pd.tvz.hr
POLYTECHNIC & DESIGN Vol. 7, No. 2, 2019.
DOI: 10.19279/TVZ.PD.2019-7-2-01

OTKRIVANJE MREŽE KOMPROMITIRANIH RAČUNALA ANALIZOM IMENIČKOG PROMETA

BOTNET DETECTING BASED ON DNS TRAFFIC ANALYSIS

Brigitta Cafuta, Bojan Nožica, Ivica Dodig, Tin Kramberger

Tehničko veleučilište u Zagrebu, Vrbik 8, Zagreb, Hrvatska

Sažetak

Svakim danom sve je više aktivnih naziva zona u imeničkom sustavu. Uslijed rasta i hijerarhijske organizacije interneta povećava se i broj organizacija koje su zadužene za registraciju zona. Disperzijom administrativnih zadaća otežava se kontrola i olakšavaju se mogućnosti zlonamjernih registracija. Iza zlonamjernih zona prikrivaju se napadački poslužitelji (engl. Command & Control Servers - C&C) koji upravljaju mrežom kompromitiranih računala (engl. botnet). Napadački poslužitelji u izabranom trenutku mogu pokrenuti instaliranu nepoželjnu programsku podršku (engl. malware agent) na klijentu. Pojedina kompromitirana računala u toj mreži mogu prema uputi napadačkog poslužitelja posluživati internetske stranice ili slati elektroničku poštu. Kroz poslužene internetske stranice ili poslanu nepoželjnu elektroničku poštu (engl. spam) širi se mreža kompromitiranih računala. Za sprječavanje aktivnosti mreže kompromitiranih računala neophodno je otkriti kompromitirane klijente i postojanje veze prema napadačkom poslužitelju. U ovom radu prikazana je metoda otkrivanja zlonamjernih domena korištenjem imeničkog servisa (engl. Domain Name System-DNS) te su prikazani uzorci algoritma za detekciju kompromitiranih računala. Provedeno je istraživanje temeljem najjednostavnijih imeničkih servisa koje dokazuje postojanje zlonamjernih domena.

Ključne riječi: *mreža kompromitiranih računala, imenički promet, skrivanje adresa*

Abstract

The number of Internet active domain names is rapidly raising, thus proportionally share of malicious domains is increasing. Behind the malicious domains are reflectors controlled indirectly by Command & Control Servers (C & C), which manage the network of compromised computers (botnet). Botnet administrator by placing and information on malicious domain at a given time can launch an installed malware agent on the compromised clients. These commands may vary from a DoS server, launching a server, visit the webpage or send an electronic mail. The consequence of the command can result on widening the botnet or performing an illegal activity. The best solution to prevent a botnet in operation is to block the communication channel from compromised client to botnet administrator by blocking the communication with the malicious domain. In this paper a method for malicious domain detection using DNS traffic is presented. Features of DNS traffic are classified according to their ability of detection in previous works in this field. Samples of the detection algorithms are presented. An experimental study to verify the existance of fast-flux botnets is performed. An Experimental study based on simplest DNS traffic characteristics verified the existence of malicious domains.

Keywords: *botnet, DNS traffic, fast-flux*

1. Uvod

1. *Introduction*

U zadnjih desetak godina mreže kompromitiranih računala su evoluirale od mreža desetak zaraženih računala kontroliranih jednim napadačkim poslužiteljem u mreže milijuna računala sa decentraliziranom kontrolom.

Danas je uobičajeno da se adrese napadačkih poslužitelja skrivaju iza niza mrežnih adresa i naziva zona (postojećih i nepostojećih, ugrađenih

unutar nepoželjne programske podrške) kao i višestrukih razina referenci koje nastaju slijedom pretraživanja istih adresa.

Mreže sa sakrivanjem mrežnih adresa (engl. fast flux) prema definiciji ICANN-a (engl. Internet Coorporation for Assigned Names and Numbers) odnose se na mreže koje brzim i često ponovljivim promjenama osnovnog zapisa adrese (engl. DNS A record) i/ili adrese imeničkog poslužitelja (engl. DNS NS record) utječu na stalnu promjenu lokacije zone, odnosno mrežne adrese koja je poslužuje ili imeničkog poslužitelja koji je autoritativan za opis zone [1][4].

Uz izmjenu mrežnih adresa navedena tehnika koristi još jedno rješenje kojim osigurava anonimnost. Korisnik postavlja upit imeničkom poslužitelju i dobiva jednu ili niz adresa koje se rotiraju i pokazuju na jedno kompromitirano računalo. Kompromitirano računalo kontaktira pravi poslužitelj zloćudnog sadržaja i njegov odgovor proslijedi klijentu sakrivajući pravi izvor, odnosno prikazujući sebe kao izvor odgovora. Time kompromitirano računalo postaje posrednički poslužitelj (engl. proxy server) internet stranica. Na ovaj način se postiže anonimnost budući da je nemoguće otkriti točnu lokaciju poslužitelja zloćudnog sadržaja, a brzom rotacijom posredničkih poslužitelja praktički je nemoguće blokirati postavljenu zonu.

Analiza imeničkog prometa danas se predstavlja kao efikasna tehnika za otkrivanje mreže kompromitiranih računala, naročito onih koje primjenjuju metode skrivanja iza mrežnih adresa ili naziva zona. Postoje anomalije u imeničkom prometu čija pojava karakterizira postojanje mreže kompromitiranih računala. Analizom karakteristika imeničkog prometa moguće je otkrivanje mreže kompromitiranih računala koji koriste metodu skrivanja iza mrežnih adresa .

U drugom poglavlju ovoga rada spomenuti su parametri imeničkog prometa koji sadrže anomalije za otkrivanje mreže kompromitiranih računala dok su u trećem poglavlju navedeni primjeri algoritama otkrivanja mreže kompromitiranih računala. U četvrtom poglavlju naveden je primjer ispitivanja postajanja mreža kompromitiranih računala koncipiranih na skrivanju adresa.

2. Parametri otkrivanja mreže kompromitiranih računala analizom imeničkog prometa

2. *Botnet detection DNS traffic characteristics*

Za otkrivanje mreže kompromitiranih računala najpogodniji je imenički protokol (engl. Domain Name System-DNS). Sva komunikacija na internetu započinje kroz upit imeničkom poslužitelju budući da primarno koristimo imena za komunikaciju. Kod tehnike sakrivanja mrežne adrese, mreže kompromitiranih računala prisiljena su koristiti nazive zona za kontakt kompromitiranog računala sa napadačkim poslužiteljem. Mrežne adrese se ne mogu koristiti jer u trenutku prevođenja zloćudnog programa iste nisu poznate. U tom trenutku ne može se znati koja će računala biti u budućnosti osvojena u mrežu kompromitiranih računala i preuzeti ulogu posredničkog servisa.

U radu za razmatranje otkrivanja kompromitiranih mreža korištene su karakteristike vezane uz ime zone, dostupnost zone kojoj pripada, različitost mrežnih adresa koje poslužuju zonu temeljem dosadašnjih radova iz toga područja. Prikaz karakteristika dan je tablicom.

Tablica 1. *Prikaz karakteristika vezane uz ime zone, dostupnost zone kojoj pripada, različitost mrežnih adresa koje poslužuju zonu*

Table 1. *Characteristics of the zone name, the availability of the zone to which it belongs, the diversity of network addresses that serve the zone*

Naziv karakteristika	**Opis karakteristika**	**Literatura**
K1 Starost zone	Uobičajene zone imaju dugi vijek trajanja. zloćudne zone kada se otkriju vrlo brzo dospiju na liste nepoželjnih zona koje blokiraju vatrozidi aplikacijskog sloja ili ih registri sami zatvore po prijavi	[2]

K2-Mjesto registracije zone (Registar)	Uglavnom se radi o zemljama koje nemaju razvijene zakone vezane uz računalni kriminal.	[2]
K3-Broj pod zona navedene zone	Mreže kompromitiranih računala da bi određenu zonu učinili iskoristivom kreiraju pod zone koje prvo oglašavaju	[8]
K4-Naziv zone	Postojanje određene vjerojatnosti da je ime zone slučajno generirano povećava vjerojatnost da se radi o mrežnom odredištu koje provodi prijevaru.	[8]
K5-Sličnost određenih elemenata naziva zone sa valjanim nazivima domena	Postoje određene riječi koje su česte u nazivima zona sa prijevarom (engl. phishing site).	[8]
K6-Vrijeme i trajanje zahtjeva prema zoni	Dokazano je da mreže kompromitiranih računala imaju kratke periode intenzivnog rada u kojemu obavljaju komunikaciju sa upravljačkim računalom.	[2]
K7-Slično dnevno ponašanje zone	Uz uvjet da nadziremo promet u vremenskim okvirima možemo očitati ponašanje zone u nekom vremenskom okviru.	[9]
K8-Stalni ponavljajući ciklusi upita prema imeničkom poslužitelju zone	Analizom broja zahtjeva prema određenim imeničkim poslužiteljima.	[2-10]
K9-Broj jedinstvenih zapisa adresa (DNS A zapisa) vraćenih na upit	Normalne stranice uglavnom će vratiti jedan do maksimalno tri zapisa adrese na upit za mrežnu adresu zone (DNS A zapis). Kod kompromitiranih mreža računala mrežne adrese su adrese komprimiranih klijenata.	[4][6][7]
K10-Tempo rasta broja zapisa adresa	U nekom vremenskom razdoblju za određenu domenu može doći do povećanja ili stabilnosti broja mrežnih adresa	[6]
K11-Vrijeme zadržavanja mrežne adrese u zapisu zone	Mreže kompromitiranih računa često rotiraju mrežne adrese	[5]

K12-Vrijeme dozvoljenog ponovnog upita prema autoritativnom zapisu	Kompromitirane mreže koje imaju probleme sa ispadima imeničkih poslužitelja tu vrijednost postavljaju na minimalnu	[2][4][5] [8]
K13-Vrijeme života imeničkih zapisa	Kompromitirane mreže računala upravo zbog nepouzdanosti svojih zaraženih klijenata kao i ostvarenja težeg blokiranja mreže kroz liste zaraženih adresa često imaju potrebe izmjena mrežnih adresa za zonu koju poslužuju	[4]
K14-Dostupnost zone	Provjerom slijednosti sadržaja i dostupnosti stranice u nekom vremenskom periodu moguće je potvrditi zloćudnost stranice	[10]
K15-Mrežno kašnjenje zone	Uzevši u obzir da većina mreža kompromitiranih računala koristi svoja računala kao posrednike za dostavu informacija, veza je sporija u odnosu na vezu klijenta sa poslužiteljem.	[10]
K16-Izračun vremena procesiranja na poslužitelju	Mjereći vrijeme dolaska i oduzimajući mu vrijeme mreže dolazimo do performansi posredničkog računala.	[2]
K17-Različitost adrese mreže zapisa mrežnih adresa vraćenih na upit	Kod mreže za distribuciju adrese potječu iz različitih mreža sa ciljem da poslužitelj bude što bliže klijentu što je svojstveno i kod mreže kompromitiranih računala.	[4][5]
K18-Izvedena karakteristika za udaljenost vraćenih mrežnih adresa	Radi jednostavnosti izračunavanja može se primijeniti logika udaljenosti dvije mreže.	[2-5][7]
K19-Različitost autonomnih sustava zapisa mrežnih adresa vraćenih na upit	Kod mreža kompromitiranih računala nije moguće izabrati klijente pa tako broj različitih autonomnih sustava raste	[7]
K20-Tempo rasta broja različitih autonomnih sustava	Kod kompromitiranih mreža broj promjena adresa će biti veći, kao što će nove adrese biti uglavnom udaljene od prethodnih.	[3]

K21-Broj jedinstvenih zapisa adresa imeničkih poslužitelja vraćenih na upit	Uobičajene stranice uglavnom su povezane sa zonom preko jednog imeničkog poslužitelja, a mreže kompromitiranih računala mijenjaju imenički poslužitelj zone čime sprječavaju njegovu blokadu	[3][5][8]
K22-Broj zapisa adresa imeničkih poslužitelja iz različitih autonomnih sustava vraćenih na upit	Kod mreža kompromitiranih računala imenički poslužitelji također mogu biti računala iz kompromitirane mreže radi težeg blokiranja navedene mreže.	[5]
K23-Broj različitih punih imena zona dobivenih na inverzni upit mrežne adrese	Bez obzira na raspodijeljenost računala na internetu i dalje određena kompanija može biti vlasnik svih tih navedenih adresa.	[2][4]
K24-Broj različitih imena mreža	Višestruke adrese mreža mogu biti grupirane u jedno mrežno ime od strane registratora, što je jedan od parametara za prepoznavanje mreže kompromitiranih računala	[2]
K25-Broj različitih organizacija vlasnika mreža	Raspodijeljeni posrednički poslužitelji mreže kompromitiranih imati će različite organizacije u kojima se nalaze poslužitelji	[2]
K26-Broj različitih država kojima pripadaju mreže	Ilegalne mreže distribuirane na kompromitirana računala pripadati će različitim državama koje često neće imati nikakvo srodstvo sa materijalima koji se poslužuju	[4]
K27-Naziv rezervnog imena za mrežnu adresu	Kompromitirana računala često pripadaju kućnim korisnicima.	[4][7]
K28-Preklapanje između mrežnih adresa i adresa imeničkih poslužitelja	Mreža kompromitiranih računala sastoji od velikog broja kompromitiranih računala	[6]

3. Algoritmi otkrivanja mreže kompromitiranih računala

3. *Botnet detection algorithms*

Primarno svaka od opisanih karakteristika se može izvesti pohranjivanjem realnih činjenica ili aproksimacijom kroz Bayesov algoritam ili neku drugu matematičku aproksimaciju temeljem dovoljnog broja ulaznih informacija po kojima će se odrediti pragovi ili konstante određene matematičke funkcije. U dosadašnjim radovima cilj je bio dokazati mogućnost otkrivanja mreže kompromitiranih računala primarno kroz naknadnu statističku analizu karakteristika

Neka od najčešćih rješenja su:

- Prema [3] parametri se uobličuju u vektor x . Temeljem vektorskog prostora izrađuje se linearna funkcija odluke: $f(x) = w^T x = w_1 k_9 + w_2 k_{19} + w_3 k_{21}$ gdje w_1, w_2, w_3 su težinski faktori određeni temeljem ulaza za učenje, a k predstavlja karakteristike opisane u poglavlju 4.1. Vrijednost funkcije se uspoređuje sa pragom koji odlučuje da li se radi o zloćudnoj domeni sa sakrivanjem mrežnih adresa.
- Prema [2] temeljem karakteristika *k1,k2,k9,k13,k17,k19,k23,k25* izvodi se Bayesova filtracija.
- Prema [4] promet se filtrira sa ciljem smanjenja volumena. Stvaraju se liste aktivnih zona. Temeljem karakteristika *k9,k13,k14,k18,k19,k23,k26,k27* izvodi se C4.5 algoritam (engl. C4.5 Decision tree-algorithm).
- Prema [6] i [7] temeljem karakteristika *k9,k10,k11,k28* izrađen je vlastiti algoritam za odlučivanje baziran na SVM klasifikatoru (engl. Support Vector Machine).
- Prema karakteristike *k3,k4,k5,k6,k9,k13,k21* čine ulaz u k-means clustering algoritam.
- Prema [8] primjenom karakteristike *k8* kroz graf zona izvodi se analiza mogućih zloćudnih zona.
- Prema [10] analizom karakteristika *k15* i *k16* kroz duljinu trajanja zahtjeva moguće je donijeti prevagu u odlučivanju kroz usporedbu kašnjenja klasične zone i zone koja se poslužuje kroz mrežu kompromitiranih računala.

Postoji trend usavršavanja karakteristika koje poboljšavaju otkrivanje kompromitirane mreže i adrese napadačkog poslužitelja. Analiza podataka iz prošlosti nije učinkovita s obzirom na to da se navedene mreže često prilagođavaju pa time otkriveni podaci ne vode do otklanjanja problema.

4. Analiza mogućnosti otkrivanja mreže kompromitiranih računala

4. *Botnet detection analysis*

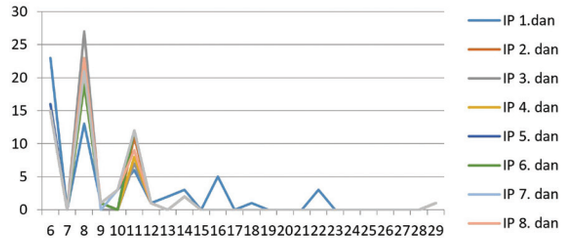
U jednom od osnovnih radova [3] u navedenom području temeljem baze neželjene elektroničke pošte prikupljene u periodu od dva mjeseca tijekom 2007. od 22264 popisanih mrežnih veza (engl. hyperlink) utvrđeno je postojanje 2197 (29.7%) zloćudnih domena koje su posluživale mreže kompromitiranih računala sa tehnikom sakrivanja mrežne adrese. Slično istraživanje provedeno 2006. godine je zabilježilo 6% takvih zona.

Radi istraživanja sakupljeno je 57022 naziva zona. U istraživanju su promatrane dvije karakteristike k9 i k22. Karakteristika k9 opisuje broj vraćenih zapisa mrežnih adresa na upit za mrežnu adresu zone. Upit se postavljao lokalnom imeničkom poslužitelju koji je obavljao proces rezolucije. Za svaku mrežnu adresu dobivenu upitom ispitivao se autonomni sustav kojem oba pripadaju. Autonomni sustav dobiva se analizom vanjskog usmjerničkog protokola (engl. Border Gateway Protocol – BGP). Temeljem dobivenih podataka utvrđivala se karakteristika k22. Ona opisuje broj različitih autonomnih sustava za mrežne adrese dobivene upitom za mrežni naziv zone.

Mjerenja su ponavljana svaki dan kroz period od devet dana. Razmaci između pojedinih mjerenja su bili veći od osamnaest sati kako bi se spriječio utjecaj međuspremnika na dobivene podatke. Budući da želimo utvrditi postojanje kompromitiranog računala unutar mreže možemo pretpostaviti da je kod takvih mreža vrijeme međuspremnika ispod osam sati [2]-[10]. Zalihu od dodatnih deset sati treba osigurati dobivanjem novog podatka. Mjerenje se izvodilo sa jedan do dva sata razlike u odnosu na vrijeme mjerenja u prethodnom danu. Navedeno treba osigurati da mreža kompromitiranih računala ne bi posumnjala da se aktivno ispituje njezino postojanje.

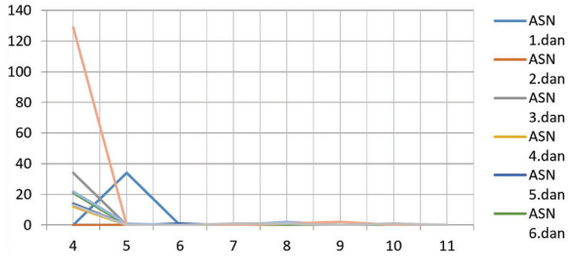
Nakon svakoga mjerenja podaci su grupirani sukladno broju vraćenih istih podataka. Graf 1. prikazuje rezultate po danima (svaki dan je zasebna krivulja), dok graf 3. prikazuje izvještaj za svih devet dana mjerenja. Na horizontalnoj osi nalazi se broj različitih adresa (element po kojem je grupiranje obavljeno), a na vertikalnoj osi broj zona za koje je upit vratio navedeni broj adresa. Prema radovima [3]-[10] na grafovima su prikazane zone čiji je broj vraćenih mrežnih adresa veći od pet i broj različitih autonomnih sustava za te adrese veći od tri.

Takvi parametri se smatraju dovoljnim da se može pretpostaviti postojanje mreže za posluživanje sadržaja ili mreže kompromitiranih računala.



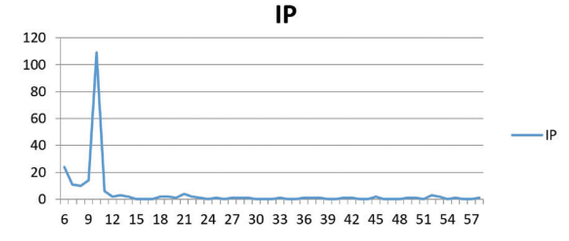
Graf 1 *Ovisnost o broju različitih zapisa vraćenih mrežnih adresa zone prema danima mjerenja*

Graph 1 *Dependence on the number of different records of returned network address zones by date of measurement*



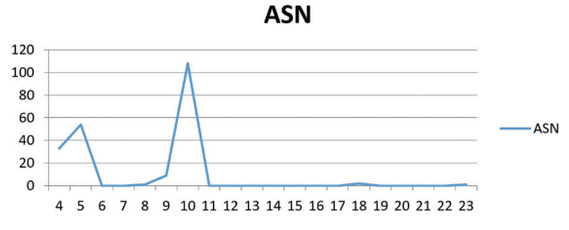
Graf 2 *Ovisnost o broju različitih autonomnih sustava vraćenih mrežnih adresa zone prema danima mjerenja*

Graph 2 *Dependence on the number of different autonomous systems of returned network address zones by date of measurement*



Graf 3 *Ovisnost o broju različitih vraćenih mrežnih adresa zone u devet dnevnom razdoblju mjerenja*

Graph 3 *Dependence on the number of different returned network address zones in nine daily measurement periods*



Graf 4 *Ovisnost o broju različitih autonomnih sustava vraćenih mrežnih adresa zone u devet dnevnom razdoblju mjerenja*

Graph 4 *Dependence on the number of different autonomous systems of returned network address zones in nine daily measurement periods*

Temeljem dobivenih podataka utvrđene su 10833 zone koje koriste tehnologiju posluživanja kroz više mrežnih adresa odnosno 20,3% u odnosu na ukupan broj promatranih zona. Od toga broja više od 5 mrežnih adresa koristi 214 zona ili 0,4%. Navedeni podatak se sastoji od zona koje su uobičajene (Google, Amazon, Yahoo) i zona koje drže mreže kompromitiranih računala.

Navedena mjerenja provedena su nad nazivima zona dobivenih od mrežnih veza sakupljenih iz baze neželjene elektroničke pošte kao i nazivima zona koje su se pojavile u prometu imeničkog poslužitelja Tehničkog veleučilišta u Zagrebu tijekom istraživanja.

Prema radovima [2][3][10] iz navedenih mjerenja možemo zaključiti da postoje mreže kompromitiranih računala koje koriste tehnologiju skrivanja mrežne adrese.

5. Zaključak
5. *Conclusion*

Upravljanje mrežom kompromitiranih računala danas je složen problem. Napadači su zamijenili nekadašnje jednostavne komunikacijske kanale IRC (Internet Relay Chat) novim modernim kanalima kao što su internetske stranice (http), Facebook, elektronička pošta, dodatni unos zapisa u imeničku zonu i drugo. Otkrivanje prisluškivanjem određenog pristupa (eng.port) ne donosi zadovoljavajuće rezultate u otkrivanju takve mreže. Radi sprječavanja lakog blokiranja mreže kompromitiranih računala razvijene su metode skrivanja putem mrežnih adresa i imena domena koje se danas primjenjuju za prikrivanje napadačkih poslužitelja.

Danas većina komunikacije zahtjeva upit imeničkom poslužitelju, a otkrivanje kompromitirane mreže omogućeno je analizom anomalija u tom prometu.
Za otkrivanje mreže kompromitiranih računala moguće je iskoristiti karakteristiku unutar mreže, primjerice učestalost upita prema adresama i zonama koje se nalaze unutar mreže davatelja usluge iz različitih autonomnih sustava. Takve mreže učestalo se prilagođavaju mogućim otkrivanjima mijenjajući svoje adrese i položaj. Time postaje važan parametar brzina otkrivanja.

Za provjeru postojanja mreže kompromitiranih računala uzet je podatak o broju vraćenih mrežnih adresa na upit zone i broj vraćenih različitih autonomnih sustava dobivenih mrežnih adresa. Za ulazne parametre nazivi zona su dobiveni iz dva izvora: baze neželjene elektroničke pošte i prometa imeničkog poslužitelja Tehničkog veleučilišta u Zagrebu u periodu od devet uzastopnih dana određene su zone koje po karakteristikama možemo proglasiti dijelom kompromitirane mreže računala tijekom provedenog istraživanja.

6. REFERENCE

6. *REFERENCES*

[1.] L. Gasster, GNSO Issues Report on Fast Fluxing Hosting, ICANN, 2008.

[2.] Emanuele Passerini , Roberto Paleari , Lorenzo Martignoni , Danilo Bruschi, FluXOR: Detecting and Monitoring Fast-Flux Service Networks, Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment, July 10-11, 2008, Paris, France

[3.] Holz, T., Corecki, C., Rieck, K., Freiling, F.C.: Measuring and Detecting Fast-Flux Service Networks. In: NDSS (February 2008)

[4.] Roberto Perdisci , Igino Corona , David Dagon , Wenke Lee, Detecting Malicious Flux Service Networks through Passive Analysis of Recursive DNS Traces, Proceedings of the 2009 Annual Computer Security Applications Conference, p.311-320, December 07-11, 2009.

[5.] Nazario, J. Holz, T. ,As the net churns: Fast-flux botnet observations, Malicious and Unwanted Software, 2008. MALWARE 2008. 3rd International Conference on,7-8 Oct. 2008.

[6.] X. Hu, M. Knysz, and K. Shin, Measurement and analysis of global ipusage patterns of fast-flux botnets, in INFOCOM, 2011 Proceedings IEEE.IEEE, 2011, pp. 2633-2641.

[7.] X. Hu, M. Knysz, and K. G. Shin. RB-Seeker: Auto-detection of Redirection Botnets. In Proc. of 16th NDSS, 2009.

[8.] Marchal, S., Francois, J. ; Wagner, C. ; State, R. ; Dulaunoy, A. ; Engel, T. ; Festor, O. DNSSM: A large scale passive DNS security monitoring framework, Network Operations and Management Symposium (NOMS), 2012 IEEE,2012

[9.] Lee Jehyun, Kwon Jonghun, Shin Hyo-Jeong and Lee Heejo, "Tracking multiple C&C botnets by analyzing DNS traffic," Secure Network Protocols (NPSec), 2010 6th IEEE Workshop on, pp. 67 -72

[10.] Ching-Hsiang Hsu, Chun-Ying Huang, Kuan-Ta Chen, Fast-flux bot detection in real time, Proceedings of the 13th international conference on Recent advances in intrusion detection, 2010.

AUTORI · *AUTHORS*

Brigitta Cafuta
Rođena u Zagrebu 1977. godine. Diplomirala je 2017. godine na Ekonomskom fakultetu u Zagrebu, u istoj godini upisuje doktorskih studij na Ekonomskom fakultetu u Zagrebu. Zaposlena na Tehničkom veleučilištu u Zagrebu u zvanju asistenta na kolegijima: Operacijski sustavi, Baze podataka, Elektroničko poslovanje i Tržište i poslovno okruženje.

Bojan Nožica - nepromjenjena biografija nalazi se u časopisu Polytechnic & Design
Vol. 7, No. 1, 2019.

Ivica Dodig - nepromjenjena biografija nalazi se u časopisu Polytechnic & Design
Vol. 5, No. 1, 2017.

Tin Kramberger - nepromjenjena biografija nalazi se u časopisu Polytechnic & Design
Vol. 5, No. 1, 2017.

Korespondencija
bcafuta@tvz.hr
bnozica@tvz.hr
idodig@tvz.hr
tkramberger@tvz.hr