MALWARE ANALYSIS PADA WINDOWS OPERATING SYSTEM UNTUK MENDETEKSI TROJAN

MALWARE ANALYSIS ON WINDOWS OPERATING SYSTEM TO DETECT TROJAN

Sabam Chandra Yohanes Hutauruk[1], Fazmah Arif Yulianto[2], Gandeva Bayu Satrya[3]

Fakultas Informatika, Universitas Telkom, Bandung

[1]chandrayohanes@live.com, [2]fazmah@telkomuniversity.ac.id, [3]gandeva.bayu.s@gmail.com

Abstrak

Salah satu tren yang mengikuti perkembangan masa adalah jenis - jenis *malware* yang muncul di dunia maya semakin beragam. Trojan adalah salah satu jenis *malware* yang ikut berkembang di dalamnya, yang memungkinkan *attacker* masuk ke dalam sistem tanpa diketahui oleh pemilik. Penggunaan *trojan* saat ini lebih ke arah kejahatan dunia maya (*cyber crime*). Cara kerja *trojan* yang cepat dan handal menjadi penyebab penggunaan *trojan* semakin marak dalam dunia kejahatan komputer. Sasaran terbanyak penyebaran *trojan* adalah pengguna sistem operasi Windows. Jumlah pengguna dan penyedia aplikasi di internet yang banyak, memungkinkan penyebaran *trojan* ini dilakukan dengan metode *social-engineering*, teknik yang menggunakan kelemahan manusia, sehingga user tanpa curiga langsung mengeksekusi sebuah *program* yang tidak dikenal.

***Malware analysis* adalah metode untuk mengetahui keberadaan *malware* (*malicious software*) dalam suatu *executable file* yang dibagi dalam dua buah tahap yaitu *static analysis* dan *dynamic analysis*. *Static analysis* dilakukan tanpa menjalankan *malware* tersebut ke dalam sistem seperti *disassembly* dan *debugging*, sedangkan *dynamic analysis* dilakukan dengan menjalankan *malware* dalam sistem untuk melihat *process detail*, *file system activity*, *registry activities*, dan *network traffic*. Dengan menggabungkan hasil dari *static malware analysis* dan *dynamic malware analysis* diperoleh karakteristik malware yang dijadikan data rekomendasi untuk mendeteksi keberadaan *trojan malware* pada *executable file* Windows.**

Kata Kunci: *Trojan, social engineering, malware analysis, executable file*

Abstract

One of the trend that follows the development period is the increasing appearance of various malwares in the internet. Trojan is a type of malware that also grows rapidly, it allows the attacker to login to the victim's system without being noticed. The use of trojan is currently moving toward cybercrime. Being fast and reliable, trojan spreads in the world of computer crime. Most trojan targets are Windows OS users. The high number of users and application providers on the internet, allows it to spread by social-engineering technique, a technique that uses human weakness that will drive the victim to download and execute that unknown program.

Malware analysis is a method to analyzing malware that is divided into two steps, static and dynamic analysis. Static analysis is done without running the malware in to the system such as disassembly and debugging, meanwhile dynamic analysis is done by running the malware in the system to see the process detail, file system activities, registry activities, and network traffic activities. Combining the results of static and dynamic analysis will produce malware's characteristic as recommendation to detect trojan malware inside windows executable file.

Keyword: *trojan, social-engineering, malware analysis, executable file*

1. Pendahuluan

Teknologi memberikan adalah tantangan dan menjadi ancaman bagi pengguna internet di dunia. Tingginya penyebaran internet menciptakan kejahatan tak hanya terjadi dalam dunia nyata, tetapi merambah ke dunia maya yang sering disebut sebagai *cyber crime*. Salah satu bentuk dari kejahatan ini adalah penyebaran *trojan* yang berupa *malicious software (malware)* dengan begitu mudah. Dalam proses penyebaran ini pelaku kejahatan menggunakan teknik dengan memanfaatkan sisi kelemahan manusia yang biasa disebut dengan *social engineering.* Karena *trojan ini berbeda dengan virus* yang memiliki sifat dapat menggandakan diri setelah dieksekusi korban [16]. Dalam penyebaran *trojan*, korban dikelabuhi menginstal perangkat lunak berbahaya ini melalui *addon* pada *advertise*, atau pun melalui email yang dikirim kepada korban. Target yang paling banyak dari penyebaran *trojan* adalah para pengguna *Windows Operating System*, karena pengguna jenis sistem operasi ini adalah terbanyak untuk saat ini [13]. Setelah korban mengeksekusi *malware* ini, maka *trojan* langsung membuka jalur untuk

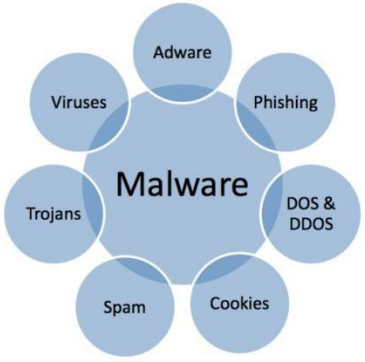
berkomunikasi dengan penyerang untuk masuk dan dikontrol melalui *C&C* milik penyerang.

Tujuan dari malware analysis yang dilakukan pada *malware* jenis *trojan* ini adalah untuk menghasilkan data karakteristik *trojan* dan menganalisis siklus hidup masing – masing jenis *trojan sample* (Bozok, Blackshades, Darkcomet, njRAT) pada *Windows Operating System*. Untuk melakukan *malware analysis* dilakukan metode penelitian berupa studi literature berupa pendalaman materi yang berhubungan dengan *malware analysis.* Selanjutnya adalah analysis dan perancangan simulasi jaringan. Kemudian melakukan implementasi pada sistem yang telah dirancang dan melakukan pengujian pada tiap *trojan sample* yang telah diberikan terhadap sistem. Setelah itu dilakukan analisis pada hasil pengujian dengan tiap skenario yang diajukan setelah mendapatkan hasil untuk ditarik sebagai kesimpulan.

2. Dasar Teori

2.1 Trojan

Trojan mengacu pada pada *malicious software (malware)* yang menginfeksi korban dengan mengambil hak akses *administrar* pada Windows OS. Dengan membuka akses *port* pada komputer memberikan penyerang untuk melakukan *remote* pada komputer dari jarak jauh. Konsep awal dari *trojan* ini adalah penggunaan RAT (*Remote Administration Tool)* yang biasa digunakan untuk melakukan remote pada komputer dimana telah terjadi kesepakatan permission terhadap akses yang diberikan. *Trojan sample* yang diberikan pada adalah jenis yang dapat melakukan *remote* melalui jarak jauh yang sering disebut sebagai *Remote Access Trojan [5].* Lain hal dengan apa yang dilakukan *trojan*, dalam kondisi ini tidak ada terjadi kesepakatan dalam penggunaannya, dan inilah yang dapat menjadi hal yang merugikan bagi korban yang sering mengarah pada kejahatan. *Trojan* tidak termasuk dalam keluarga virus, karena tidak dapat menggandakan diri.



Gambar 2.1 *Trojan* berbeda dengan *virus* [15].

2.1.1 Jenis – jenis trojan

Karena beragam jenis dan fungsinya, *trojan* dapat dikelompokkan dalam kategori sebagai berikut [4]:

a. Backdoor
Trojan yang sering digunakan dengan komputer yang sama – sama sebagai korban untuk membentu *botnet* pada jaringan yang bertujuan sama untuk melakukan tindak kriminal.

b. Exploit
Exploit adalah program yang mengandung data atau code yang menggunakan *vulnerability application software* yang ada pada komputer korban seperti *flash, adobe reader*

c. Rootkit
Dirancang untuk menyembunyikan objek atau aktivitas dalam sistem. Dirancang untuk menghalangi *malicious code* tidak bisa dihapus, sehingga dapat hidup dan lebih lama menginfeksi.

d. Trojan – Banker
Trojan – Banker adalah program yang dirancang untuk mencuri data aku *online banking system, e-payment* berupa *credit card* dan *debit card.*

e. Trojan – DDOS
Merupakan lanjutan dari *trojan backdoor,* digunakan untuk melumpuhkan sistem, seperti *webserver,* dengan mengirimkan *muliptle request,* dari komputer korban dan komputer yang lainnya.

f. Trojan – Downloader
Jenis *trojan* ini dapat mengunduh dan menginstal versi baru dari *malicious program* pada komputer korban, termasuk memperbaharui jenis *trojan* itu sendiri.

g. Trojan – Dropper
Program jenis ini sering digunakan untuk menghindari deteksi antivirus

h. Trojan – FakeAV
Jenis ini melakukan simulasi seperti *software antivirus.* Bertujuan untuk mengambil uang dari koban dengan cara menipu korban bahwa komputer korban terinfeksi virus, padahal belum tentu ada bagian sistem yang terinfeksi.

i. Trojan – GameThief
Dapat berupa progam yang mencuri *user account information* dari pemain *game online.*

j. Trojan – IM
Trojan jenis ini mencuri data *login* dan *password program* pesan instan seperti *Live Messenger, AOL IM, Yahoo! Messenger, Skype,* dan lainnya.

k. *Trojan – Ransom*
Tipe *trojan* ini dapat melakukan modifikasi pada data komputer yang terinfeksi, sehingga data tersebut tidak dapat dibuka, kecuali korban membayar sejumlah uang yang diminta oleh peyerang.

l. Trojan – SMS
Jenis *trojan* ini merugikan dalam hal uang berupa mencuri nilai kredit pulsa yang dimiliki korban dengan mengirim pesan *request* sms ke nomor premium seperti 0899, 6288 dsb

m. Trojan – Spy
Bertujuan untuk memata – matai bagaimana dan apa yang sedang dilakukan oleh korban pada komputer yang terinfeksi, dengan mengambil *screenshot* atau melihat *running application* pada komputer korban.

n. Dan tipe lain dari *trojan*

- *Trojan – Arcbomb*
- *Trojan – Clicker*
- *Trojan – Notifier*
- *Trojan – Proxy*
- *Trojan - PSW*

2.1.2 Prinsip kerja trojan

Cara bagaimana *trojan* bekerja adalah dengan membukan jalur koneksi dari komputer yang terinfeksi ke penyerang. Data mengalir dari dua arah yakni dari korban dan penyerang dengan menggunakan *well – known protocol* dan *unusual port* untuk terhubung dengan korban.

2.1.3 Comunication protocol

Agar dapat terhubung, *trojan* memliki struktur bagian *attacker, victim,* dan server [2], dengan menggunakan protocol *TCP/IP* agar tetap terhubung dengan *server* yang memungkinkan *Command* and *Control* membentuk komunikasi dan mengirimkan command pada sejumlah besar *client* yang terhubung dengan *attacker.*

2.2 Malware

Malware (malicious software) adalah perangkat lunak yang dapat mengganggun kirnerja sistem operasi computer seperti mencuri informasi data sensitif dan melakukan remote pada Komputer korban tanpa seizin pemilik. *Malware* ada dalam berbagai bentuk seperti *script, code, active content,* dan perangkat lunak [11].

2.2.1 Jenis Malware

Menurut buku *Pratical Malware Analysis [16]*, *malware* dapat dikategorikan sebagai berikut:

a. *Backdoor: Malicious code* yang melakukan instalasi pada sebuah komputer agar penyerang dapat mengakses komputer tersebut, tanpa proses autentikasi.

b. *Botnet:* serupa dengan backdoor, memungkinkan penyerang tunggal mengakses ke system komputer, dan dapat dikontrol dari C&C.

c. *Downloader: malicious code* yang berfungsi sebagai pengunduh *malicious code* yang lain.

d. *Information stealing:* Jenis *malware* yang mengumpulkan informasi dari korbannya, misalnya *password hash grabber, sniffer* dan *keylogger.*

e. *Launcher*: *Malicious code* yang digunakan untuk menjalankan *malware* lain.

f. *Rootkit: Malicious code* yang didesain untuk menyembunyikan *malware* lain misalnya *backdoor*

g. *Scareware*: *Malware* yang didesain untuk menakuti *user*, seakan – akan perangkat *user* terinfeksi *virus,* lalu diinstruksikan untuk mengunduh program tertentu sebagai *antivirus* yang ternyata adalah *malware.*

h. *Spam – sending malware: Malware* yang menginfeksi computer lain dan mengirimkan *spam.*

i. *Virus atau worm: Malware* yang sifatnya dapat memperbanyak dirinya dan menginfeksi komputer lain.

2.3 Malware Analysis

Malware analysis: kumpulan dari proses penentuan tujuan dan fungsionalitas dari *sample malware* yang diberikan seperti *virus, worm, trojan,* dan sebagainya untuk melakukan deteksi *malicious code.* Baik dengan mengeksekusi malware tersebut (*dynamic analysis)* ataupun denga menginspeksi kode program saat sebelum dieksekusi [8] [13].

3. Perancangan Sistem

3.1 Implementasi Jaringan

Jaringan yang akan dibuat terdiri dari computer yang bersi 4 buah virtual machine yaitu *attacker*, *victim*, *server* dan *mikrotik router* dengan perangkat inputan mouse dan keyboard.

3.2 Tujuan Pengujian

Setiap pengujian yang dijalankan harus mempunyai tujuan agar sesuai dengan skenario yang diterapkan. Berikut adalah tujuan yang akan dicapai:

1. Mendapatkan informasi bagaimana *malware analysis* pada *executable file* (.exe) *trojan* pada Sistem Operasi Windows untuk mendeteksi *malware* jenis *trojan* [4].
2. Mendapatkan informasi untuk membuat data rekomendasi untuk mendeteksi *malware* jenis *trojan* pada Sistem Operasi Windows.

3.3 Skenario Pengujian

Dalam mencapai tujuan yang dipaparkan, diperlukan beberapa skenario, dengan menyiapkan 4 buah sample *trojan malware* yang paling sering digunakan dalam berbagai kasus *cybercrime* yang terungkap di dunia maya. Sample yang disediakan tersebut akan dibedah dengan menggunakan skenario – skenario yang dibagi menjadi 2 bagian yaitu *static malware analysis* dan *dynamic malware analysis* [10].

3.3.1 Static Malware Analysis

Static malware analysis dilakukan tanpa mengeksekusi sample *trojan*, dengan skenario sebagai berikut: *File finger printing by hashing* menggunakan *tool*: *hashmyfiles, Extraction of hard coded string* menggunakan *tool*: *ShowString, Disassembly* menggunakan *tool*: IDA Pro 5, *Extract linked libraries and function* menggunakan *tool: Dependency Walker, Debugging* dengan menggunakan *tool*: Ollydbg.

3.3.2 Dynamic Malware Analysis

Dynamic malware analysis adalah pengamatan perilaku dari sample *trojan* setelah dieksekusi dalam sistem, mulai dari interaksi terhadap jaringan, perilaku *persistence system.* Berikut adalah scenario yang digunakan seperti *Viewing process detail* dengan menggunakan tool: *process explorer*, *File System Activity Monitoring* dengan menggunakan tool: *Sysinternal Process Monitor, Registry activities monitoring* dengan menggunakan tool: *Sysinternal autoruns,* dan *Network Traffic Monitoring* dengan menggunakan *tool*: *wireshark.*

4. Analisis Pengujian dan Implementasi

Dalam bab ini dibahas hasil analisa jenis *trojan* yang telah dilakukan pada bab sebelumnya.

4.1 Hasil Pengujian Malware Analysis

4.1.1 Hasil pengujian static malware analysis

Dari hasil pengujian static malware analysis didapatkan informasi yang disimpulkan adalah kode – kode program yang akan masuk apabila dieksekusi ke dalam sistem. Informasi berisi tentang *hash trojan sample.* Informasi proses pengaktifan *trojan* dapat berupa infeksi, perubahan pada registry, perekam informasi *keystroke (keylogger),* koneksi ke luar sistem untuk update dan download, serta melakukan uninstall dari sistem yang terinfeksi.

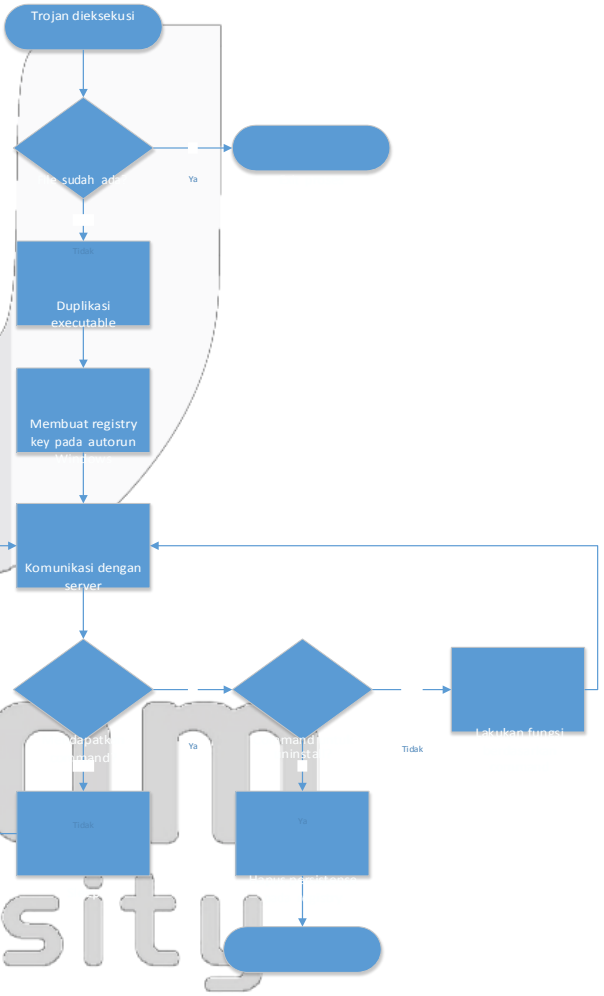
4.1.2 Hasil pengujian dynamic malware analysis

Dari hasil pengujuan dynamic analysis didapat informasi mengenai

- process detail dimana tidak satu pun dari sample yang memiliki *verified signature*
- terdapat *file* hasil duplikasi running sebagai *file system activities*
- terdapat perubahan pada *registry* sebagai mekanisme untuk mempertahankan diri (*persistence)* agar file system yang ditanam bisa *running* saat *startup system*
- terdapat pertukaran infromasi dari komputer korban menuju *C&C attacker*,

4.2 Kombinasi hasil Pengujian Static Analysis dan Dynamic Analysis

Dari hasil dari pengujian static analysis dan dynamic analysis dapat digabungkan hasilnya dalam model bagaimana siklus hidup sebuah *trojan* ketika menginfeksi sebuat sistem.



Gambar Siklus hidup *trojan*

Berikut adalah penjelasan dari *flow chart* di atas:

- *Trojan* dieksekusi: ada pengecekan apakah apakah ada *trojan* dengan *mutex* yang sama *running* dalam sistem
- Duplikasi executable: mekanisme mempertahankan diri (*persistence)* proses nya

melakukan *selfduplicate file trojan* tersebut ke dalam salah satu user folder

- Membuat registry key pada autorun Windows: mekanisme *persistence* berikutnya, agar *trojan* tetap *running* walaupun sistem telah di *reboot* oleh user.
- Komunikasi dengan server: melalui protokol *TCP/IP*
- Periksa command: untuk melakukan fungsionalitas sesuai permintaan *attacker* melalui *C&C*

4.3 Data rekomendasi pendeteksian Trojan

Dari data yang dihasilkan pada pengujian bab 4.1 dan bab 4.2 dibuat rekomendasi untuk mendeteksi *trojan* sebagai berikut:

Tabel Data Karakteristik *Trojan*

No	Kriteria	bozok	blackshad	darkcome	njRAT
1	**Tidak memiliki *verified signature***	✓	✓	✓	✓
2	**Memiliki kemampuan untuk melakukan *self file duplication***	✓	✓	✓	✓
3	**Memiliki *keylogger***	✓	✓	✓	✓
4	**Memiliki kemampuan untuk menambahkan *autorun registry* pada sistem**	✓	✓	✓	✓
5	**Memiliki kemampuan untuk *remote* perubahan *registry***	✓	✓	✓	✓
6	Memiliki kemampuan untuk melakukan akses *remote* terhadap folder korban	✓	✓	✓	✓
7	Pada *network traffic* terlihat melakukan komunikasi pertukaran informasi	✓	✓	✓	✓
8	Memiliki kemampuan untuk *remote desktop / screen viewer*	✓	✓	✓	✓
9	Memiliki kemampuan untuk mengakses *remote shell* komputer *victim* untuk melakukan fungsionalitas	✓	✓	✓	✓
10	Memiliki fungsi untuk melakukan *remote execute file* melalui *url*	✓	✓	✓	✓

Nilai risk level pada *trojan* sample

No	RAT Name	MD5 hash	Risk Level
1	Blackshades	45ef635951e7e2da3dd8fc5090105fd7	10
2	Bozok	e3409c0f9575e26f7e1563f10736fd7c	10
3	DarkComet	725c03e97e1f33bef9f47021ad8883b6	10
4	njRAT	08f223ac15e2e92561ed310ae71415c1	10

Data karakteristik pada *sample non – trojan*

No	Kriteria	Team Viewer	Remote Utilities	Aero Admin	Ammyy Admin
1	**Tidak memiliki *verified signature***	×	×	×	×
2	**Memiliki kemampuan untuk melakukan *self file duplication***	×	×	×	×
3	**Memiliki *keylogger***	×	×	×	×
4	**Memiliki kemampuan untuk menambahkan *autorun registry* pada sistem**	×	×	×	×
5	**Memiliki kemampuan untuk *remote* perubahan *registry***	×	×	×	×
6	Memiliki kemampuan untuk melakukan akses *remote* terhadap folder korban	×	×	×	×
7	Pada *network traffic* terlihat melakukan komunikasi pertukaran informasi	✓	✓	✓	✓
8	Memiliki kemampuan untuk *remote desktop / screen viewer*	✓	✓	✓	✓
9	Memiliki kemampuan untuk mengakses *remote shell* komputer *victim* untuk melakukan fungsionalitas	×	✓	×	×
10	Memiliki fungsi untuk melakukan *remote download file* melalui *url*	×	×	×	✓

Nilai *risk level* pada *non – trojan sample*

No	Program Name	MD5 hash	Risk Level
1	Team Viewer	10af80866260b9c98337b73f4fa9edb2	2
2	Remote Utilities	197a5f96e7aa3ddf8ae3b5e2067b0b1a	3
3	Aero Admin	5cc3407420af93114932ae79be765fa1	2
4	Ammyy Admin	11bc606269a161555431bacf37f7c1e4	3

Tabel nilai *risk level* pada *non – trojan sample*

5. Kesimpulan dan saran

5.1 Kesimpulan

Dengan melakukan pengujian pada dan analisis terhadap 4 *sample trojan* dapat ditarik kesimpulan-kesimpulan.

- Kesimpulan pertama adalah dengan menggunakan gabungan kedua data dari hasil *static analysis* dan *dynamic analysis* dapat dihasilkan data karakteristik troja, yang dapat digunakan sebagai indikator untuk menganalisa *trojan* berdasarkan *behavior*nya. Dengan menggunakan nilai *threshold* ≥ 5 dimana tidak semua *sample* pada *non – trojan* mencapai nilai tersebut dan dikarenakan *trojan* memiliki sifat khusus yang menjadikannya berbeda dari *non – trojan sample*.
- Kesimpulan kedua adalah dengan menggunakan gabungan kedua dari data hasil *static analysis* dan *dynamic analysis* dapat digambarkan bagaimana perilaku atau sifat *trojan* saat menginfeksi sistem, terutama dalam hal ini Sistem Operasi Windows sebagai subjek percobaan.

5.2 Saran

Untuk pengembangan tugas akhir di masa mendatang, penulis menyarankan beberapa hal berikut:

1. Pengujian dilakukan untuk mendeteksi malware jenis lain semisal *rootkit, virus,* atau *worm*
2. Sistem Operasi yang ada saat ini tidak hanya Windows OS saja, melainkan ada Unix dan turunannya yang juga memungkinkan dapat digunakan sebagai subjek percobaan dalam melakukan *malware analysis*
3. Terkait dalam buku ini yang menggunakan 32 bit version, dapat juga memungkinkan menggunakan sistem operasi versi 64bit dari sebagai subjek percobaan

DaftarPustaka

[1] Adelstein, Frank, "Live Forensics: Diagnosing Your System Without Killing It First", ACM Vol 49, No 2, February (2006).

[2] Agrawal, Monika, Heena Singh, et al "Evaluation on Malware Analysis", in International Journal of Computer Science and Information Technologies (IJSCIT) Vol 3, (2014).

[3] Bhojani, Nirav. "Malware Analysis", Conference Paper, DOI: 10.13140/2.1.4750.6889 , 2014

[4] Carvey, Harlan. 2012. Windows Forensic Analysis Toolkit: Advanced Analysis Technique for Windows 7.

[5] Chen, Zhongqiang dkk (2000) "Catching Remote Administration Trojan (RATs), SP&E, California, USA.

[6] Eagle, Chris. 2011. The IDA Proo Book. San Fransisco, USA.

[7] Egele, Manuel, dkk. 2011. A Survey on Automated Dynamic Malware Analysis Techniques and Tools. California, USA.

[8] Gadhyin, Savan & Kaushal Bhavsar. "Techniques for Malware Analysis", International Journal of Advance Research in Computer Science and Software Engineering (IJARCSSE), pp 972-975, April (2013).

[9] Ismail, Anis, Mohammad Hajjar, Haissam Hajjar. "Remote Administration Tools: A Comparative Study" Journal of Theorical and Applied Information Technology, Libanon, (2008).

[10] Ligh, Michael Hale. Malware Analyst's Cookbook And DVD. Indianapolis, IN: Wiley, 2011.

[11] Milošević, N. "History of malware" Computer Security, pp 1, (2013).

[12] Satrya, Gandeva B. dkk (2015). The Detection of 8 Type Malware botnet using Hybrid Malware Analysis in Executable File Windows Operating Systems. Proceedings of the 17th International Conference on Electronic Commerce 2015 - ICEC '15.

[13] Netmarketshare.com. (2016). Operating system market share. [online] Available at: https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0 [Accessed 29 May 2016].

[14] SebastianZ (2015). Security 1:1 - Part 2 - Trojans and other security threats [online] Available at: http://www.symantec.com/connect/articles/security-11-part-2-trojans-and-other-security-threats [Accessed 29 May 2015].

[15] Ponangi, Preethi Vinayak (2011). Cognitive Cyber Weapon Selection Tool Empirical Evaluation, Wright State University, Ohio, USA.

[16] Sikorsi, M. & Honig, A. 2012. Practical Malware Analysis. San Francisco, USA.