Detecting and Preventing the Botnet's Activity based on DNS Investigation

P. Ashok, G. Manimala

Abstract— Attackers, typically busy to initiate malicious threat to scratch the compromised host. Botnet's are newly developed technology by attackers and its task to raise the traffic in DNS service to launch attacks. Due to increased traffic in DNS, botmaster's create a new channel between server and client to disseminate commands to all bots; it has capability to command and control the Operating System and repeatedly generate more queries over DNS which increase the traffic. Many botnet operators used HTTP, IRC server to pass the information. In this paper, we proposed feasible approach called Wide Packet Inspection to analyze the DNS traffic to control and avoid the Botnet. This paper provides a countermeasure against botnet operators to slow down the bot activity.

Index Terms— botnet tracking, botnet avoidance, wide packet inspection, honeyspot, communication flow, propogation of botnet

1 INTRODUCTION

THE common dissimilar between a bot and other type of malwares lies within a bot's able to issue a command and control over operating system and automatic generating queries to increase the traffic in DNS. Recent malicious are intended to get financial benefits through collection of compromised hosts, which are known as bots. A collection of bot infected machines are refered as botnet. Bots receives new attack command from botmaster's to launch DDOS attacks and stealing others personal information from host. As growing esteem of botnets in internet, it is very hard to find defense mechanism with the speed of botnet technologies because it automatically changes bot program methods and command &control strategies. The characteristics of bot can able to create channel for establishing a command and control issues that makes attackers to control or update a compromised host. A Botnet operator uses HTTP protocol or IRC to steal the confidential information with new stealthy communication to avoid the detection. HTTP based command and control is hard to distinguish from legitimate web traffic. From defenders' point of view, the approach of user-intention-based anomaly detection has been demonstrated effective in detecting abnormal system events such as unauthorized file creation and malware-triggered outbound traffic. Because DNS queries automatically issued by applications or the OS, the relations between user actions and DNS traffic may not be understandable. In order to reduce the traffic in DNS, we approached technique called Wide Packet Inspection which provide reliable service and reduced Distributed Denial of Service.

- *P. Ashok, is currently pursuing masters degree program in Computer Science and Engineering at Sri Sai Ram Engineering College, Anna University,India, E-mail:ashokit009@mail.com*
- *G. Manimala, is currently working as Associate Professor at Sri Sai Ram Engineering College, Chennai, India,Email:manimala.cse@sairam.edu*

2 PROPAGATION OF BOTNET

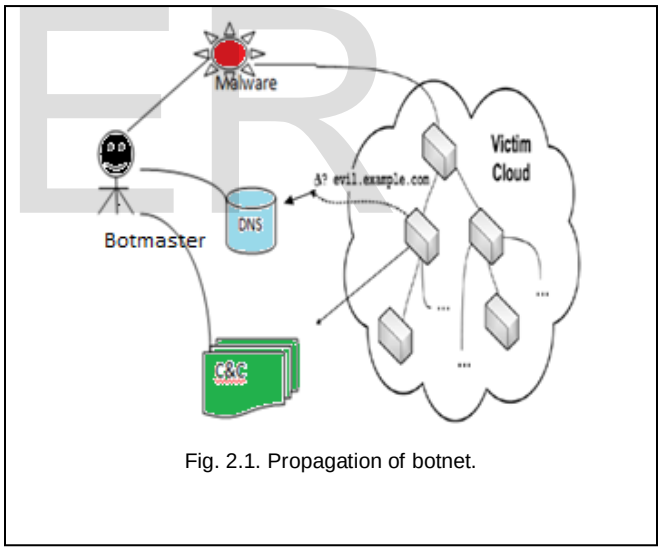


Fig. 2.1. Propagation of botnet.

Let us consider the above illustration of propagation of botnet. A Botmaster who control all bots release virus and start spreading randomly to steal confidential information from compromised host. The virus enforce victim's host to join with command and control service at the domain called evil.example.com. From there, botmaster make use of services like spamming, phishing, DDoS, identity theft. Each infected victim leads to create victim cloud and virus make infected victim to contact with command and control server (eg., IRC server, Web server, P2P network), infected individuals must perform DNS lookups of evil.example.com. The botmaster, who has authorized to use domain, can able to control the DNS resolution at the authority server. In case network administrator block the access to IP of command and control site, then the botmaster renumber the command and control IP.

3 BOTNET COMMUNICATION FLOW

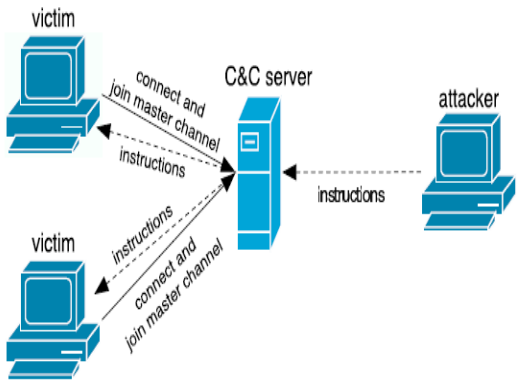


Fig. 3.1. Communication Flow.

A botnet is a collection of compromised host in a network which runs under command and control server. Bots eventually scans whole network range to compromise the various systems and then launch command and control channel that enables remote control of victim computer via IRC, FTP, and HTTP. Bots provide dynamic DNS names so it is easy to evade detection by defenders. With help of special pet name, bots try to join master's channel using channel password. This channel can be controlled by attacker remotely to issue the command as

```
http.update http://<server>/rBot.exe c:\msy32awds.exe 1
```

it instructs the bots to download a binary from the Internet via HTTP and execute it . Suppose if this instruction does not contain any command, bots wait to receive command from botmaster. Today attackers, often used to launch DDoS in the internet by implementing TCP SYN command like

```
ddos.syn XXX.XXX.XXX.XXX 80 600
```

Instruct the bots to start flood attack against the specified IP address against TCP port 80 for 800 seconds. With the above command bots launch the DDoS attacks in compromised host.

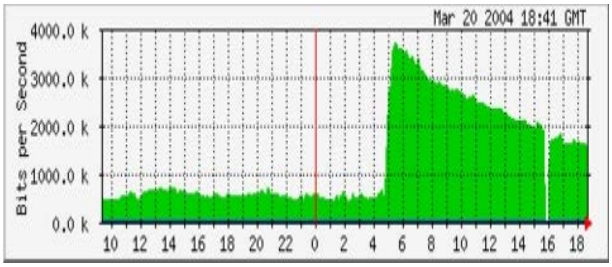


Figure from the Team Cymru Web site that shows how Darknet detected worm just minutes after it's released. The graph shows sudden spike in DNS traffic due to bots.

4 BOTNET DETECTION PROBLEM

Botmasters who controls bots aware of such a situation, when anyone tries to detect botnets it randomly move command and control service location. With the combination of more number of command and control server, botmaster minimize the chance that the network can be disrupted through simple remediation. In some case, botmasters can able to turn "ON" or "OFF" the bots. Queries from compromised host's entry into DNS as innocent hostname like host.domain.com. This type of hostname may be stored as any type of record (e.g., A, MX, CNAME). A request for an A or CNAME record tends to be the most common, and therefore, a preference should be given to these records types, so that queries would appear most like legitimate traffic. When client queries host.domain.com, and it wait for particular value in server's response. so, upon receiving queries, DNS server returns the response which has information as

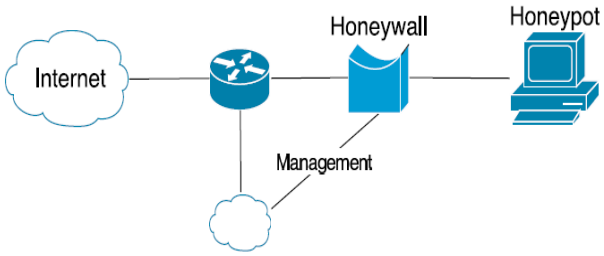
- Upstream: Ask CNAME for:
  `NBSWY3DPFQQHO33SNRSA000.domain.com`
- Downstream: CNAME points to:
  `NBUSYIDCN5ZXG000.domain.com`
  `3600`
  `CNAME`
  `NBSWY3DPFQQHO33SNRSA000.domain.com`

To conquer this type of bots activity is to perform Wide Packet Inspection before bots try to entry in DNS.

5 BOTNET TRACKING AND AVOIDANCE

5.1 Tracking Botnets

Botnets tracking can able to observe bots activity and used to avoid Distributed Denial of Service in compromised host. Observation can be done with help of setting *honeyspots* technique.



Honeyspots uses special software that is used to collect the data permanently about the system behavior and assist automatic post-incident forensic analysis. With help of collected data enables to determine the necessary information about the existing of botnets in compromised host. Further, when a bot try to connect with command and control server after obtained a new attack command once it successfully attacked the honeyspot, honeywall plays a vital role to track the bots. Honeywall provides transpar-

ent bridge between two tasks such as Data Control and Capture. Due to Data Control, it helps to control all suspicious in and out going messages and can able prohibit the bot from accepting valid command from botmasters via created channel. Due to Data Capture, it enables to determine the DNS/IP address that the bot needs to connect and also port number. It logs the pet name, server's password, name of the channel and its password. Thus honeywall collects all necessary information and honeyspot able to track further malware.

5.1 Botnets Avoidance

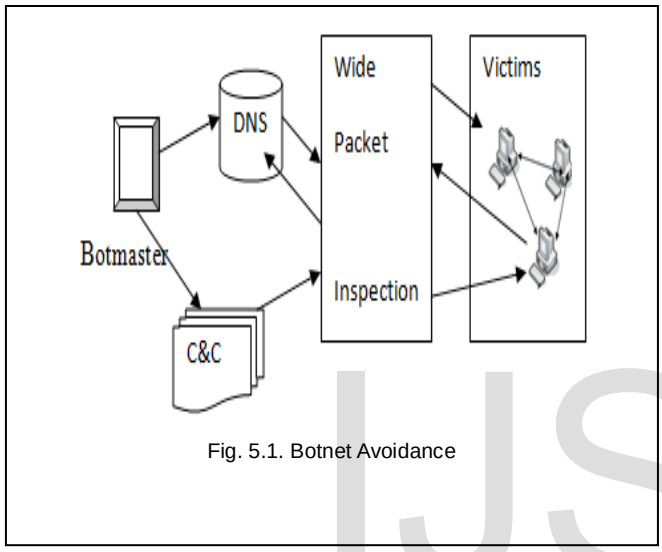
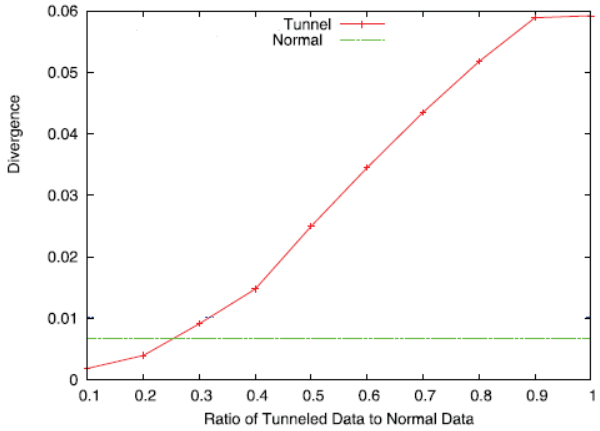


Fig. 5.1. Botnet Avoidance

Botnet avoidance can be done by DNS-Based Detection which helps to avoid Distributed Denial of Service and it increases the service time. Bot's make use of higher legal traffic to mix with DNS query to launch the attack. Thus, Wide Packet Inspection initially allows bots to enter in it and perform packet payload check to quantitatively evaluate the probability distributions of (botnet) DNS-packet.



In wide packet inspection test, DNS tunneling with normal traffic rate were observed and record with a long hour network activity. The Result shows that tunneling trace contains more illegal 'A' queries and 'TXT' queries which generated by bots to increases the traffic. Generally, Tunneling trace does not provide query confidentiality because it contains encrypted Secure Shell activity. So, we concentrate only on DNS payload to minimize the bots activities. In fig., shows the comparative trace of Tunneled data with normal data of DNS query. Red line shows the mixing of bots with legal traffic and green line represents normal DNS traffic. Thus, bots activity can be identified and avoided with help of Wide Packet Inspection.

6 Related Evaluation

6.1 Top-5 botnet outbreaks.

Botnet	Percentage of Victim Population
ZeusBotnet[X]	19%
KoobfaceBotnetB	15%
ClickfraudBotnet[X]	9%
SpamfraudBotnet[X]	8%
MonkifBotnetA	8%

In 2009, Damballa observed thousands of illegal botnets operators and found millions of newly compromised host in the network. He also stated that criminals manage this botnets to control 600,000 victims at any single point in time and has ability to breach the millions of additional hosts.

6.2 Botnet Detection Information

In March 2012, Waledac/Kelihos botnet took control of more than 118,000 system under unique bot ID's. Each red line represents the infected machines of more than 430,000 unique IP address from various countries that awaiting to get the command to launch attack at Dell Secure House.

7 CONCLUSION

In this paper, we examined the Wide Packet Inspection to check the botnet activities and eliminate with help of DNS packet payload. Before bots try to enter into DNS queries, Wide Packet Inspection Mechanism filter illegal entry and provide a countermeasure against the bot operators from compromised host. Thus, this approach provides prior knowledge about the command and control activities from botmasters which used to detect bots and response with alternate loop.

8 CONCLUSION

[1]. Ashok. P.; Manimala. G.; "*Detecting and Preventing the Malicious System based on DNS Analysis*," Journal of Computer Applications (JCA) ISSN: 0974-1925, Volume VI, Issue 3, 2013

[2]. Kui Xu, Patrick Butler, Sudip Saha, and Danfeng (Daphne) Yao, "DNS for massive scale command and contorl" ,*IEEE. Dependence and secure computing.*,*vol.10*.,may/june.2013.

[3]. The Honeynet Project. Know your Enemy: Tracking Botnets, March 2005. http://www.honeynet.org/papers/bots.

[4]. Computer Emergency Response Team. CERT advisory CA-1996-21 TCP SYN
Flooding Attacks. Internet: http://www.cert.org/advisories/CA-1996-21.html, 1996.

[5]. Felix C. Freiling, Thorsten Holz? und Georg Wicherski "Laboratory for Dependable Distributed Systems", RWTH Aachen University, 52056 Aachen, Germany. http://aib.informatik.rwth-aachen.de/

[6]. D. Eastlake & A. Panitz, "RFC 2606: Reserved Top Level DNS Names", June 1999, http://www.faqs.org/rfcs/rfc2606.html

[7]. IANA, "Special-Use IPv4 Addresses", Sept.2002,http://www.faqs.org/rfcs/rfc3330.html", and Y. Rekhter, B. Moskowitz, D.
Karrenberg, G. J. de Groot & E. Lear, "Address Allocation for Private Internets", Feb.1996,http://www.faqs.org/rfcs/rfc1918.html

[8]. D. Dagon, C. Zou, W. Lee, Modeling botnet propagation using time zones, in: Proceedings of the Annual Network and Distributed System Security Symposium (NDSS), 2006.

[9]. G. Ollmann, "Botnet Communication Topologies: Understanding the Intricacies of Botnet Command-and-Control," https://www.damballa.com/downloads/r_pubs/WP_Botnet_ Communications_Primer.pdf, 2013

[10]. C.J. Dietrich, C. Rossow, F.C. Freiling, H. Bos, M. van Steen, and N. Pohlmann, "On Botnets that Use DNS for Command and Control," Proc. European Conf. Computer Network Defense, Sept. 2011.

[11]. E. Kartaltepe, J. Morales, S. Xu, and R. Sandhu, "Social Network- Based Botnet Command-and-Control: Emerging Threats and Countermeasures," Proc. Eighth Int'l Conf. Applied Cryptography and Network Security (ACNS), pp. 511-528, 2010.

[12]. M.A. Rajab, F. Monrose, A. Terzis, and N. Provos, "Peeking through the Cloud: DNS-Based Estimation and Its Applications,"
Proc. Sixth Int'l Conf. Applied Cryptography and Network Security (ACNS), S.M. Bellovin, R. Gennaro, A.D. Keromytis, and M. Yung, eds., pp. 21-38, 2008.

[13]. C.J. Dietrich, C. Rossow, F.C. Freiling, H. Bos, M. van Steen, and N. Pohlmann, "On Botnets that Use DNS for Command and Control," Proc. European Conf. Computer Network Defense, Sept. 2011.

[14]. Grzegorz Landecki ., "A simple solution combining Darknet and IDS" , http://www.linuxjournal.com/magazine/detecting-botnets., Jan 01, 2009.

[15]. Brett Stone-Gross,"Dell SecureWorks Counter Threat Unit Threat Intelligence", http://www.secureworks.com/research/threats/waledac_kelihos_botnet_takeover/, "Detection & Protection Against the Waledac Kelihos Botnet.,"Release Date: 28 March 2012"