Deployment of Proposed Botnet Monitoring Platform using Online Malware Analysis for Distributed Environment

Vidhya Sathish^{*} and P. Sheik Abdul Khader

Department of Computer Applications, B. S. Abdur Rahman University, Chennai, Tamil Nadu, India; vidhyasathish83@gmail.com, psakhader@bsauniv.ac.in

Abstract

The main intention of this paper is to elaborately discuss about seriousness of Botnet problem and project the importance of online malware analysis in Botnet defense research.

Keywords: Botnet, Honeypot, IDS, Malware Analysis, OpenDNS

1. Introduction

Botnet^{1,2} acts as a base for many illicit works, according to cyber community. Botnet has been categorized into centralized, decentralized and hybrid structures. In Centralized Structure³, one or group of compromised client machine will be remotely controlled by single server: Examples of Centralized Structure are IRC-based and HTTP-based. IRC-based Botnet is the oldest method followed by hacker. Main feature is it acts as communication protocols to reroute with compromised networks. Many defensive techniques have been proposed. Behalf of this, these communication protocols has been isolated from normal traffic. But IRC [Internet-Relay-Chat] based Botnet is still exists. Later, Hacker developed HTTPbased Botnet to achieve the destination by disrupting defensive techniques which was built against them. The main feature of HTTP-based Botnet is to hide from the users using the concept of dynamic domain name service, as a resolution to update and frequently changes the server location. In Decentralized Structure⁴, each Bot [compromised machine] acts as client and server. There is no centralized point of failure in such approaches. Examples of Decentralized Structure are P2P-based and fast-flux-based. These two approaches use the concept of fully qualified dynamic domain name service [FQDDNS] for frequent updates of new Botnet in automate manner. Many detection approaches are still being developed recent years. But it finds very difficult in shutdown and disrupt the Botnet resilience. Hybrid structure involves the combination of both centralized and decentralized structure. Recently, these types of structures are used as deliberate to spread Botnet in distributed environment. Based on History of Botnet, Figure 1 provides the complete structure of problem overview and detection approaches used.

1.1 Scope of Research Work in Botnet Defense

A lot of researchers engaged with the new techniques⁵ in recent years. But, advancement of Botnet defense is limited in scope. Some of them quietly impressed with Honeypot technology in Botnet defense research. Intrusion Detection/Prevention systems also plays effective role in understanding Bot and Botnet behavior. Finally, malware analysis also takes part as a major key role to identify the intention of attacks and also about hacker's nature. The concept of this paper is to provide proposed framework

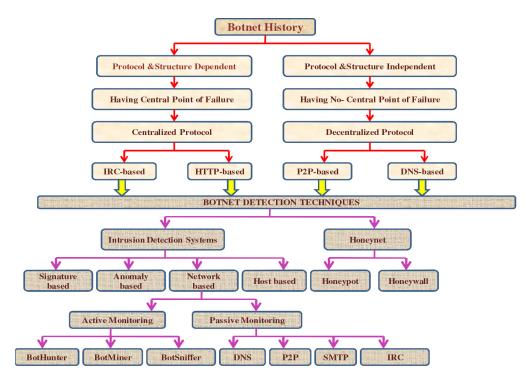


Figure 1. Botnet History and its Detection approaches.

by integrating Honeypot, Intrusion Detection Systems and malware analysis with aim to study Bot malware behavior and its nature in better phenomenon.

In this paper section II provides brief history about Honeypot technology, Intrusion Detection Systems and malware analysis importance in Botnet defense. Section III provides the related works done in Botnet mitigation and defense research. Section IV discusses about research directions in Botnet Defense. Section V presents detailed description of proposed framework using online malware analysis. Section VI concludes the future of proposed framework.

2. Brief History

2.1 Honeypot Technology

It is a technology^{6.7} designed to trap attackers to study their intention and behavior in automated manner. In other words, Honeypot is designed as a decoy system with an isolated environment to make the attackers voluntarily interact with them without their intention of that their idea is being trapped by an isolated source. The main ethic of this technology is data capturing; monitoring and analyzing the malware behavior. Another merit is, based on the user convince Honeypot can be deployed in both physical and virtual environment.

2.2 IDS

Intrusion Detection Systems⁸ able to handle various kinds of techniques and methods to identify abnormal malicious activities found in the network. The main ethic of IDS is to monitor the network traffic and analyze it, if any suspicious file present. It may also notify the presence of signature-based and anomaly-based attacks. Another merit is easy to deploy and maintain and also provide the real-time alert to novice users.

2.3 Malware Analysis

Malware analysis⁹⁻¹¹ is most attractive topic for lot of researchers recent days. The 'malware analysis' is to study malicious piece of program and also makes the users to understand the malware behavior with deep inspection in an isolated environment i.e., why, when, where it should be reached. Generally, observing real-time network traffic is most challenging task. But, through malware analysis it is possible to achieve this task without affecting the system.

3. Related Works

Botnet detection and mitigation has been classified as Intrusion Detection Systems based, Data Mining based and DNS based.

3.1 IDS based Detection

IDS¹²⁻¹⁵ are generally classified into signature-based and anomaly-based intrusion detection systems. In Signaturebased approach, the detection systems able to capture and log malicious traffic based on rules and signatures generated already i.e., able to capture only known malicious activity. In Anomaly-based approach, the detection systems depend on network traffic anomalies present in it. Anomaly based further classified into Host-based and Network-based. In Host-based, network traffic packets analyze both known and unknown suspicious files. In Network-based, capture and analyze the data to detect known attacks by comparing the signatures or patterns of database or detection of illegal activities by scanning traffic for anomalous activity. The major drawback of these approaches is they seem to be protocol structure and dependent and also these are fails to analyze malware behavior and nature.

3.2 Data Mining based Detection

The main purpose of this type of detection^{16,17} is used for optimization. It has been further classified into flowcorrelation algorithm, classification algorithm, and clustering and finally association rule. In Flow-correlation algorithm, useful to compare flow objects based on some characteristic other than packet content. This technique is very effective and utilizes the characteristic values as input into one or more functions to create metric used to decide if flows are correlated. In classification algorithm, incoming packet will match one of previous patterns. The major limitation is, it is not appropriate approach to detect new attacks. In clustering, divide entire set data into subgroups or clusters containing relatively identical features and limitation is it does not require a labeled dataset for training. In association rule based, derive the implication relationship between data items under the conditions of set of given project types and number of records and finally analyzing the records. The major drawback behind is no real-time detection; protocol structure and dependent and also no proof of utilizing malware analysis to overcome Botnet resilience.

3.3 DNS based Detection

This technique^{18,19} identifies key metrics for measuring Botnet utility and describes various topological structures that BOTNET may use to coordinate attacks.. The limitation of this approach it could be evaded if Botmasters know the mechanism or suspect it is running. Botmaster may also poison the scheme through 'fake DNS' thus generating many false alarms. Another approach is DNS based BlackHole List (DNSBL) used to publish the addresses of computers or networks linked to spamming and other malicious activities. The major limitation is approach is not effective because it is not difficult to design evasion strategies.

4. Research Directions in Botnet Defense

Most of Detection approaches fail²⁰ to analyze the malware to study its nature and behavior. Moreover analyzing data in real-time is tend to be most tedious task; also disruption of Botnets is lack of efficient techniques. Most of malware²¹ used by Botnets "runs only" on MS Windows, making - "ms windows machines the main targets". More advanced Botnet technique at present is DDNS [Dynamic Domain Name Service] - also known as fast-flux [Bots would query certain domain i.e., mapped onto IPADDRESSES, which change frequently]. Fast-flux makes Botnet more difficult to takedown or blocks a specific C&C server. Research on Botnet is relatively new and it has been subject of increasing interest in recent years. Existing studies remain limited in scope do not include recent research & developments. It is necessary to analyze a massive amount of data, which is difficult to perform in real-time thus making detection in large-scale networks a prohibitive task. The sandboxed training environment²² can be improved to better circumvent malware authors to probe for virtual machine settings and react by stopping all activity. Creating "real-time Botnet Monitoring platform" and identifying new Bot variants and developing network sandboxing mechanisms that prevent captive Bot nodes from causing them.

5. Proposed Framework for Online Malware Analysis

Proposed framework has been designed based on descriptive architecture of Botnet problem. It paved the new way of research to study and analyze the malware behavior. As reviewed from lot of journals related to Botnet defense research, utilizing the DNS Sinkhole server for malware analysis is not in a sufficient way for research work. Based on this, proposed work has taken as a challenge to use this task for online malware analysis. In proposed work, virtual testbed will be created using vmware workstation in windows 7 Host machine. Figure 2 of results shows desktop display of Windows 7 in virtual machine. The major reason to choose windows operating system as platform to work with proposed, because MS windows machines are main targets for most cyber attacks. Benefit of vmware is able to create one or more virtual machines within single system. It will be treated as guest machine. Additional tools used for proposed work are listed below:

5.1 Opendns

Opendns servers²³ store the ip addresses of millions of websites in their cache. It works in cloud to track malicious traffic and blocks phishing websites from loading the system. In Figure 3 of results show the utilization of opendns for internet access. Also, Figure 4 of results



Figure 2. Desktop display of virtual machine.



Figure 3. Utilizing opendns for internet access.



Figure 4. Homepage using opendns.

shows the homepage access. OpenDNS runs a high-performance network which is geographically distributed and serviced by several redundant connections. Table 1 shows the comparative study of DNS services.

5.2 KFSensor

Windows based Honeypot Intrusion Detection Systems is a simulation tool²⁴ act as Honeypot to attract and detect Hackers and worms by simulating vulnerable system services and Trojans. By acting as decoy server it can divert attacks from critical systems and provide a higher level of information than can be achieved by using firewall and NIDS alone. From the Figures 5 and 6 of results shows the normal and abnormal behavior of network activity in opendns network traffic. The system is highly configurable and features detailed logging, analysis of attack and security alerts. This approach complements other forms of security and adds another defense against growing security threat faced by organization.

Table 1.Comparing DNS services

	Comcast AT&T	Google publicDNS	OpenDNS Basic
Servers located world-wide		yes	yes
DNS security	maybe	yes	yes
IPV6 support			yes
Domain category			yes
Tagging			yes
Filter unwanted sites			yes

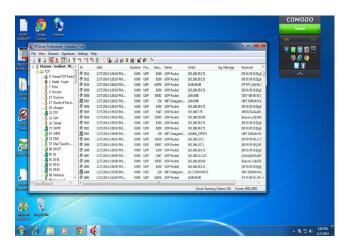
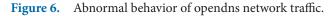


Figure 5. Normal behavior of opendns network traffic.

5632 PC Anywhere 2	* ID	Start	Duration	Pro.,	Sens	Name	Visitor	Received
Ston VINC HITTP - Enter	0.1	181 2/27/2014 #10-44 PM	0.000	102	1947	LIDP Packet	admin.91	103 00 00 0A3402 00 00 00 00 00 00 00 00 00 00 00 0001 (Y+U/L
- 🏘 5900 VNC	0	180 2/27/2014 4:00-44 PM	0.000	UDP	43440	UDP Packet	192,168,42,77	[00 02 00 00 00 00 00 00 11 00 14]E[A4]i/3[8E]#[98]E1]
- 📑 6101 Veritas Agent Browser		179 2/27/2014 4-10-43 PM	0.000	INP		LIDP Packet	RSAMNET	unf15740448C10FNTVI14HW9G9k3Ta388kW16
▲ 6112 CDE	(Ø)	178 2/27/2014 4:00:42 PM	0.000	UDP	1947	UDP Packet	SURSCRIBER	VL/UHOWAA8TVU/T01//0K/SAG9:b3/TaXR8bWUA
6129 Dameware		177 2/27/2014 4:00:39 PM	0.000	UDP		UDP Packet	192,168,7,149	iDOHUvATAA8hZG1pbi03NG/IMmM2ZicAaXR8bWUA
6346 BearShare		176 2/27/2014 4:00:38 PM	0.000			UDP Packet	SURSCRIBER	VL/UHOWAA8TVU/TOLIIOW/SAG2xb3/TaXR8bWUA
6881 Bit Toment 6912 Shit Heep, Troisn		175 2/27/2014 #10-32 PM	0.000		10505	100 Parket	11 YAS	Beacon-v/2III.YASIWindowsPCI/e5dtx8b5ca7eb87792a29
- 🖶 6912 Shit Heep, Trojan - 🖨 6969 GateCrasher, Trojan		174 2/27/2014 4:00:37 PM	0.000	LIDP		DOS Attack	BYAS	Connections: 50010D 0AlActive Connections: 010D 0AIR
- 6970 GateCrasher, Trojan		173 2/27/2014 4:00:35 PM	0.000			LIDP Packet	acroathi-PC	[0C]/(80 00 00 01 00 01 00 00 00 00 02]54[03]168[03]168[
- A training and the state of t		172 2/27/2014 4:00:34 PM	0.000			NBT Datagram		NBT DGRAM Packet: id:53504 Type: Direct GroupI0D 0
A 7215 kfSubSeven Matrix		171 2/27/2014 4:00:35 PM	0.000	UDP		LIDP Packet	B YAS	Beacon-v2III.YASIWindowsPCI7e5dfa865ca7eb82792a29
7213 Ki Subseven Watrik 7291 Unknown		170 2/27/2014 4:00:33 PM	0.000	UDP		UDP Packet	192,168,42,77	100 02 00 00 00 00 00 00 11 00 141d/IBFIMI15MD2 CB
8000 ES Prony		169 2/27/2014 4:00:33 PM	0.000	LIDP		LIDP Packet	11105	Beacon-v2III.YASIWindowsPCI7e5dfa805ca7eb82792a29
8080 IIS Proxy - Recent Activity		169 2/27/2014 4:00:35 PM	0.000	UDP		UDP Packet	1145	Beacon v28LVASWindowsPC7re5dia865ca7eb82792a29
8555 Cisco Tomcat		167 2/27/2014 4:00:29 PM	0.000			UDP Packet	ADMIN-74882	traEUDQIAARRETITIEINEICHEMENDECHEMENUA
8879 Hack Office Armageddon		167 2/27/2014 4:02/29 PM	0.000	UDP		UDP Packet	LYAS	Beacon v28LVASIWindowsPC7r55Ha865ca7eb82792a29
8967 Command console		165 2/27/2014 4:00:27 PM	0.000			UDP Packet	1145	Beacon v28LVASIWindowsPCI7e5dfa805ca7eb82792a29
9898 Command console		05 2/2//2014 4:00:27 PM 164 2/27/2014 4:00:25 PM	0.000			UDP Packet	IL YAS	Beacon-vzju, YASJWindowsPC(/e5dfa865ca7e582/92a29 Beacon-v28, VASJWindowsPC(7e5dfa865ca7e582792a29
9996 Sasser worm conole		163 2/27/2014 4:00:23 PM	0.000			UDP Packet	IL YAS	Beacon v28LYASIWindowsPCI7e5dfa805ca7eb82792a29
a 10000 Veritas Backup Exec		163 2/2//2014 4:00:23 PM 162 2/27/2014 4:00:22 PM	0.000	UDP		UDP Packet	102.168.7.75	
🔒 10085 Syphillis, Trojan		161 2/27/2014 410/22 PM	0.000			UDP Packet	4DMIN-74882	d87JUZAGAA8CU0FVLTc1NDc4QTV4QkEAsXR8bWUA
10617 IIS Prevy								tri40UDQIAABBREIJTI03NEICMKM2RjicAaXR8bWUA
🔒 11768 dipnet, trojan		160 2/27/2014 4:00-21 PM	0.000	UDP		UDP Packet	ILVAS	Beacon v2/JLVAS/WindowsPC/7e5dfa865ca7eb82792a29
🔒 17300 Kuang 2, Trojan		159 2/27/2014 4:00:09 PM	0.000			UDP Packet	192.168.154.2	sLk+UTQQAABBRELITILQQwBtRG9sb3JTabXnBiUA
- 🔓 2000 Milennium, Irojan		158 2/27/2014 4:00:05 PM	0.000			UDP Packet	192.168.154.2	sLk+UTQOAABBRELITILQQwBrR93sb3ITabXxBiUA
🗛 20034 NetiBus		157 2/27/2014 4:00:12 PM	0.000	UDP		UDP Packet	ILYAS	Beacon-v2jlLYAS/WindowsPC(7e5dfa865ca7eb82792a29
- 🥪 20168 Lovegate worm		156 2/27/2014 4:00:00 PM	0.000	UCP		UDP Packet	ILYAS	Beacon v2JILVAS/WindowsPCJ7e5dfx865ca7eb82792a29
🔮 20525 Unknown		155 2/27/2014 4:00:09 PM	0.000			UDP Packet	PSSL24	1TGmTDQIAA8QU1NMMjQAc3VtR09sb3/TaXR8bWUA
🤮 21544 GirlFriend, Trojan		154 2/27/2014 4:0008 PM	0.000	UDP		UDP Packet	ILYAS	Beacon-v2/ILVAS/WindowsPC(7e5dfa865ca7eb82792a20
📲 23476 Donald Dick		153 2/27/2014 4:00:08 PM	0.000	UDP		UDP Packet	192.168.7.24	ZvqFS0AEAABEQ0woNQBwc3VtRG9sb3JTaXRBbWUA
🙀 24186 IIS Provy		152 2/27/2014 4:00:06 PM	0.000	UDP		UDP Packet	ILYAS	Beacon v2JLYAS/WindowsPC(7e5dfa865ca7eb82792a29
- 🏠 27015 Half Life		151 2/27/2014 4:00:05 PM	0.000	UDP		UDP Packet	BSAMINET	wmfXS7APAABCU0FNTkyUAHVtR09sb3JTaXR8bWUA
A 77374 MichiGeuen Genuer	, 07	150 2/27/2014 4:00:04 PM	0.000	UDP	10505	UDP Packet	ILYAS	Beacon v2/JLVAS/WindowsPC(7e5dfa865ca7eb82792a29



5.3 SnortIDS

SnortIDS²⁵ is an open source network intrusion detection/prevention system. Used as real-time in proposed system. Snort can be configured in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. From the Figure 7 of results shows the snort running for real-time alert in virtual machine. The program will then perform a specific action based on what has been identified.

5.4 COMODOfirewall

Comodo firewall²⁶ is really good personal firewall which has several configurable features that makes use of latest technologies like 'Host based IDS' for actively monitoring and protecting your system from multiple type of attacks. The merit of comodo is plays a major role in maintaining the functionality and usability of system. It also prevents network-based attacks from the system.

5.5 Netflow Analyzer-Manage Engine

Used as network bandwidth^{27,28} monitoring tool in proposed work to provide holistic view about network bandwidth and traffic patterns. ManageEngine NetFlow Analyzer is a web-based bandwidth monitoring tool that collects, correlates, and analyzes NetFlow versions exports to show you what applications are using bandwidth, who is using them, and for how long. View in-depth bandwidth reports across your WAN and LAN without having to deploy expensive hardware probes. Recognize most enterprise applications and see how traffic flows across your network. NetFlow Analyzer also monitors critical VoIP metrics.

5.6 Fakenet

FakeNet²⁹ is a tool that aids in the dynamic analysis of malicious software. The tool simulates a network so that malware interacting with a remote host continues to run allowing the analyst to observe the malware's network activity from within a safe environment. The main features are being easy to install and use; the tool runs on Windows and requires no 3rd party libraries. Support the most common protocols used by malware. Figure 8 of results shows the fakenet observation in opendns from the virtual machine. Perform all activity on the local machine to avoid the need for a second virtual machine. Provide python extensions for adding new or custom protocols. Keep the malware running so that you can observe as much of its functionality as possible. Have a flexible configuration, but no required configuration



Figure 7. Running snort for real-time alert.

C 6 D sedistus/2012/07/update-fake	net-v-1-0c-a-tool-that-helps-with-the-dynamic-analysis-of-malicious-	software html	(c)
I C/Users/VIDHYA-J/AppData/Loca//Temp/RarSEX39.0		MontonioSistem Administrator	[4]
IStarting program, for help open a web (Pross CIRL-C to exit.)	brouser and surf to any UHL.1		
[Pross CIRL-C to exit.] [Medifying local DNS Settings.]	e Determy		
(Project Ciki-C to exit.) [Inditying local INS Settings.] Scanning Installed Providers Installing Lawred Providers Preparing To Reader Installed Chains			
Readering Installed Chains Saving New Protocol Order	thware analysis. It		
Listening for SSL traffic on port 88.]	ing hard-coded IP traffic		
[Listening for SEL traffic on port 844] [Listening for traffic on port 8080.]	hat malicious code		
Listening for traffic on port \$880.1 University for DNS traffic on port: 53			
Unistening for traffic on port 1337.1	12.1 Is a python extension		
[Can't listen on part 88 because anoth	or program is already listening.] e capability to listen to		
[Can't listen on port 8880 because and [Can't listen on port 8880 because and [Listening for ICMP traffic.]	ther program is already listening.] ther program is already listening.]		
	tool gaps fipe on Window		
Bind call failed: 10048. [Listeniny for SSL traffic on port 465		Scatter	
L	j=		
	If the application fails to initialize, then you need to download and install the Visual		
	Studio 2008 redistributables (http://www.microsoft.com/download/en/details.asp/?		
	(d) 21). This is a temporary workaround until this issue can be properly fixed.		
	 Supports DNS, HTTP, and SSL 		
	 HTTP server always serves a file and bles to serve a meaningful file; if the 		
	malware request a jpg then a properly formalted jpg is served, etc. The files		
	being served are user configurable.		
	 Ability to redirect all traffic to the localhost, including traffic destined for a hard- 		
	coded IP address.		
	 Python extensions, including a sample extension that implements SMTP and 		
	SMTP over SSL		

Figure 8. Observation of fakenet in opendns.

5.7 Capture BAT

This is a behavioral analysis tool of applications for the Win32 operating system family. Capture BAT^{30,31} is able to monitor the state of a system during the execution of applications and processing of documents, which provides an analyst with insights on how the software operates even if no source code is available. Known event noise can be excluded by a fine-grained mechanism that allows an analyst to take into account the process that cause the various state changes. As a result, this mechanism even allows Capture to analyze the behavior of documents that execute within the context of an application, for example the behavior of a malicious Microsoft Word document.

6. Results

The experimental setup has been created using VMware workstation in Windows 7 operating system. The proposed work utilizes the openDNS sinkhole system to have real-time observation in network traffic. Also utilize the supporting tools to make the observation accuracy such as KFsensor, SnortIDS, and Fakenet etc. some of the screenshots of proposed work listed below.

7. Conclusion

We presented an approach for effective Botnet defense by utilizing the DNS sinkhole for online analysis. The proposed has been designed by integrating Honeypot technology, Intrusion Detection Systems and malware analysis in Windows based platform for Botnet research. We also discussed about research limitations in Botnet defense. In future, it can be employed offline using python based forensic analysis.

8. References

- 1. Zhu Z, Lu G, Chen Y. Botnet research survey. Annual IEEE International Computer Software and Application Conference, IEEE Computer Society. 2008.
- 2. Gross B-S, Cova M et.al. Your botnet is mybotnet: analysis of a botnet takeover. CCS'09, Nov 9–13 2009, ACM.
- 3. Li C, Jiang W, Zou X. Botnet: survey and casestudy. In 4TH International Conference on Innovative Computing, Information & Control, IEEE Computer Society; 2009; IEEE.
- 4. Feily M, Shahrestani A et al. A survey of Botnet & Botnet detection. 2009 3rd International Conference on Emerging

Security Information, Systems & Technologies IEEE Computer Society; 2009; IEEE.

- 5. Silva SSC, Silva RMP et al. Botnets: A Survey. Computer Networks. 2013; 57:378–403.
- 6. Tiwari R, Jain A. Improving network security and design using honeypots. CUBE; 2012 Sep 3–5.
- 7. Pham V-H, Dacier M. Honeypot trace forensics: the observation viewpoint matters. Future Generation Computer Systems Elsevier; 2010.
- Raghava NS, Sahgal D, Chandna S. Classification of botnet detection based on botnet architecture. 2012 International Conference on Communication Systems & Network Topologies, IEEE Computer Society. 2012
- 9. Kasama T, Yoshika K et al. Malware sandbox analysis with efficient observation of herder's behavior. J Inform Secur. 2012 Oct; 20(4):835–45.
- Egele M, Scholte T, Kirda E, Kruegel C. A survey on automated dynamic malware analysis techniques & tools. ACM Computing Surveys. 2012; 1–49.
- 11. Graziano M, Leita C, Balzarotti D. Towards network containment in malware analysis systems. ACSAC'12, 2012 Dec 3–7.
- Goebel J, Holz T, Rishi. Identify Bot contaminated hosts by IRC nickname evaluation. Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, USENIX Association, Berkeley, CA, USA; 2007.
- Liu L, Chen S, Yan G, Zhang Z. BotTracer: Execution-based Bot like malware detection. Wu T, Lei C, Rijmen V, Lee D, editor. Information Security, Lect Notes Comput Sci. 2008; 5222: 97–113.
- Xu K, Yao D, Ma Q, Crowell A. Detecting infection onset with behavior-based policies. 5th International Conference on Network & System Security (NSS); 2011. p. 57–64.
- Gu G, Yegneswaran V, Porras P, Stoll J, Lee W. Active Botnet Probing to Identify Obscure C&C Channels. Computer Security Applications Conference, ACSAC'09; 2009. p. 241–53.
- 16. Gu G, Porras P, Yegneswaran V, Fong M, Lee W. BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation. in: proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, USENIX Association, Berkeley; 2007; CA: USA. p. 12:1–12:6.
- Gu G, Perdisci R, Zhang J, Lee W. BotMiner: Clustering Analysis of Network Traffic for Protocol & Structure Indepdenent Botnet Detection. Proceedings of 17th Conference on Security Symposium, USENIX Association; 2008; Berkeley, CA: USA. p. 139–54.
- Choi H, Lee H, Kim H. BOTGAD: Detecting Botnets By Capturing Group Activities in Network Traffic. Proceedings of the fourth International Conference on Communication System Software & Middleware, COMSWARE'09; 2009; New York: USA. p. 21–8.

- Villamerin-Salomon R, Brustoloni J. Identifying Botnets using Anomaly Detection Techniques Applied to DNS Traffic. 5th IEEE Consumer Communications and Networking Conference, CCNC 2008; 2008. p. 476–81.
- Zhuge J, Holz T, Han X et al. Collecting Autonomous Spreading Malware using High-Interaction Honeypots. ICICS 2007, LNCS 4861; 2007; Springer-Verlag; Berlin Heidelberg 2007. p. 438–51,
- Tegeler F, Fu X, Vigna G, Kruegel C. Botfinder: Finding Bots In Network Traffic Without Deep Packet Inspection. Co-NEXT'12; 2012 Dec 10–13.
- 22. BrettStone-Gross, Marco Cova, Bob Gilbert et.al. Analysis of a botnet takeover. IEEE Computer and Reliability Societies; 2011. p. 1540–7993, IEEE 2011.
- 23. Available from: www.404techsupport,com/2010/02/ opendns-pt-2-a-comparison/
- 24. Available from: www.highbeam.com/doc/1G1.101853773. html/

- Chakraborti S, Chakraborty M, Mukhopadhyay I. Study of Snort-based IDS. Proceedings of International Conference & Workshop on Emerging Trends in Technology; 2010. p. 43–47.
- 26. Available from: www.ida.liu.se/projects/firewallcomparison/infosecpaper.pdf
- 27. Available from: www.manageengine.com/products/net-flow/manageengine-netflowanalyzer.pdf
- 28. Available from: www.manageengine.com/products/netflow/netflow-features.html
- 29. Available from: www.practicalmalwareanalysis.com
- 30. Available from: www.honeynet.org
- Watson D, Riden J. The honeynet project: data collection tools, infrastructure, archives and analysis. WISTDCS '08. WOMBAT Workshop on Information Security Threats Data Collection and Sharing, 2008; 2008 Apr 21–22. p. 24–30.