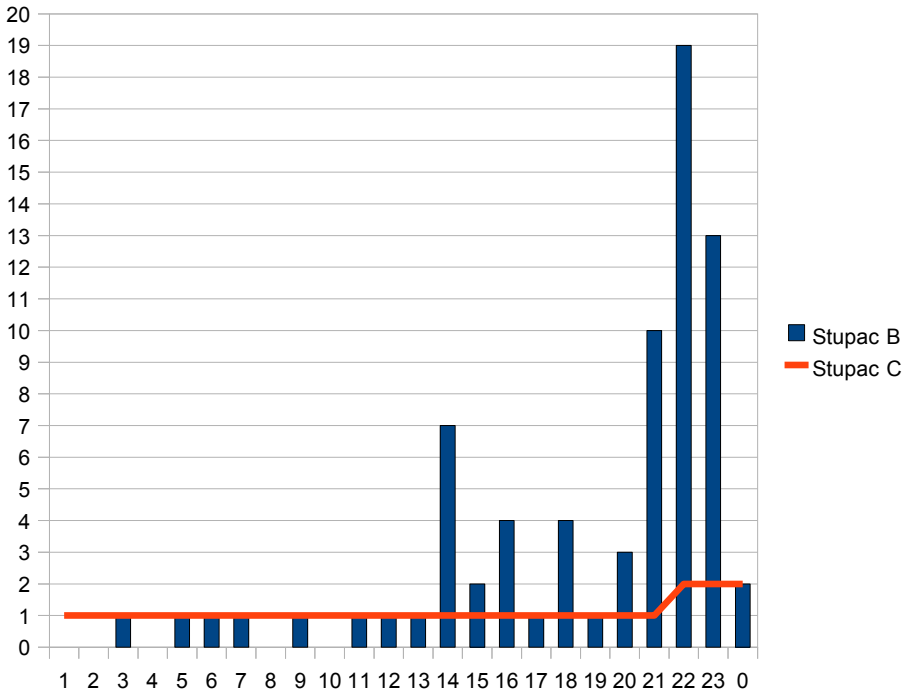
Slika 5.7. Prikaz reputacije sustava

Treći autonomni sustav po broju poslane neželjene elektroničke pošte je Telemar iz Brazila, broj autonomnog sustava 7738. U promatranom razdoblju je s sustava pristiglo 6480 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 6909 što čini 2,62% ukupnog obujma. Na slici 5.8 prikazana je statistika za autonomni sustav 7738.



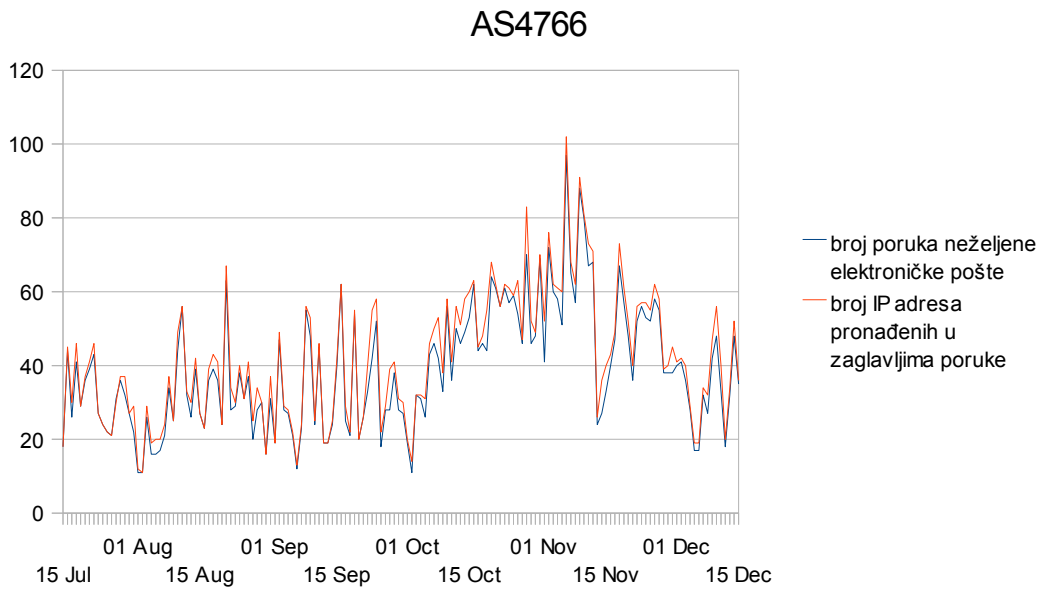
Slika 5.8. Statistika za autonomni sustav 7738

Reputacija sustava za dan 7. Kolovoza prikazana je na slici 5.9.



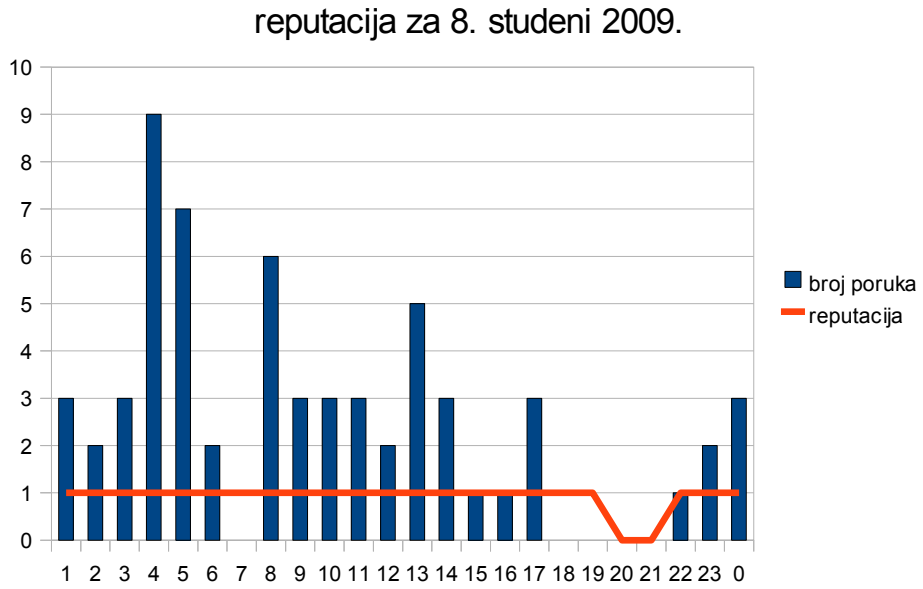
Slika 5.9. Prikaz reputacije sustava

Četvrti autonomni sustav po broju poslane neželjene elektroničke pošte je KORNet iz Koreje, broj autonomnog sustava 4766. U promatranom razdoblju je s sustava pristiglo 5958 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 6435 što čini 2,44% ukupnog obujma . Na slici 5.10 prikazana je statistika za autonomni sustav 4766.



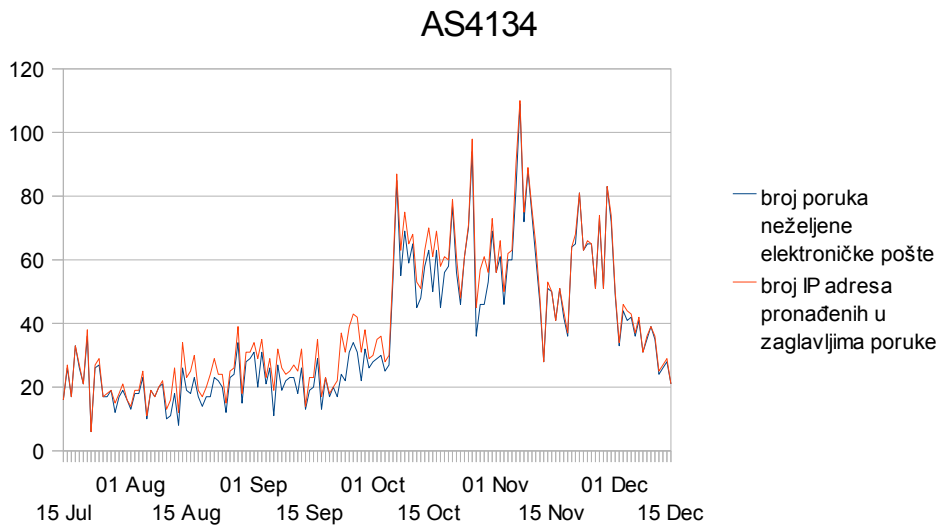
Slika 5.10. Statistika za autonomni sustav 4766

Reputacija sustava za dan 8. studeni 2009. prikazana je na slici 5.11.



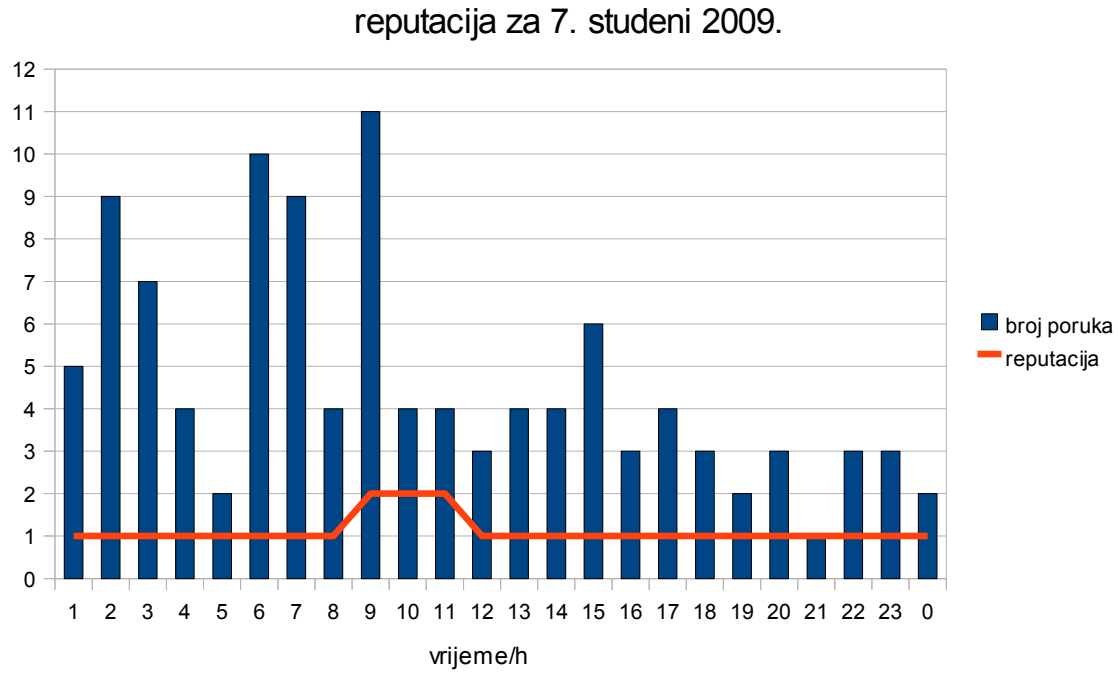
Slika 5.11. Prikaz reputacije sustava

Peti autonomni sustav po broju poslane neželjene elektroničke pošte je *China Telecom* iz Kine, broj autonomnog sustava 4134. U promatranom razdoblju je s sustava pristiglo 5667 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 6161 što čini 2,34% ukupnog obujma. Na slici 5.12 prikazana je statistika za autonomni sustav 4134.



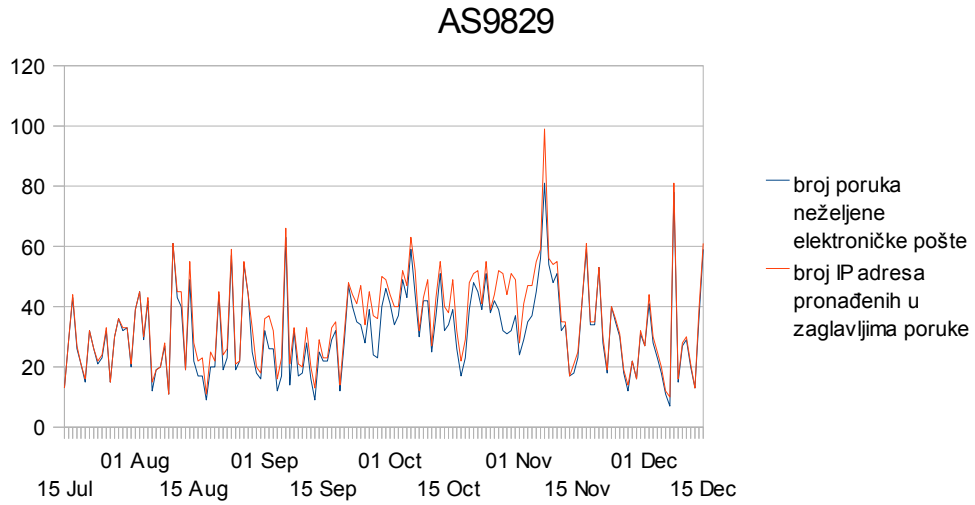
Slika 5.12. Statistika za autonomni sustav 4134

Reputacija sustava za dan 7. studeni 2009 prikazana je na slici 5.13.



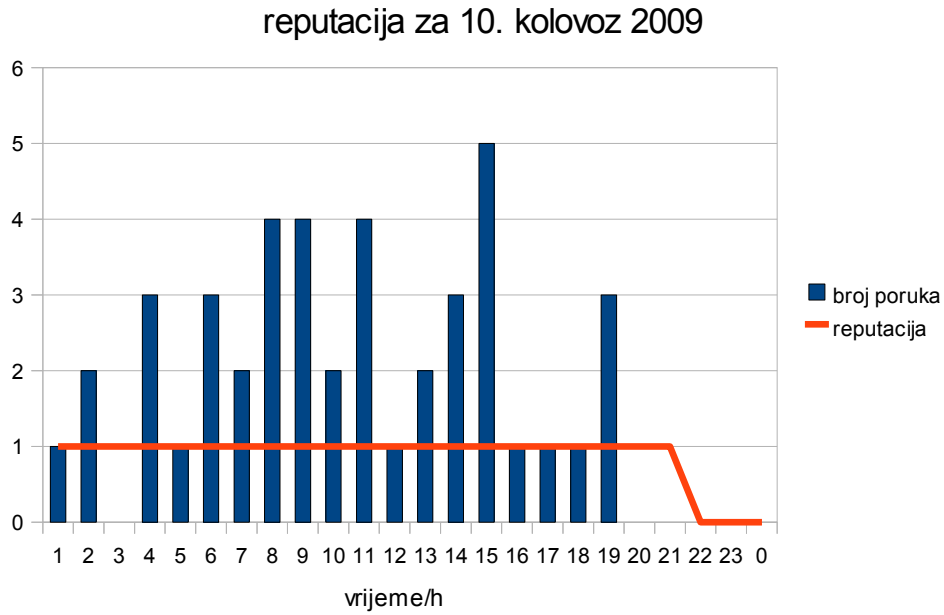
Slika 5.13. Prikaz reputacije sustava

Šesti autonomni sustav po broju poslane neželjene elektroničke pošte je *National Internet Backbone Bharat Sanchar Nigam Limited* iz Indije, broj autonomnog sustava 9829. U promatranom razdoblju je s sustava pristiglo 4851 poruka neželjene elektroničke pošte Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 5408 što čini 2,05% ukupnog obujma. Na slici 5.14 prikazana je statistika za autonomni sustav 9829.



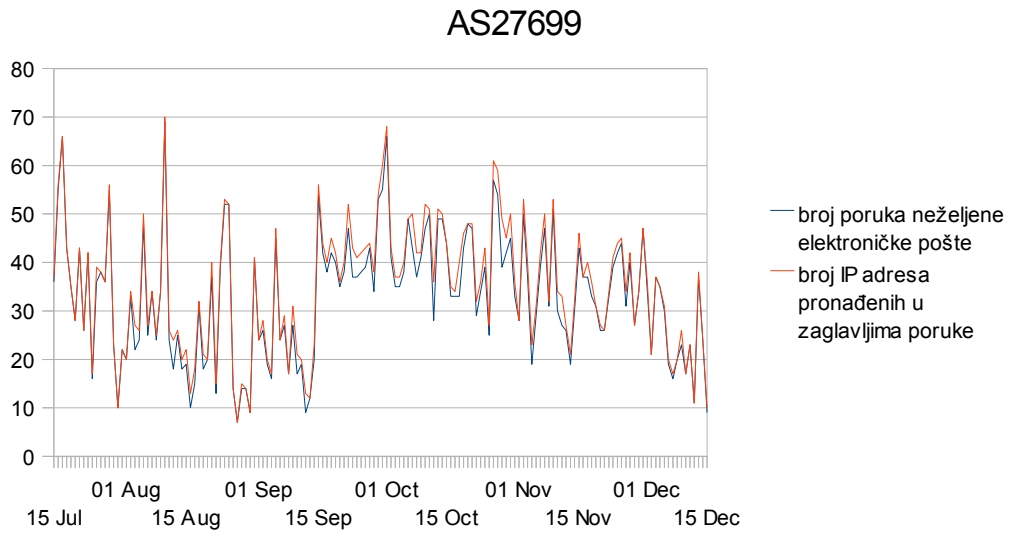
Slika 5.14. Statistika za autonomni sustav 9829

Reputacija sustava za dan prikazana je na slici 5.15.



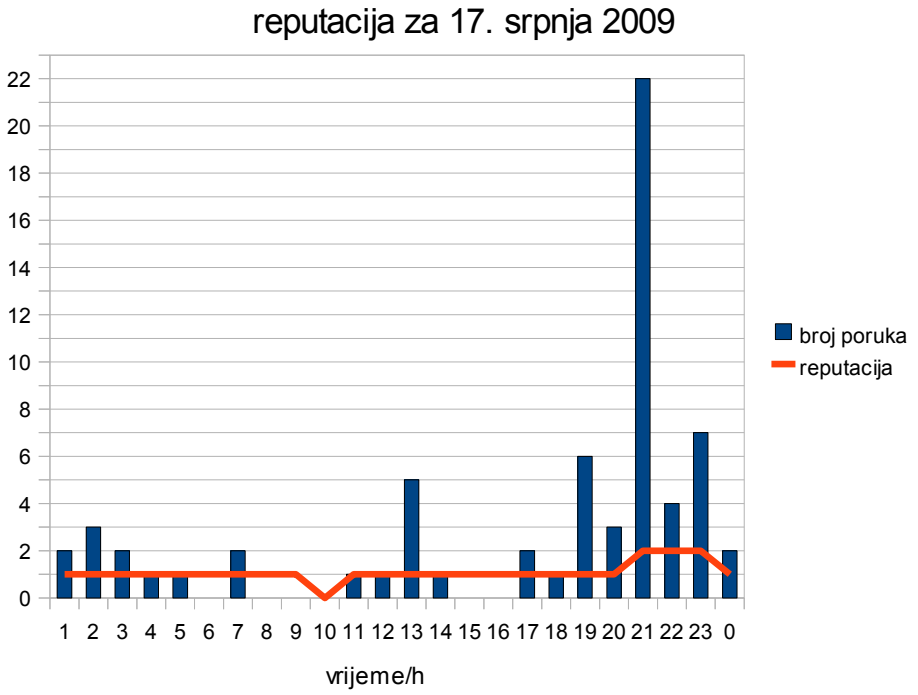
Slika 5.15. Prikaz reputacije sustava

Sedmi autonomni sustav po broju poslane neželjene elektroničke pošte je *Telecomunicacoes de Sao Paulo S/A – Telesp* iz Brazila, broj autonomnog sustava 27699. U promatranom razdoblju je s sustava pristiglo 5082 poruka neželjene elektroničke pošte što čini 2,04% ukupnog obujma. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 5369. Na slici 5.16 prikazana je statistika za autonomni sustav 27699.



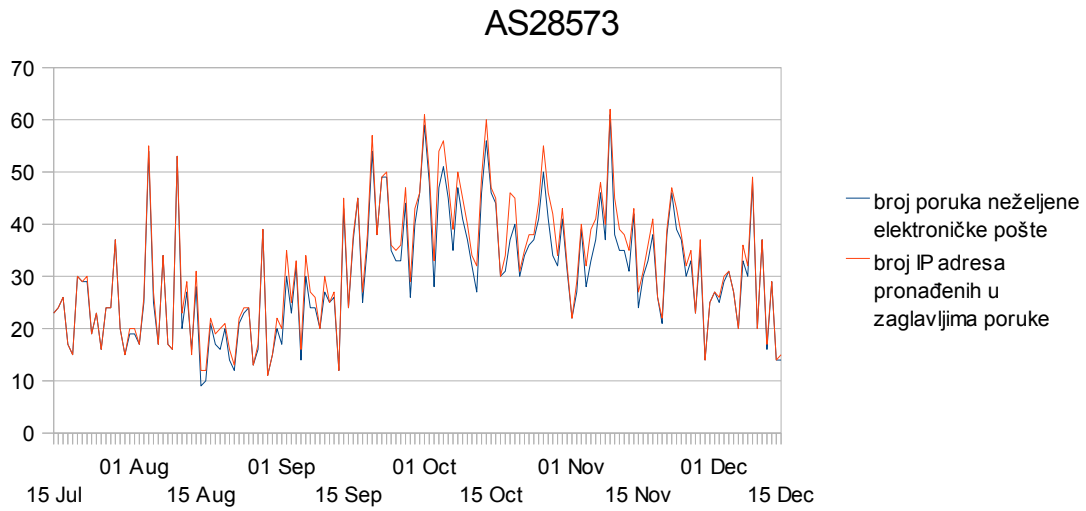
Slika 5.16. Statistika za autonomni sustav 27699

Reputacija sustava za dan prikazana je na slici 5.17.



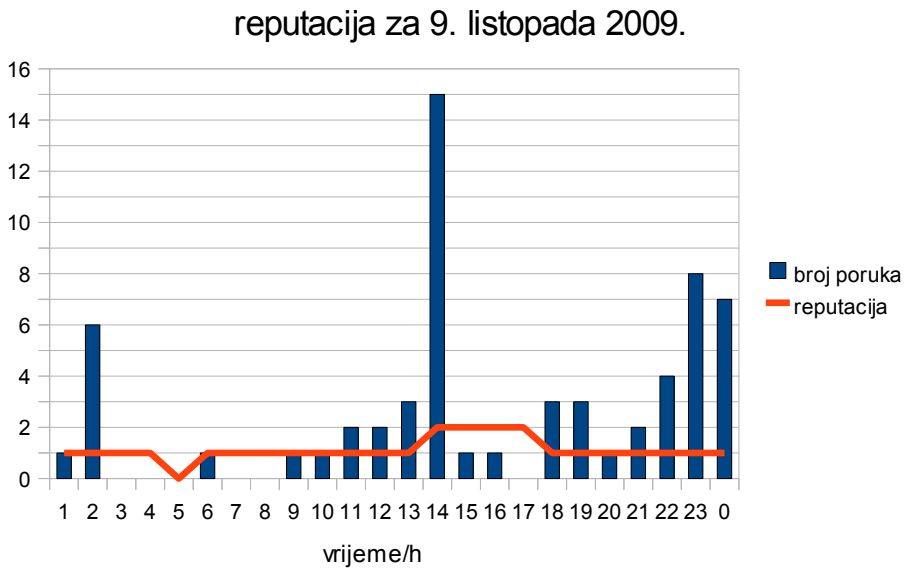
Slika 5.17. Prikaz reputacije sustava

Osmi autonomni sustav po broju poslane neželjene elektroničke pošte je *Virtua Net Servicos de Comunicacao S A* iz Brazila, broj autonomnog sustava 28573. U promatranom razdoblju je s sustava pristiglo 4557 poruka neželjene elektroničke pošte što čini 1,87% ukupnog obujma. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 4922. Na slici 5.18 prikazana je statistika za autonomni sustav 28573.



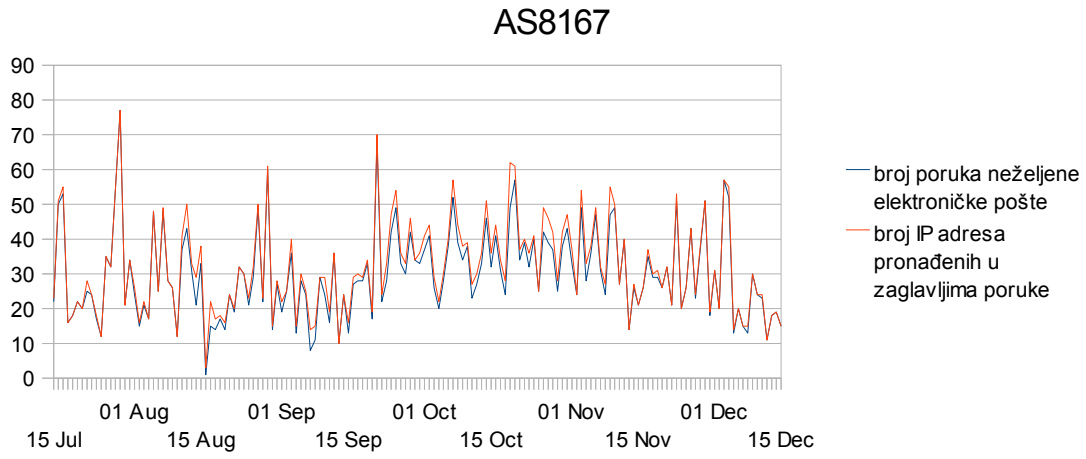
Slika 5.18. Statistika za autonomni sustav 28573

Reputacija sustava za dan prikazana je na slici 5.19.



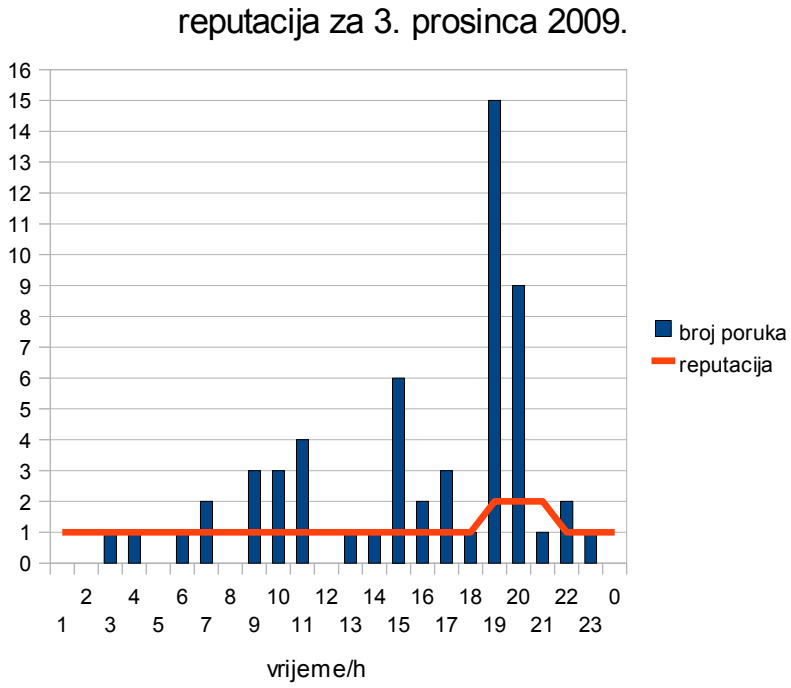
Slika 5.19. Prikaz reputacije sustava

Deveti autonomni sustav po broju poslane neželjene elektroničke pošte je *Telesc – Telecomunicacoes de Santa Catarina SA* iz Brazila, broj autonomnog sustava 8167. U promatranom razdoblju je s sustava pristiglo 4613 poruka neželjene elektroničke pošte što čini 1,87% ukupnog obujma. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 4916. Na slici 5.20 prikazana je statistika za autonomni sustav 8167.



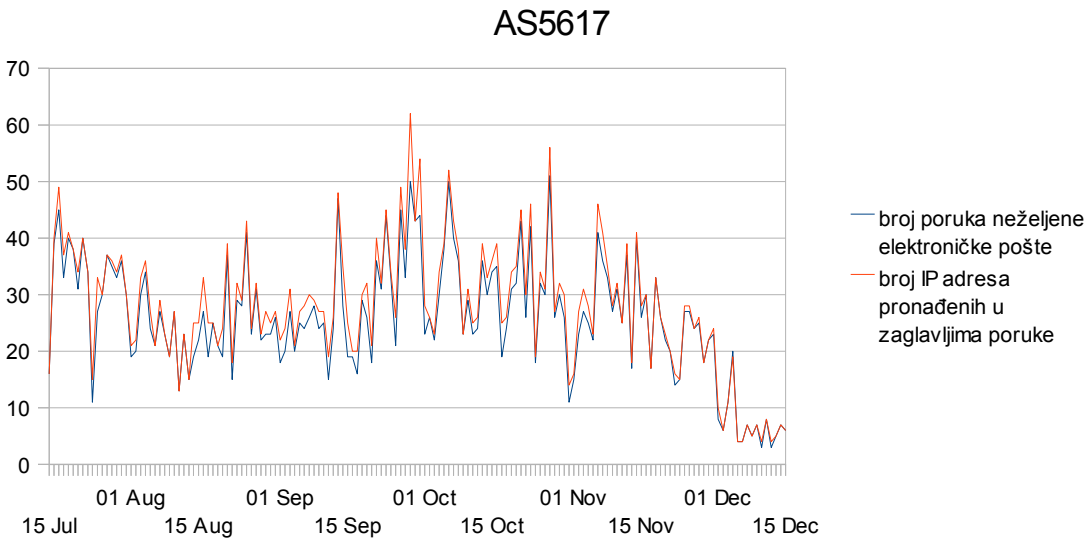
Slika 5.20. Statistika za autonomni sustav 8167

Reputacija sustava za dan 3. prosinca 2009. prikazana je na slici 5.21.



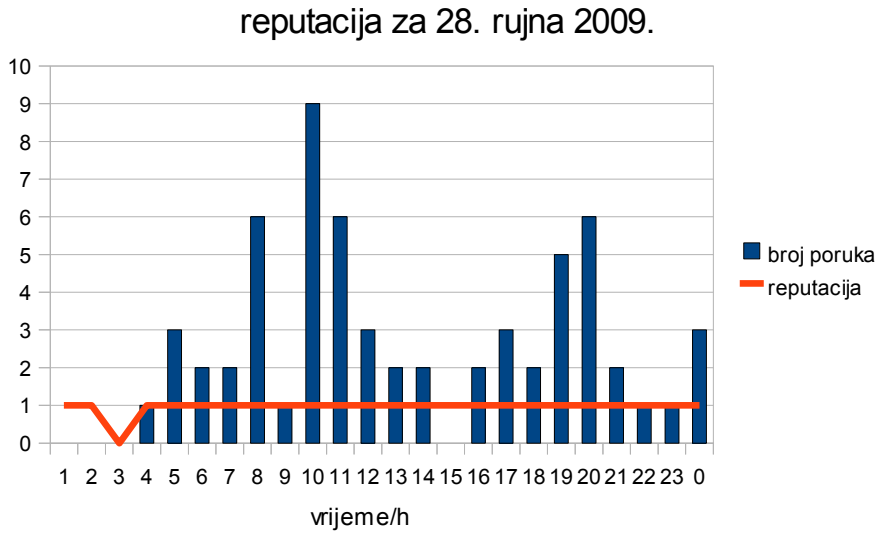
Slika 5.21. Prikaz reputacije sustava

Deseti autonomni sustav po broju poslane neželjene elektroničke pošte je *TPNet* iz Poljske, broj autonomnog sustava 5617. U promatranom razdoblju je s sustava pristiglo 3970 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 4286 što čini 1,63% ukupnog obujma. Na slici 5.22 prikazana je statistika za autonomni sustav 5617.



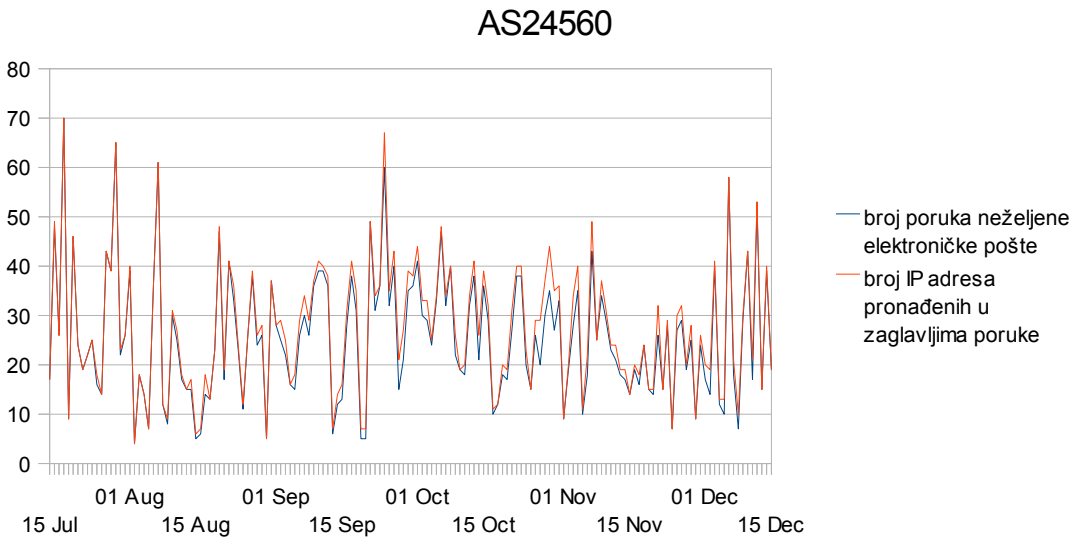
Slika 5.22. Statistika za autonomni sustav 5617

Reputacija sustava za dan prikazana je na slici 5.23.



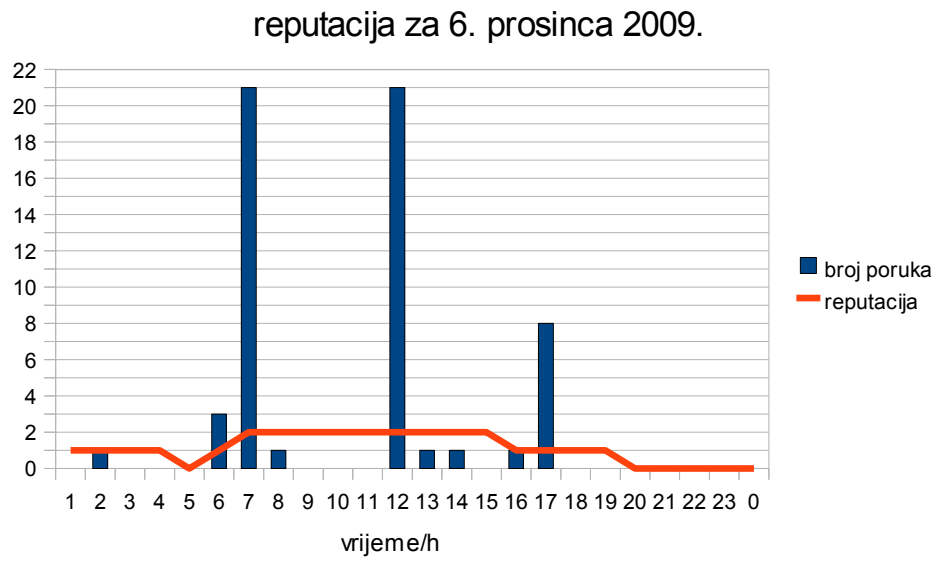
Slika 5.23. Prikaz reputacije sustava

Jedanaesti autonomni sustav po broju poslane neželjene elektroničke pošte je *Virtua Net Servicos de Comunicacao S A* iz Brazila, broj autonomnog sustava 24560. U promatranom razdoblju je s sustava pristiglo 3939 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 4226 što čini 1,6% ukupnog obujma. Na slici 5.24 prikazana je statistika za autonomni sustav 24560.



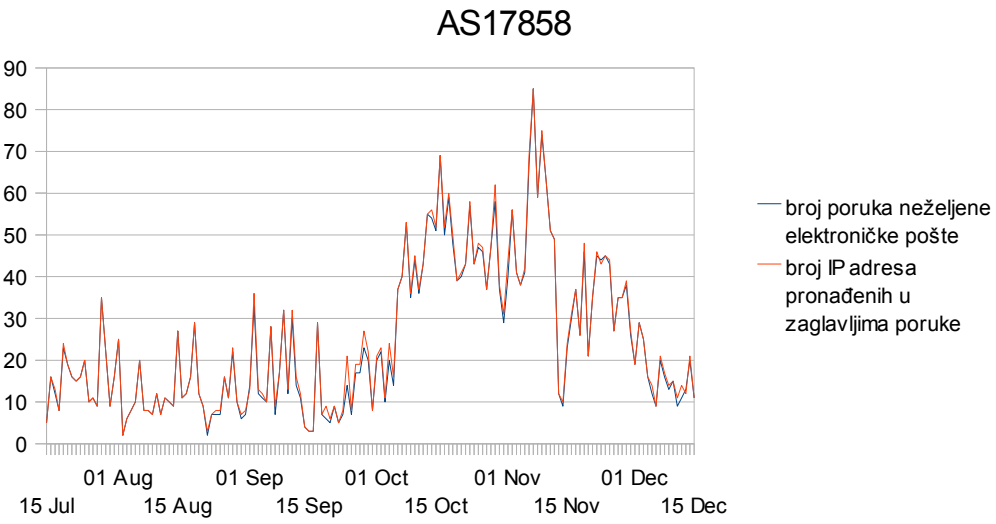
Slika 5.24. Statistika za autonomni sustav 24560

Reputacija za dan 6. prosinca 2009. dana je na slici 5.25.



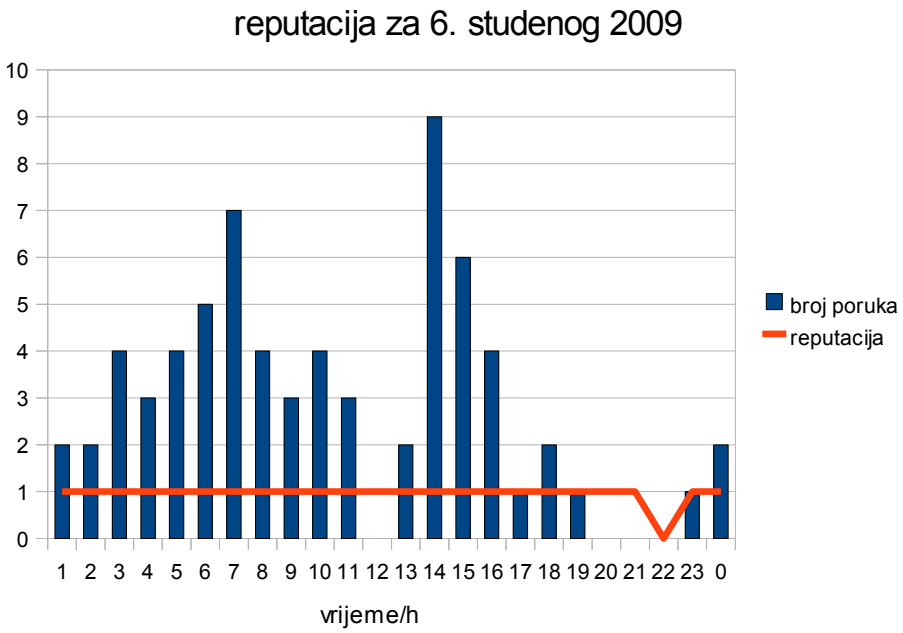
Slika 5.25. Prikaz reputacije sustava

Dvanaesti autonomni sustav po broju poslane neželjene elektroničke pošte je *Korea Network Information Center* iz Koreje, broj autonomnog sustava 17858. U promatranom razdoblju je s sustava pristiglo 3793 poruka neželjene elektroničke pošte Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 3893 što čini 1,48% ukupnog obujma. Na slici 5.26 prikazana je statistika za autonomni sustav 17858.



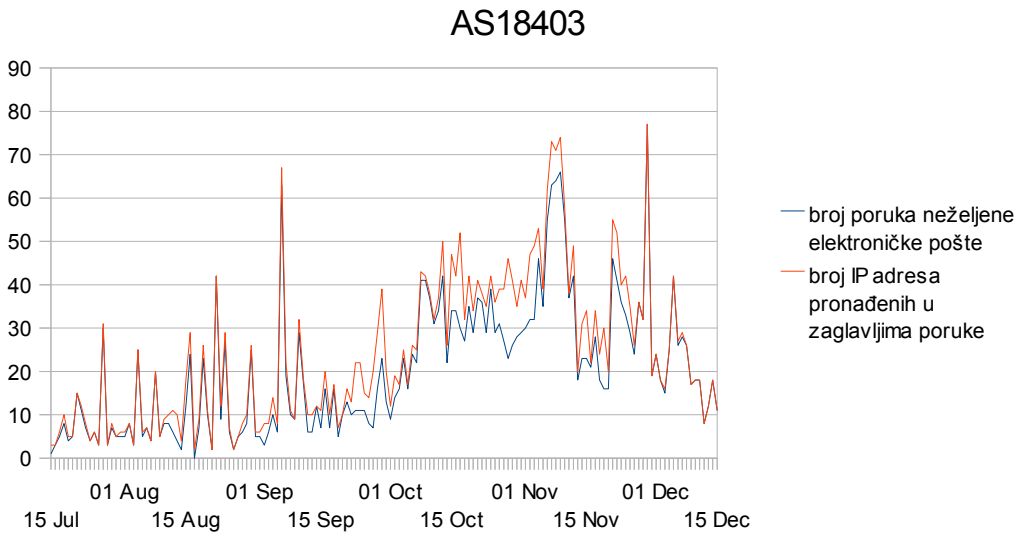
Slika 5.26. Statistika za autonomni sustav 17858

Reputacija sustava za dan 6. studenog dana je na slici 5.27.



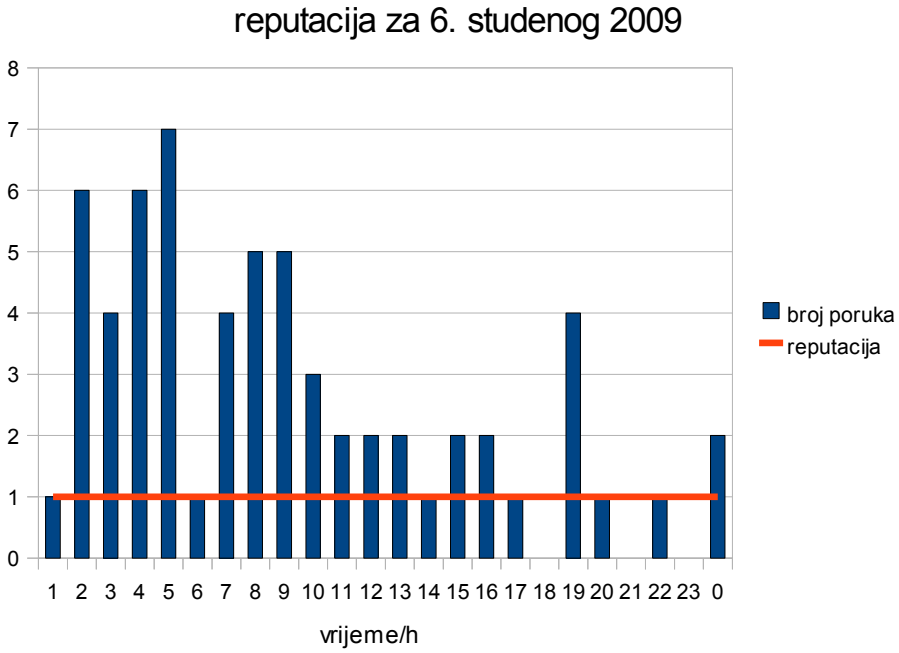
Slika 5.27. Prikaz reputacije sustava

Trinaesti autonomni sustav po broju poslane neželjene elektroničke pošte je *FPT Telecom Company* iz Vijetnama, broj autonomnog sustava 18403. U promatranom razdoblju je s sustava pristiglo 3124 poruka neželjene elektroničke pošte Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 3704 što čini 1,41% ukupnog obujma. Na slici 5.28 prikazana je statistika za autonomni sustav 18403.



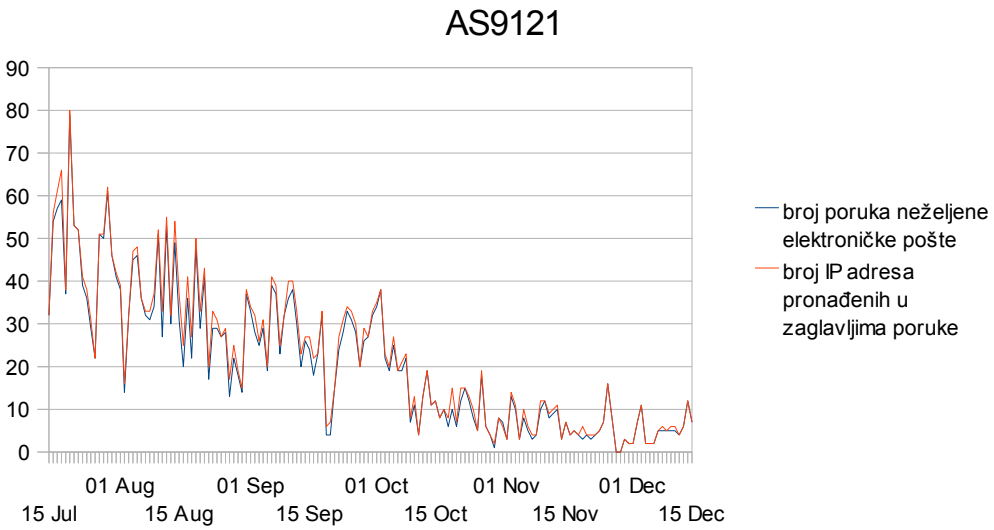
Slika 5.28. Statistika za autonomni sustav 18403

Reputacija sustava za dan 6. studenog 2009. prikazana je na slici 5.29.



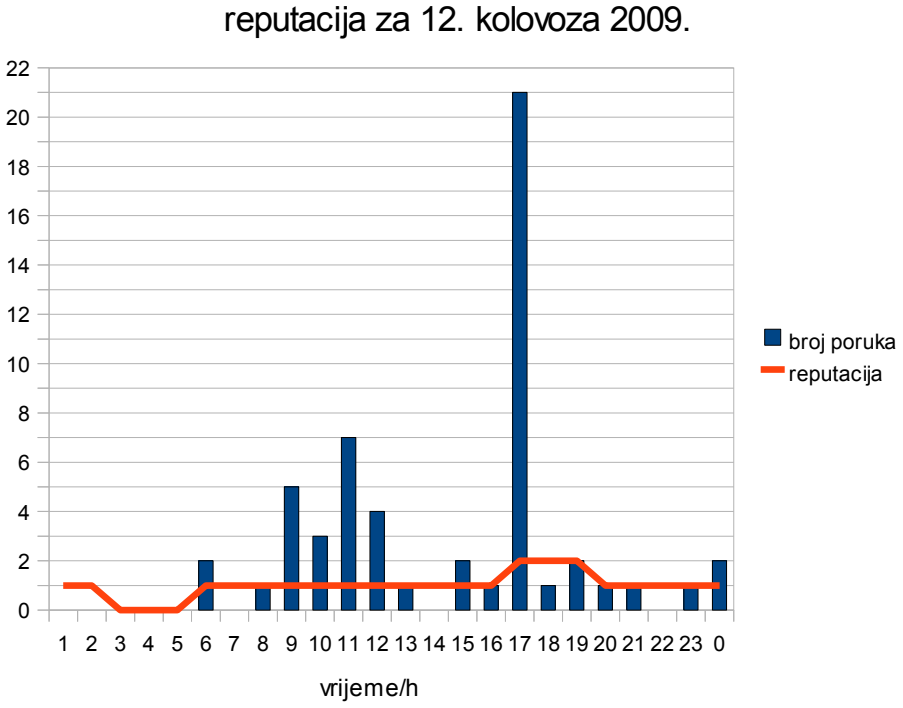
Slika 5.29. Prikaz reputacije sustava

Četrnaesti autonomni sustav po broju poslane neželjene elektroničke pošte je *Virtua Net Servicos de Comunicacao S A* iz Brazila, broj autonomnog sustava 28573. U promatranom razdoblju je s sustava pristiglo 3228 poruka neželjene elektroničke pošte Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 3430 što čini 1,3% ukupnog obujma. Na slici 5.30 prikazana je statistika za autonomni sustav 9121.



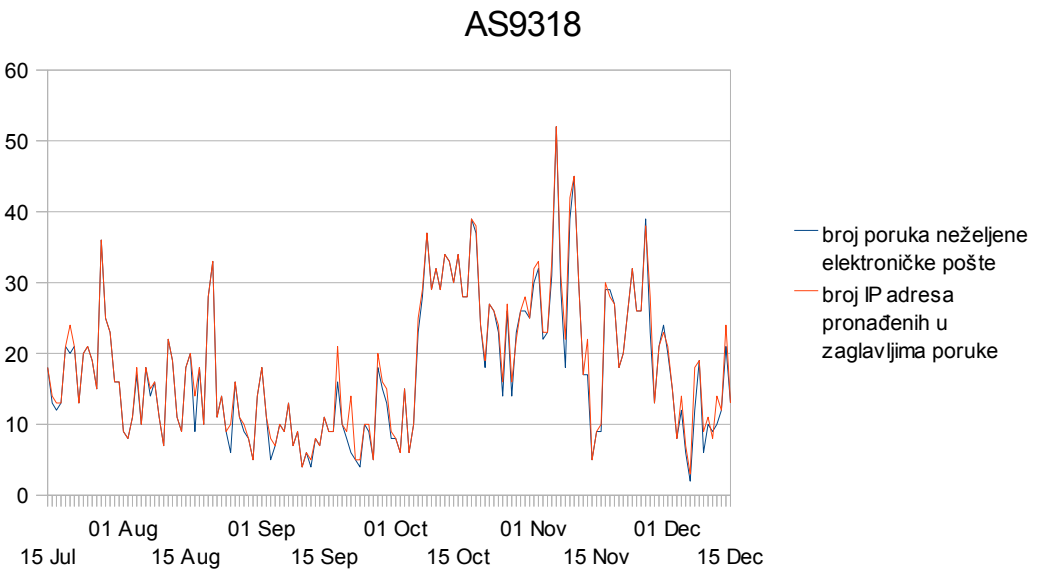
Slika 5.30. Statistika za autonomni sustav 9121

Reputacija sustava za dan 12. kolovoza 2009. dana je na slici 5.31.



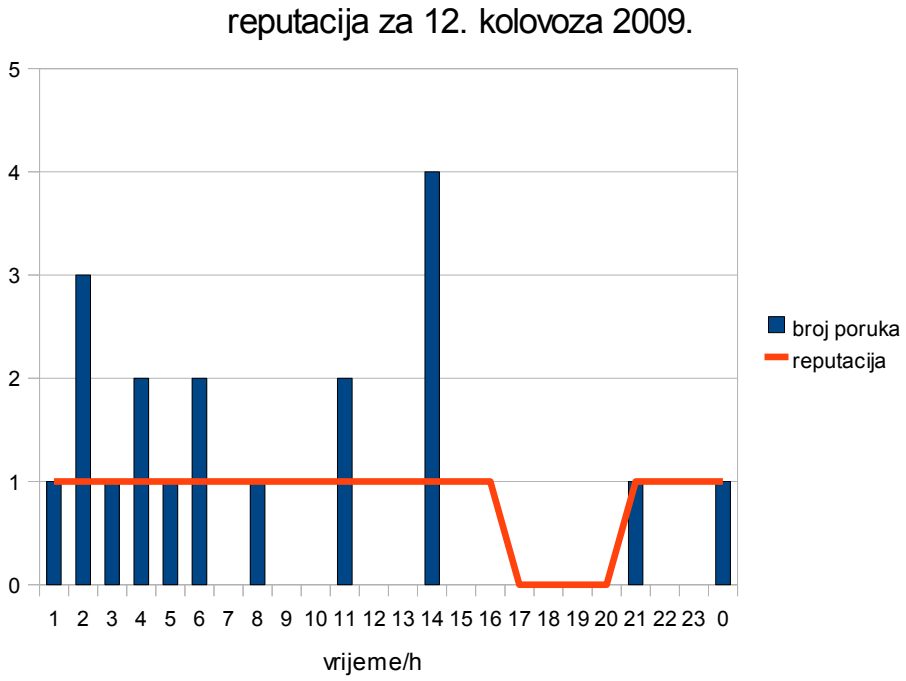
Slika 5.31. Prikaz reputacije sustava

Petnaesti autonomni sustav po broju poslane neželjene elektroničke pošte je *Virtua Net Servicos de Comunicacao S A* iz Brazila, broj autonomnog sustava 3918. U promatranom razdoblju je s sustava pristiglo 2711 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 2812 što čini 1,07% ukupnog obujma. Na slici 5.32 prikazana je statistika za autonomni sustav 9318.



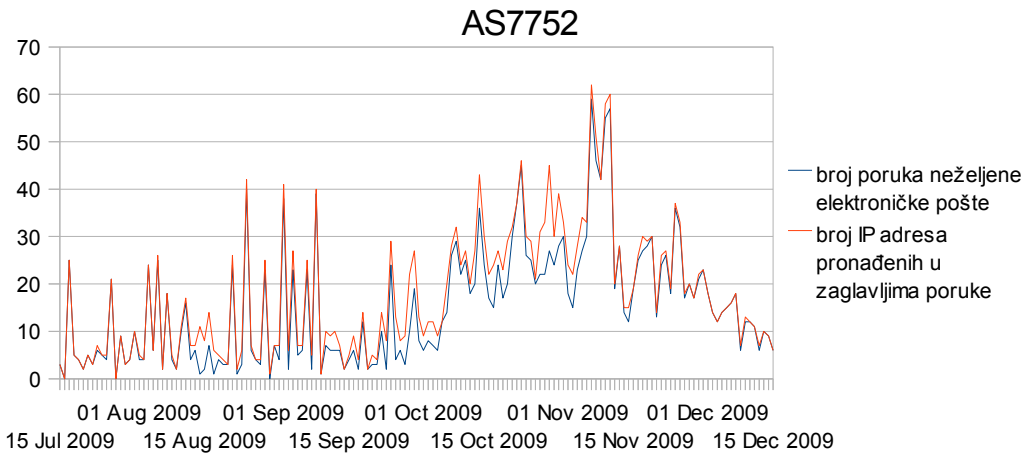
Slika 5.32. Statistika za autonomni sustav 9318

Reputacija sustava za dan 12. kolovoza 2009. prikazana je na slici 5.33.



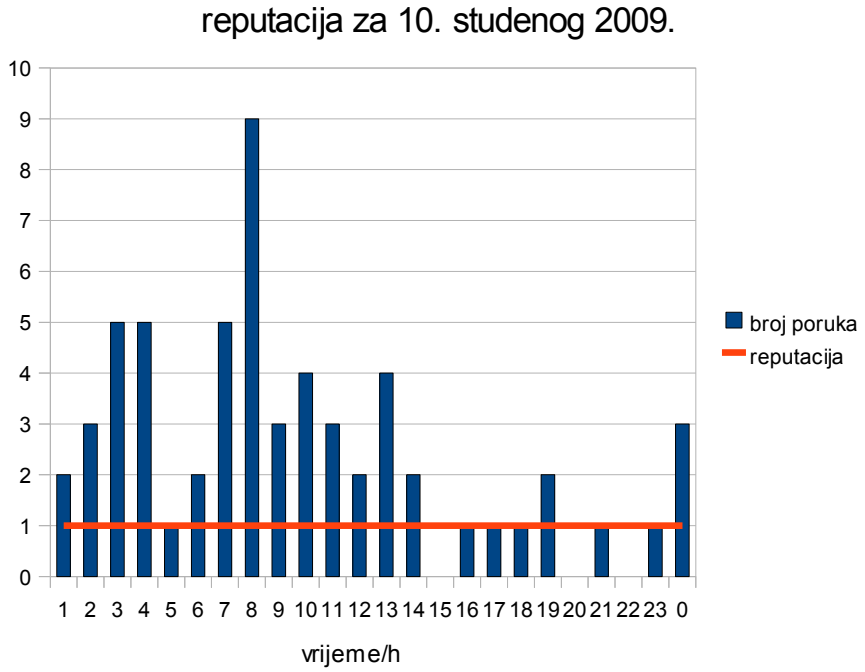
Slika 5.33. Prikaz reputacije sustava

Šesnaesti autonomni sustav po broju poslane neželjene elektroničke pošte je *Threshold Communicatioins, Inc.* iz Sjedinjenih američkih država, broj autonomnog sustava 7752. U promatranom razdoblju je s sustava pristiglo 2336 poruka neželjene elektroničke pošte Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 2710 što čini 1,03% ukupnog obujma. Na slici 5.34 prikazana je statistika za autonomni sustav 7752.



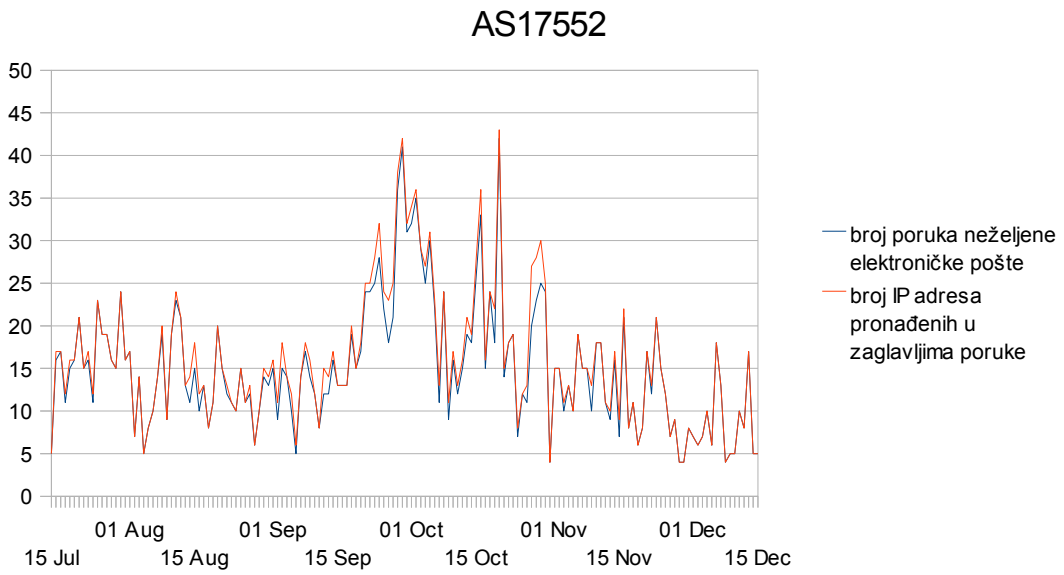
Slika 5.34. Statistika za autonomni sustav 7552

Reputacija sustava za dan 10. studenog 2009. prikazana je na slici 5.35.



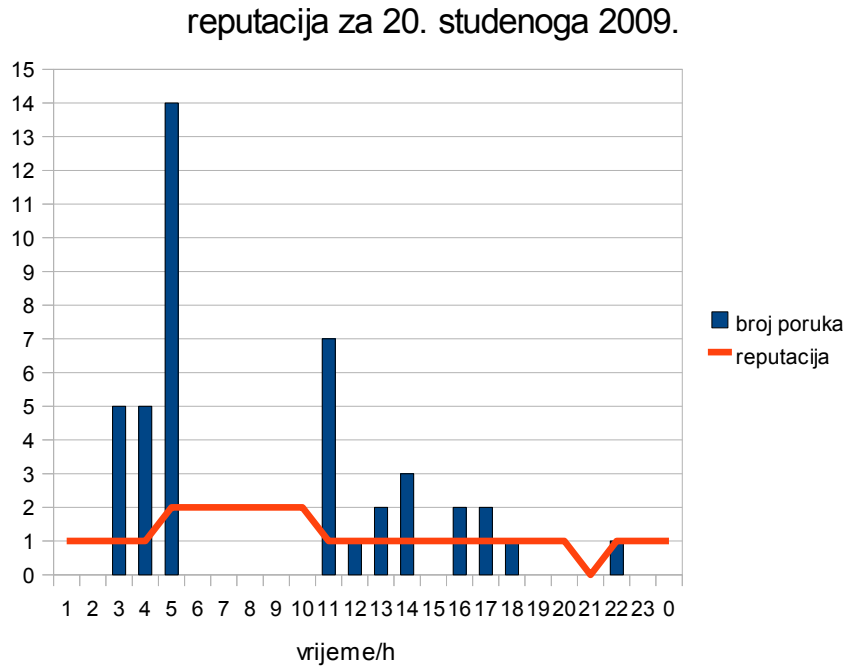
Slika 5.35. Prikaz reputacije sustava

Sedamnaesti autonomni sustav po broju poslane neželjene elektroničke pošte je *True Corporation Co, Ltd.* iz Tajlanda, broj autonomnog sustava 17552. U promatranom razdoblju je s sustava pristiglo 2326 poruka neželjene elektroničke pošte Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 2449 što čini 0,93% ukupnog obujma. Na slici 5.36 prikazana je statistika za autonomni sustav 17552.



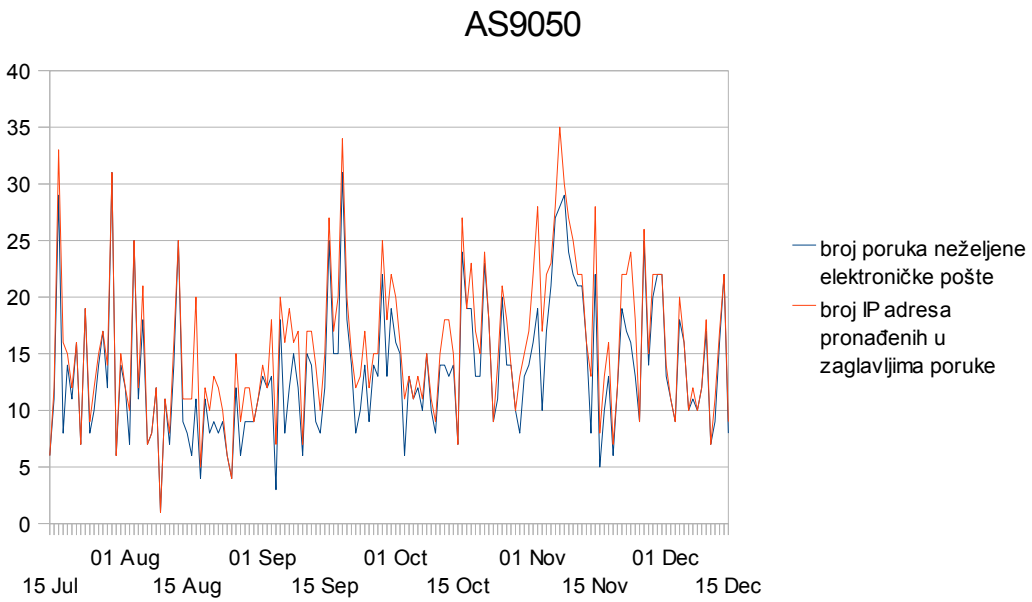
Slika 5.36. Statistika za autonomni sustav 17552

Reputacija sustava za dan 20. studenog 2009 prikazana je na slici 5.37.



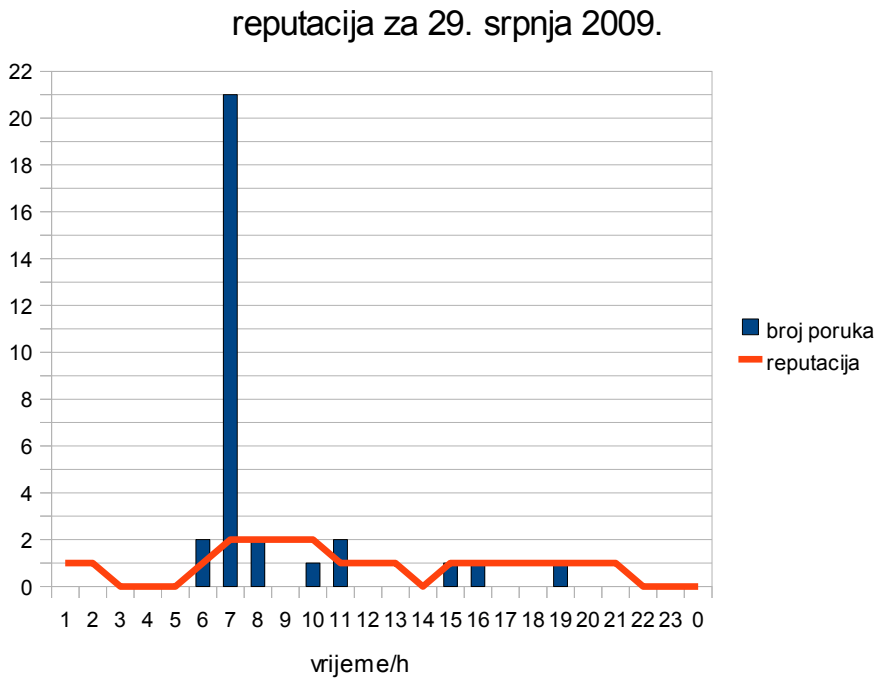
Slika 5.37. Prikaz reputacije sustava

Osamnaesti autonomni sustav po broju poslane neželjene elektroničke pošte je *Romtelecom S.A* iz Rumunjske, broj autonomnog sustava 9050. U promatranom razdoblju je s sustava pristiglo 2083 poruka neželjene elektroničke pošte Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 2408 što čini 0,91% ukupnog obujma.. Na slici 5.38 prikazana je statistika za autonomni sustav 9050.



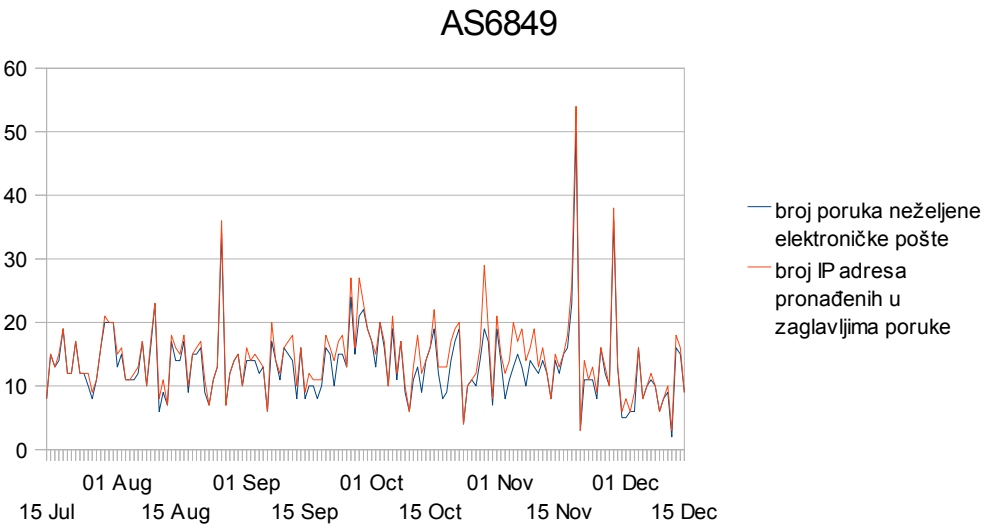
Slika 5.38. Statistika za autonomni sustav 9050

Reputacija sustava za dan 29. srpnja 2009. prikazana je na slici 5.39.



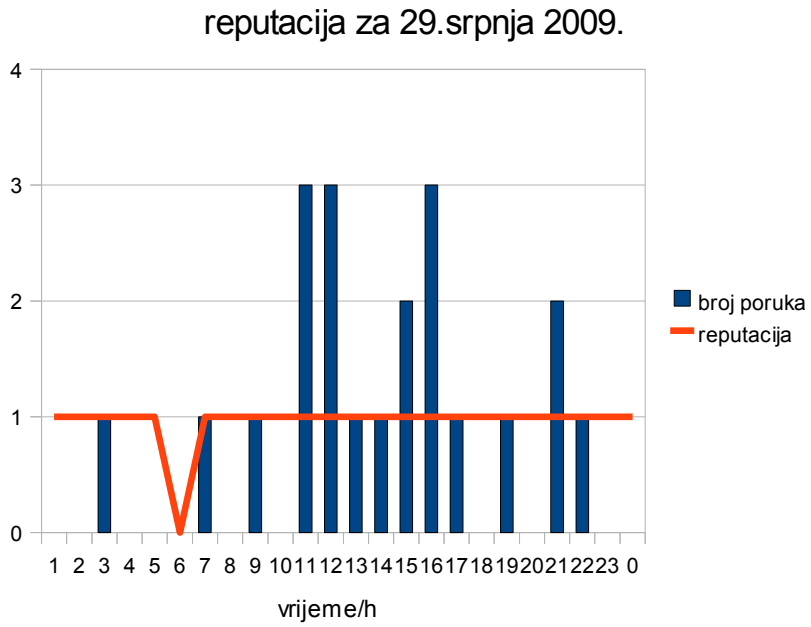
Slika 5.39. Prikaz reputacije sustava

Devetnaesti autonomni sustav po broju poslane neželjene elektroničke pošte je *Virtua Net Servicos de Comunicacao S A* iz Brazila, broj autonomnog sustava 6849. U promatranom razdoblju je s sustava pristiglo 2034 poruka neželjene elektroničke pošte Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 2235 što čini 0,85% ukupnog obujma. Na slici 5.40 prikazana je statistika za autonomni sustav 6849.



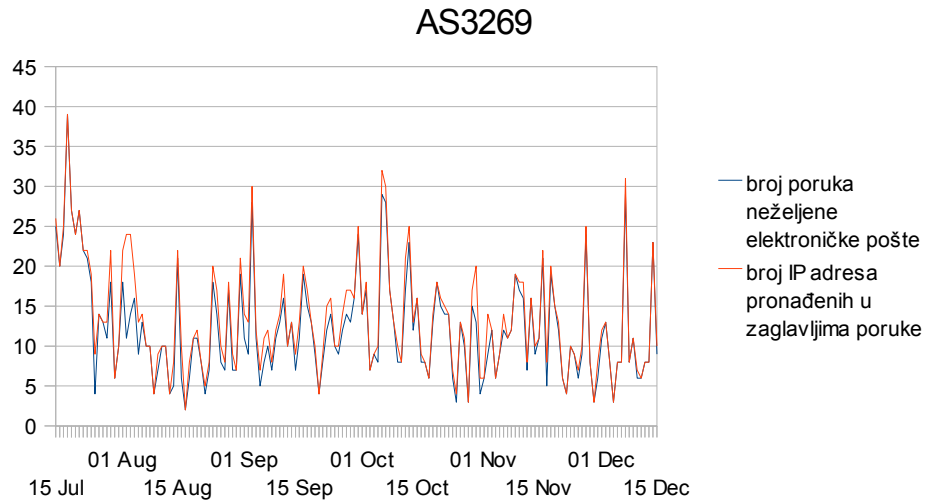
Slika 5.40. Statistika za autonomni sustav 6849

Reputacija sustava za dan 29. srpnja prikazana je na slici 5.41.



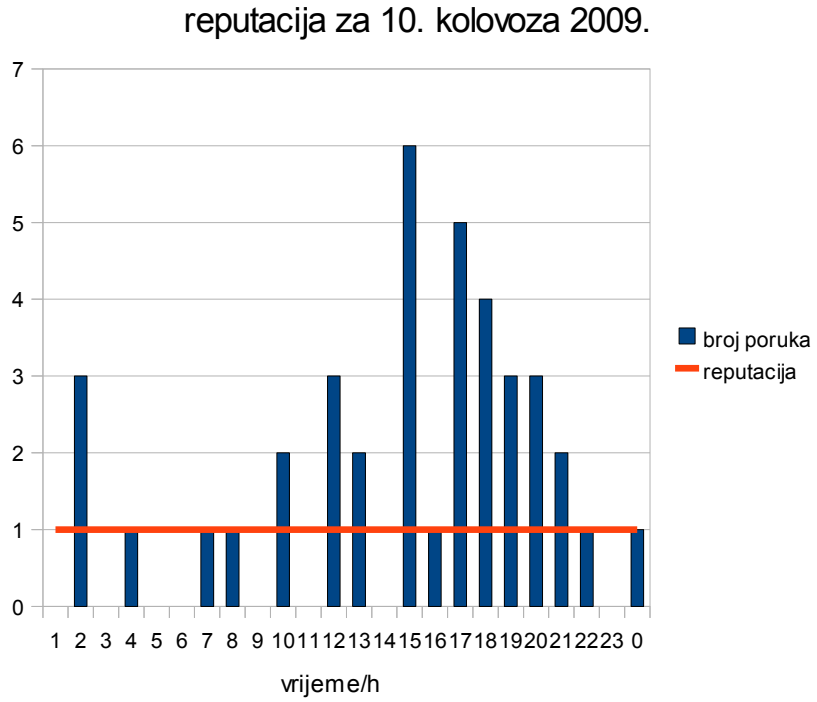
Slika 5.41. prikaz reputacije sustava

Dvadeseti autonomni sustav po broju poslane neželjene elektroničke pošte je *Telecom Italia* iz Italije, broj autonomnog sustava 3269. U promatranom razdoblju je s sustava pristiglo 1876 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 2065 što čini 0,78% ukupnog obujma. Na slici 5.42 prikazana je statistika za autonomni sustav 3269.



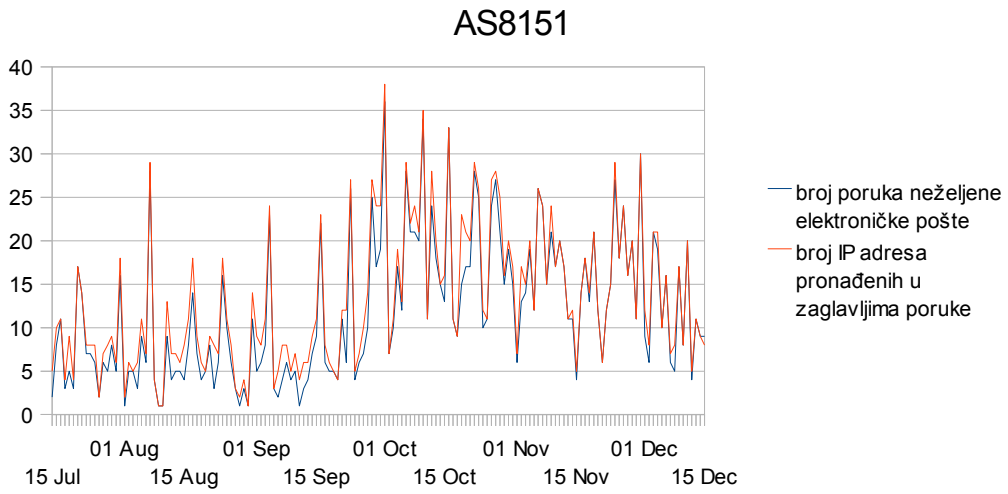
Slika 5.42. Statistika za autonomni sustav 3269

Reputacija sustava za dan 10. kolovoza 2009. prikazana je na slici 5.43.



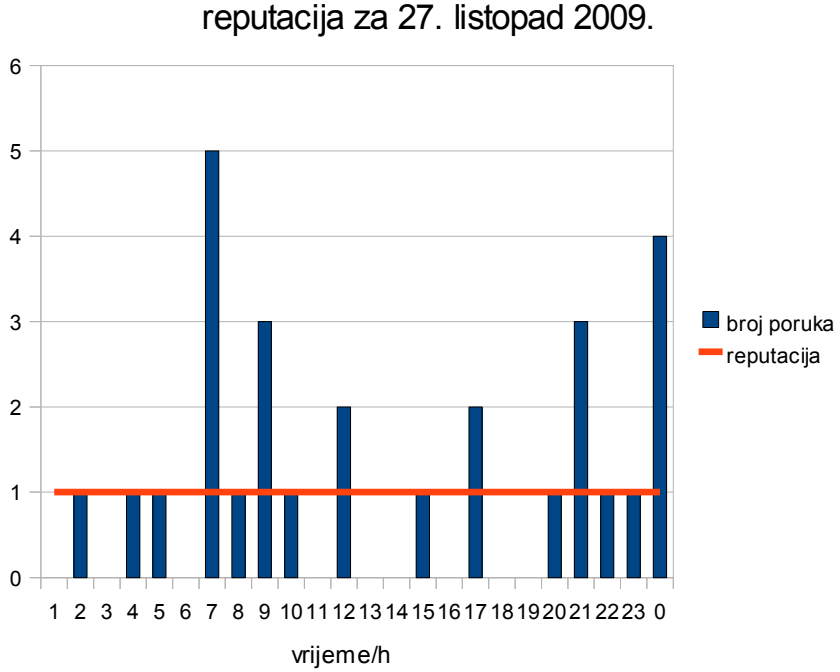
Slika 5.43. Prikaz reputacije sustava

Dvadeset i prvi autonomni sustav po broju poslane neželjene elektroničke pošte je *Virtua Net Servicos de Comunicacao S A* iz Brazila, broj autonomnog sustava 8151. U promatranom razdoblju je s sustava pristiglo 1825 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 2047 što čini 0,78% ukupnog obujma. Na slici 5.44 prikazana je statistika za autonomni sustav 8151.



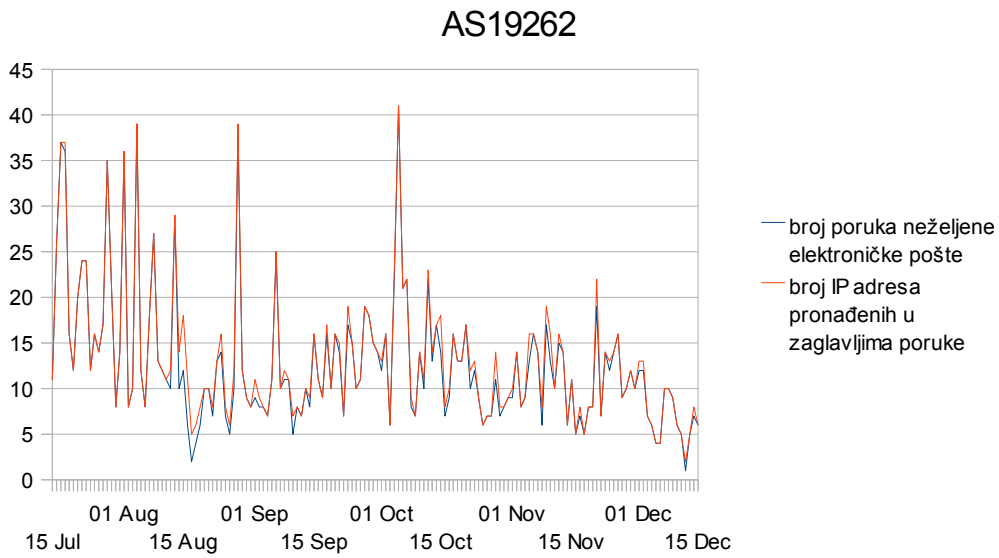
Slika 5.44. Statistika za autonomni sustav 8151

Reputacija sustava za dan 27. listopada 2009. prikazana je na slici 5.45.



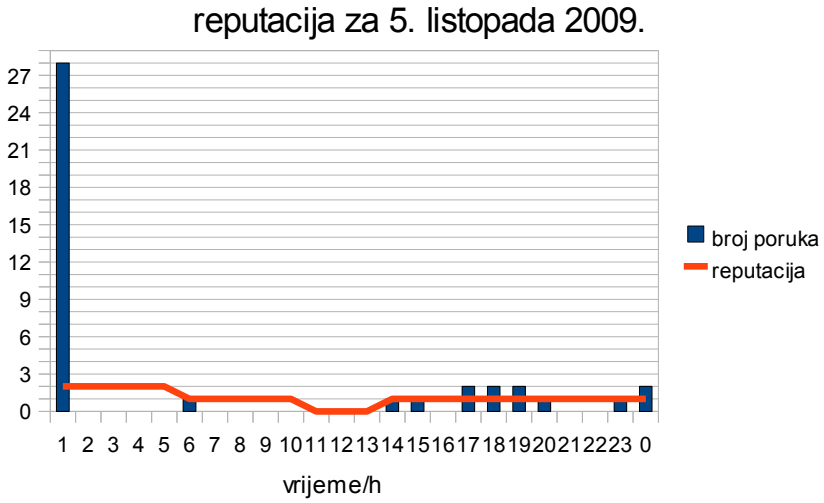
Slika 5.45. Prikaz reputacije sustava

Dvadeset i drugi autonomni sustav po broju poslane neželjene elektroničke pošte je *Verizon Global Networks New York* iz Sjedinjenih američkih država, broj autonomnog sustava 19262. U promatranom razdoblju je s sustava pristiglo 1956 poruka neželjene elektroničke pošte. Broj ukupnih IP adresa koje su pronađene u porukama a pripadaju danom autonomnom sustavu je 2040 što čini 0,77% ukupnog obujma. Na slici 5.46 prikazana je statistika za autonomni sustav 19262.



Slika 5.46. Statistika za autonomni sustav 19262

Reputacija sustava za dan 5. listopada 2009. prikazana je na slici 5.47.



Slika 5.47. Prikaz reputacije sustava

6. Zaključak

Veliki dio moderne komunikacije odvija se putem elektroničke pošte. Kako ona nije početno zamišljena za tako velik obujam došlo je do određenih problema, posebice ako se uzme u obzir količina neželjene elektroničke pošte koja svaki dan pristiže u sandučiće elektroničke pošte. Dosadašnji pokušaji da se smanji ukupna neželjena elektronička pošta svodili su se na statička pravila kojim se pošiljatelji neželjene elektroničke pošte brzo prilagode.

U sklopu ovoga rada izgrađen je reputacijski sustav koji na dinamički način ocjenjuje autonomne sustave praćenjem njihovog ponašanja u realnom vremenu. Sustav je trenutno vrlo jednostavan, tj. u izgradnji baze koristi samo jednu stavku (IP adresu). Postojeća proširenja protokola *SMTP* kao i druga nezavisna rješenja koja za cilj imaju poboljšanje sigurnosti protokola *SMTP* mogla bi se u daljnjem radu uvrstiti u ocjenu određenog autonomnog sustava. Modularna izrada reputacijskog sustava kao i upotreba jezika *python* za izradu, nude jednostavne mogućnosti poboljšanja. Sustav trenutno računa reputaciju svakih sat vremena, što možda za neke velike sustave nije dovoljno, no module je jednostavno modificirati i prilagoditi potrebama svakog sustava.

Rezultati rada reputacijskog sustava koji su prikazani u poglavlju 5 daju naslutiti da već i ovako izgrađen sustav ima mnogo potencijala i daje realnu sliku ponašanja nekog autonomnog sustava. Reputacijski sustav trenutno nema ugrađene mehanizme zaštite od zlouporabe, osim pridjeljivanja inicijalne reputacije svakom novom sustavu. Pošiljatelji neželjene elektoničke pošte mogu iskoristiti činjenicu da reputacijski sustav nagrađuje autonomne sustave koji ne šalju neželjenu elektroničku poštu. Ugrađivanjem raznih proširenja moguće je provjeravati autonomne sustave na više razina i tako sakupiti one kojima se više vjeruje, dok se drugima može inicijalna reputacija više dignuti dok se ne dokažu.

Problem neželjene elektroničke pošte neće najednom nestati, niti će se jedinstvenom tehnikom iskorijeniti, potrebno je zajedno upotrijebiti mnogo kako statičkih tako i dinamičkih metoda, a ovaj izgrađeni reputacijski sustav samo je mali dio.

7. Literatura

1. Spam survey – Enisa,
   URL: http://www.enisa.europa.eu/act/res/other-areas/anti-spam-measures/studies/spam-survey (2/5/2010).
2. The Spamhaus project – The top 10 worst countries,
   URL: http://www.spamhaus.org/statistics/countries.lasso (21/6/2010).
3. Spam Statistics from the Security Labs team at M86 Security,
   URL: http://www.m86security.com/labs/spam_statistics.asp (10/6/2010).
4. The State of Spam | Symantec,
   URL: http://www.symantec.com/business/theme.jsp?themeid=state_of_spam (21/6/2010).
5. Cisco 2009 Annual Security Report – Cisco Systems,
   URL: http://cisco.biz/en/US/prod/vpndevc/annual_security_report.html (15/6/2010).
6. Top 10 botnets and their impact,
   URL: http://www.net-security.org/secworld.php?id=8599 (2/5/2010).
7. The top 10 spam botnets: New and improved | 10 Things | Techrepuclic.com,
   URL: http://blogs.techrepublic.com.com/10things/?p=1373 (2/5/2010).
8. Lars Eggert, SPF Deployment Trends,
   URL: https://fit.nokia.com/lars/meter/spf.html (12/6/2010).
9. Joe Stewart, The return of Warezov,
   URL: http://www.secureworks.com/research/threats/warezov/ (3/5/2010).
10. FireEye Malware Intelligence Lab: McColo hosting Srizbi C&C,
    URL: http://blog.fireeye.com/research/2008/10/mccolo-hosting-srizbi-cc.html (3/5/2010).
11. Brian Krebs, Security Fix – Spam volumes drop by two-thirds after firm goes offline,
    URL:
    http://voices.washingtonpost.com/securityfix/2008/11/spam_volumes_drop_by_23_after.html (3/5/2010).
12. John E. Dunn, Srizbi grows into world's largest botnet,
    URL: http://www.csoonline.com/article/356219/srizbi-grows-into-world-s-largest-botnet (3/5/2010).
13. Russian Business Network (RBN),
    URL: http://rbnexploit.com/ (15/6/2010).
14. UAB computer forensics links internet postcards to virus,
    URL: http://www.hindu.com/thehindu/holnus/008200907271321.htm (15/6/2010).
15. The Spamhaus Project – Effective Spam Filtering,
    URL: http://www.spamhaus.org/whitepapers/effective_filtering.html (25/4/2010).

16. Tim Webber, Criminals 'may overwhelm the web',
URL: http://news.bbc.co.uk/2/hi/business/6298641.stm (17/7/2010).

17. Anatomy of a Targeted Attack,
URL: http://www.dambala.com/d_pubs/Targeted-Attack-Anatomy.html (1/7/2010)

18. DNSBL information – SPAM database lookup,
URL: http://www.dnsbl.info (6/7/2010)

19. The Spamhaus Project – SBL,
URL: http://www.spamhaus.org/faq/answers.lasso?section=Spamhaus%20SBL (4/7/2010)

20. The Spamhaus Project – XBL,
URL: http://www.spamhaus.org/faq/answers.lasso?section=Spamhaus%20XBL (4/7/2010)

21. The Spamhaus Project – DBL,
URL: http://www.spamhaus.org/faq/answers.lasso?section=Spamhaus%20DBL (4/7/2010)

22. The CAN-SPAM Act: A Compliance Guide for Business,
URL: http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm (1/9/2010)