Indian Journal of Science and Technology, *Vol 9(16), 10.17485/ijst/2016/v9i16/92207, April 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

An Investigation of Botnet Activity based on DNS Analysis

P. Ashok*, J. Velmurugan, M. Abinaya and B. Usha Shree Jayanthi

Department of Information Technology,
Vel Tech High Tech Dr. Rangarajan Dr. Sakunthala Engineering College,
Avadi, Chennai - 600062, Tamil Nadu, India;
ashokit009@gmail.com, velmurugan@velhightech.com
rajalakshmiabinaya@gmail.com, ushashreejayanthi@gmail.com

ABSTRACT

Background/Objectives: Botnet is used to increase congestion over DNS. The botmasters can establish a network between client and server to generate more queries to increase traffic via HTTP1. Thus, this paper used DPI approach to control botnet activities. **Methods/Statistical Analysis**: Deep Packet Inspection (DPI) is implemented to spot the bots behaviour and it reduced by assist of DNS packet load. DPI method cleans illegitimate entry towards DNS before bots try to enter. So, DPI method can able to suggest previous information about the Command and Control (CC) activities to reduce its performance. **Findings**: Monitoring the traffic over DNS and reducing the illegal connection from compromised host (botnet) using DPI were obtained in this study. **Applications:** Data secure can be created in Defence area, government sectors and private concerns.

Keywords: Botnet Avoidance, Botnet Communication, Botnet Propagation, Deep Packet Inspection (DPI), Tracking Botnet

1. Introduction

The contradictory among a bot and malwares is that the bot's has capable to deliver a Command and Control (CC) to take control of operating system and spontaneously making so many queries to raise the level of traffic over DNS. Thus, harmful Malicious are projected to obtain economic profits with help of victims hosts, called as bots. A group of contaminated bots hosts are called botnet[1]. As increasing activities of botnet in internet, it is tough to discover defence mechanism in respect to the speed of botnet because it automatically switches off/on the methods and commands activities. The ability of bots to produce separate path for launching a Command and Control (CC). Bots are stealing the confidential data via HTTP protocol, IRC since it is tough to differentiate from valid traffic over DNS. In order to slow down the DNS traffic, the proposed method in this study called Deep Packet Inspection (DPI) that provide consistent service and reduced Distributed Denial of Service (DDoS)[2].

2. Transmission of Botnet

Figure 1 shows the transmission of botnet. Botmaster who controls bots release are very harmful viruses and start scattering unsystematically to form victim cloud. Then virus insists target's system to join with botmaster's Command and Control server. The botmasters utilize services like spamming, phishing, Distributed Denial of Services (DDoS), identity theft etc. Every infected target

**Author for correspondence*

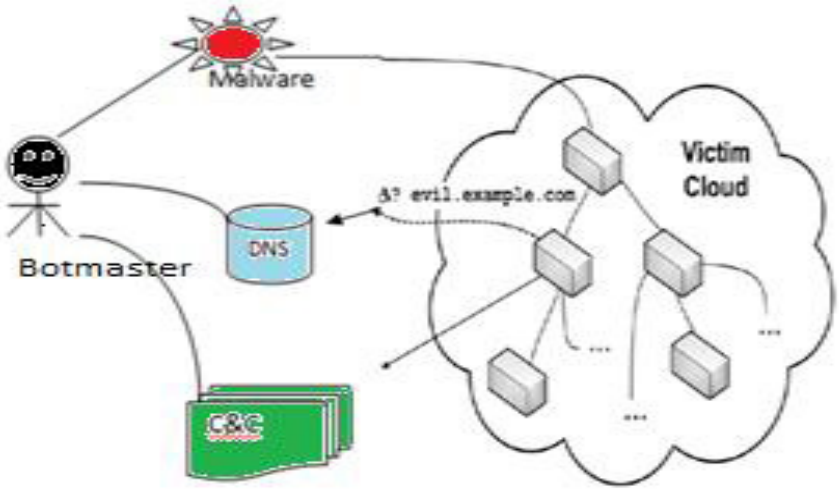


Figure 1. Botnet transmission.

systems then create victim cloud and spread virus to infect all hosts to connect botmaster's server, then bots make each infected systems to execute DNS lookups with innocent host name. Then botmaster could capable to manage the DNS resolution in the authority server side of particular domain. Then, botmaster can able to renumber the Command and Control of IP even when network administrator blocks the access[3].

3. Interaction Flow of Botnet

Figure 2 indicates the interaction flow of botnet. A cluster of infected system that works under Command and Control (CC) server can ultimately inspect entire range of network to infect numerous hosts that create Command and Control (CC) path via IRC, FTP and HTTP protocols that are used for communication over internet.

It is an easy task to avoid defenders detection by providing dynamic DNS names. By help of duplicate name, bots attempt to connect botmaster's channel with channel password. Now the attacker can able to issue command remotely over the channel like:

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

It orders botnets to copy a binary file via HTTP and implement it[4]. Suppose, the file doesn't consist of any commands, bots will remain until it receives command from botmasters. Nowadays attackers are regularly

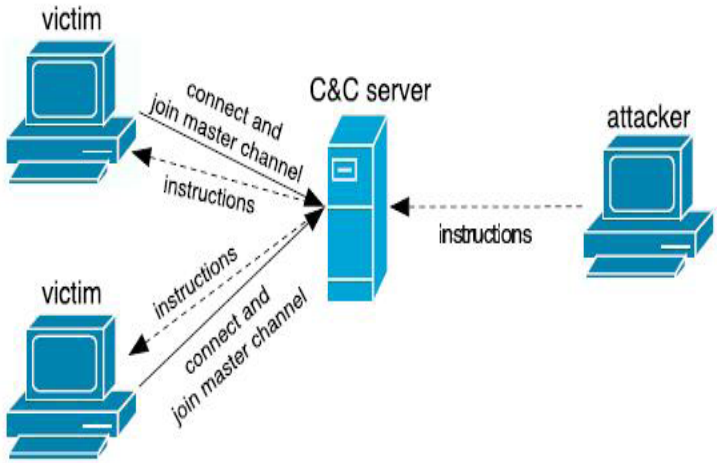


Figure 2. Interaction flow.

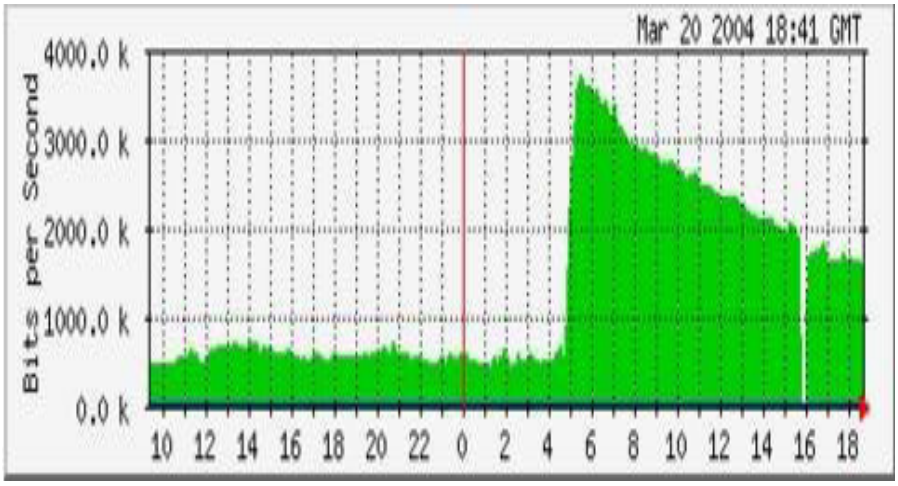


Figure 3. Sudden spikes in traffic.

launching DDoS over the internet by executing TCP SYN command like:

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

The above command line shows that the bots are waiting to launch new attack command (DDoS) in various compromised systems which issued by botmaster[4]. Figure 3 from the Team Cymru Web spot displays the behaviour of bots which sensed by Darknet once immediately released. A sudden network raise due to bots was observed in Figure 3.

4. Problem in Recognition of Botnet

Bots which are under Command and Control server aware that someone tries to identify it can randomly switch the control spot infinitely[5]. Botmaster reduce the possibility of identifying the bots in networks by creating a various Command and Control (CC) server. But, bots has ability to switch "ON" or "OFF" the activities of bots when defenders try to identify it. Then, queries from infected hosts enter into DNS as innocent hostname (e.g., A, MX, CNAME). Now, preference will be given to these innocent hostname over the DNS, so that it will generate a legal traffic.

- 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 as mentioned above, it is to perform Deep Packet Inspection (DPI) before bots enter into DNS.

5. Tracking and Evading the Botnet

5.1 Tracking Bots

Tracking bots can able to locate the movement of bots to avoid DDoS from compromised host[6]. Honey spots technique done for observation purpose is shown in the Figure 4. It helps to gather information perpetually about the behaviour of the host for post-incident forensic investigation purpose. By gathered information, honey spot tracks the prevailing of botnets from infected host[7]. Added that, when a bots attempts to communicate with botmaster's server it effectively attacks honey spot, then honey wall plays important task to track the bots activities. Honey wall offers the bridge between Capture and Data Control[8]. Data Capture decides DNS/IP address that the bot wants to communicate with botmaster's server and also port number[9]. Data Control assists in and out going suspicious communications that prohibit the bots movements. Thus, honey wall accumulates all essential information and honey spot able to track further bots activities.

5.2 Evading Botnet

Figure 5 shows evading botnets of DNS-based detection helps to evade the DDoS attack issued by botnets and

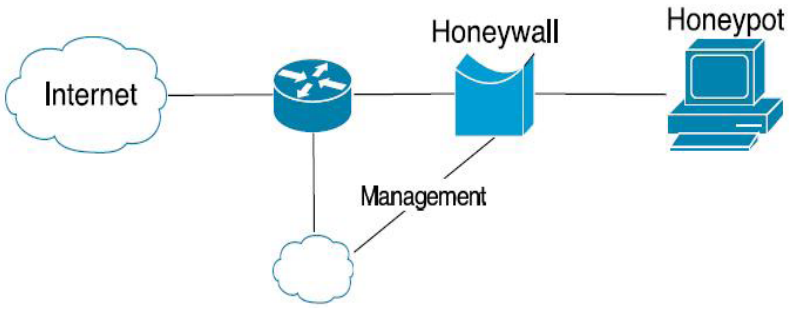


Figure 4. Tracking bots.

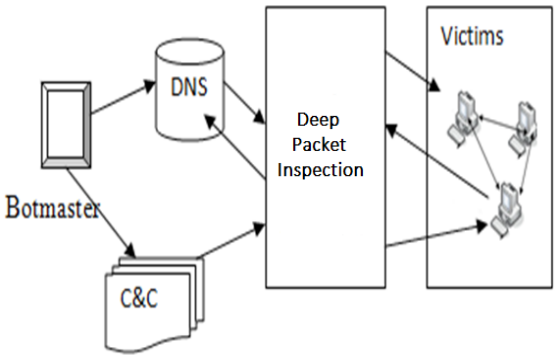


Figure 5. Evading botnet.

increases the service time. Bots have an ability to mix with legal traffic over the DNS queries to establish the harmful attack to target host. Thus, initially bots are allowed to enter Deep Packet Inspection (DPI) and check the payload to estimate the scatterings of DNS-Packet (bots). In Deep Packet Inspection, tunnelling with ordinary network traffic rate was observed and recorded long hours of traffic movement. The outcome illustrates tunnelling trace holds more illegitimate "A "and "TXT" type queries over DNS. In Figure 6, it was found that the relative tracing of Tunnelled normal data. Every red contour shows illegitimate bots activity in the network and green contour denotes usual traffic in the DNS[10]. Therefore, bots can be predicted and evaded by DPI.

6. Related Evaluations

6.1 Top Outbreaks in Botnet

Figure 7 shows outbreaks happened on 2009; Damballa witnessed thousands of illegitimate bonnet's activities

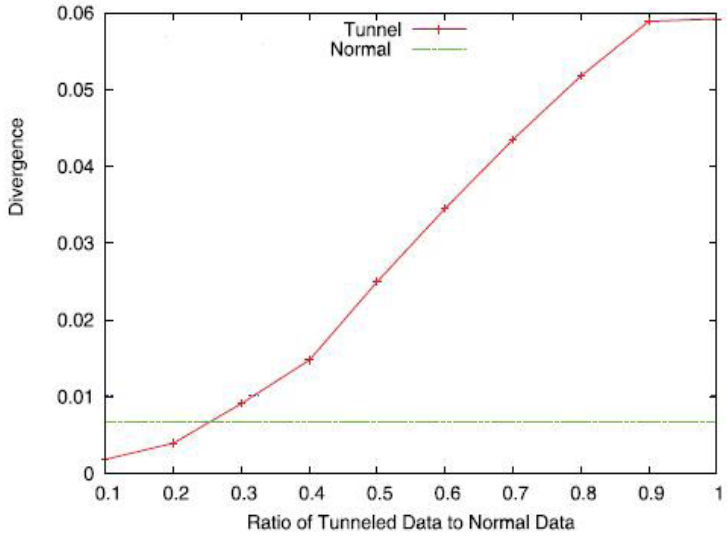


Figure 6. Comparison of normal and tunnelled flow.

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

Figure 7. Botnet outbreaks.

and identified millions of freshly negotiated systems over the network. Furthermore, specified that offenders can able to control bots over 600,000 victim's hosts and it has capacity to break millions of further systems.

6.2 Evidence for Botnet Detection

Figure 8 shows bots detection evidence happened on 2012, Kelihos/Waleda bots attained the control of more than 118,000 hosts of matchless ID's. Every single red mark shows affected systems of more than 430,000 matchless IP address from innumerable countries that looking to acquire the attack instruction from harmful bot server.

7. Conclusion

In this paper, Deep Packet Inspection (DPI) was inspected to identify bots behaviour in a network and it will be reduced by examining DNS packet payload. Deep Packet Inspection (DPI) method filter illegitimate bots passes over DNS and provide safety measures against botmaster's Command and Control (CC) server. This technique offers prior awareness about the Command and Control (CC) actions/attack issued by botmaster's which helps to reduce the bots activities.

8. References

1. Xu K, Saha S, Butler P, Yao D. DNS for massive scale command and control. IEEE Transactions on Dependence and Secure Computing. 2013 May-Jun; 10(3):143–53.
2. Ashok P, Manimala G. Detecting and preventing the malicious system based on DNS analysis. JCA. 2013; 6(3):62–5.
3. Deepak SR, Naveen G, Sushil KC. A study and detection of TCP SYN flood attacks with IP spoofing and its mitigations. Int J Computer Technology and Applications. 2012; 3(4):1476–80.



Figure 8. Evidence of botnet detection.

4. Dagon D, Zou C, Lee W. Modeling botnet propagation using time zones. Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS); 2006. p. 1–15.
5. Dietrich CJ, Rossow C, Freiling FC, Bos H, Van Steen. M, Pohlmann. N. On botnets that use DNS for command and control. 7th European Conference on Computer Network Defence; 2011. p. 9–16.
6. Mahmoudpour S, Mirabedini SJ. Diagnosis of distributed denial of service attacks using the combination method of Fuzzy Neural Network and evolutionary algorithm. Indian Journal of Science and Technology. 2015 Oct; 8(28):1–7.
7. Nagamuthu Krishnan SS, Saravanan V. A novel approach for mitigating distributed denial of service attacks drawn on bit-torrent protocol in computer networks. Indian Journal of Science and Technology. 2012 Jul; 5(7):3005–9.
8. Achar RK, Swagath Babu M, Arun M. Border gateway protocol performance and its protection against disturbed denial of service attack. Indian Journal of Science and Technology. 2015 Feb; 8(S2):127–32.
9. Kartaltepe EJ, Morales JA, Xu S, Sandhu R. Social network based botnet command and control: Emerging threats and countermeasures. Proc Eighth Intl Conf Applied Cryptography and Network Security (ACNS); 2010. p. 511–28.
10. Shaikh A, Tewari R, Agrawal M. On the effectiveness of DNS based server selection. Proceedings of IEEE INFOCOM; Anchorage, AK. 2001. p. 1801–10.