Design, Deployment and use of HTTP-based Botnet (HBB) Testbed

Esraa Alomari**, Selvakumar Manickam*, B. B. Gupta***, Parminder Singh*, Mohammed Anbar*

*National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Malaysia

**University of Wasit, Iraq, Wasit

***National Institute of Technology Kurukshetra, India

{esraa,selva,parminder,anbar@nav6.org}, gupta.brij@gmail.com

***Abstract*— Botnet is one of the most widespread and serious malware which occur frequently in today's cyber attacks. A botnet is a group of Internet-connected computer programs communicating with other similar programs in order to perform various attacks. HTTP-based botnet is most dangerous botnet among all the different botnets available today. In botnets detection, in particularly, behavioural-based approaches suffer from the unavailability of the benchmark datasets and this lead to lack of precise results evaluation of botnet detection systems, comparison, and deployment which originates from the deficiency of adequate datasets. Most of the datasets in the botnet field are from local environment and cannot be used in the large scale due to privacy problems and do not reflect common trends, and also lack some statistical features.**

To the best of our knowledge, there is not any benchmark dataset available which is infected by HTTP-based botnet (HBB) for performing Distributed Denial of Service (DDoS) attacks against Web servers by using HTTP-GET flooding method. In addition, there is no Web access log infected by botnet is available for researchers. Therefore, in this paper, a complete test-bed will be illustrated in order to implement a real time HTTP-based botnet for performing variety of DDoS attacks against Web servers by using HTTP-GET flooding method. In addition to this, Web access log with http bot traces are also generated. These real time datasets and Web access logs can be useful to study the behaviour of HTTP-based botnet as well as to evaluate different solutions proposed to detect HTTP-based botnet by various researchers.

***Keywords*— Cyber attacks, Botnet, DDoS attacks, HTTP-based botnet, HTTP flooding**

I. INTRODUCTION

Today, botnet is extensively used in various cyber attacks which lead to serious threats to ours network assets and organization's properties [1, 2]. Botnet detection is a very challenging issue which makes attention of several researchers for identifying the increasing issue of the malicious activities. The key elements for the analysis and development of adequate security solutions and for the training of security personnel and researchers, is to have an adequate test-beds which can be used to conduct security experiments and various test under controlled, safe and realistic environment. In particular, botnet detection has been the main focus of many of the researchers due to its potential in detecting novel attacks such as Zero-day attacks [3]. However, its adoption to real-world application has been obstructed owing to unavailability of a benchmark test-bed which is infected by HTTP-based botnet that can be used for testing, evaluation, and standardization of various detection and mitigation systems [4].

Running these detection and mitigation systems over real labelled network and application traces with a significant set of bots and abnormal behaviour is the most perfect methodology for testing, evaluating and validating the researcher's assumptions and systems. Although it is a considerable challenge, since the availability of such datasets are very rare. So far, there are several types of security benchmark datasets publicly available to the researchers such as KDD [5], DARPA [6], LBNL [7], DEFCON [8], CAIDA [8], which have been used to detect various types of attacks, and for systems evaluation. However, these are extensively criticized in the intrusion detection domain [9] and do not have any type of bot traces.

Recently, a new dataset released in the intrusion detection domain named as ISOT dataset [10] is created by using a systematic approach to create a profiles of such malicious traces and normal traffic, since this dataset meet a lot of researchers need. However, it has limitation that it has specific traces of specific type of botnet such as P2P botnets. Therefore, it is not a comprehensive dataset in terms of botnet traffic and also limited to various botnets, e.g. Waledac botnet, etc. Therefore, in this paper, a complete test-bed will be illustrated in order to implement a real time HTTP-based botnet for performing DDoS attacks against Web servers by using HTTP-GET flooding method [11]. In addition to this, Web access log with http bot traces are also generated. These real time datasets and Web access logs can be useful to study the behaviour of HTTP-based botnet as well as to proposed different solutions to detect HTTP-based botnet for the researchers who are new to this research domain.

The remainder of the paper is organized as follows. Section II contains the botnet threat evolution in HTTP attacks. Section III presents HTTP-based botnet structure. Some famous HTTP botnets which have been used in HTTP flooding DDoS attacks are described in section IV. Section V describes existing Botnet test-beds. Section VI presents overview of the proposed test bed setup and design. Finally,

Section VII concludes the paper and presents further research scope.

II. The Botnet Threat Evolution in HTTP Attacks

In past years, we have seen a change in the way of the attackers to control many botnets from IRC channels using HTTP [12]. Generally, the main advantage of using HTTP protocol is that the botnet traffic and normal web traffic both are same as the attack is in intent not in content [13]. Attack traffic will simply bypass firewalls which are port-based such as port 80 filtering mechanisms and avoid intrusion detection systems (IDS) detection. During this evolution, the attacker will exploit a Web server as a command and control (C&C) server often using PHP-based servers. After successfully installation to its C&C server, the attacker can generate its bots that will infect the victims known as "zombies" [14]. The commands are given after the online bot clients will communicate with C&C server and wait for a command from C&C server side. The attack target will be one or more such Web server or multi-Web servers.

III. HTTP-based Botnet Structure

Generally, the botnets can be classified into two categories depending on their topology structure: centralized botnets and distributed botnets. Recent HTTP-based centralized botnets that are often used for DDoS attacks [15, 16] are Black energy [17], Zemra [18], etc.

One of the most important aspects of HTTP-based botnets is that attacks are performed using web services that are used frequently on the Internet as a medium of instruction delivery, as it is difficult to close port 80 which is used for Web page communication and this port has a high proportion of normal traffic [19]. Figure 1 illustrates the structure of HTTP-based centralized botnets. Attackers can be cyber-attackers and spread bots to vulnerable PCs and servers by sending attack and control commands to zombies via a C&C server [20].

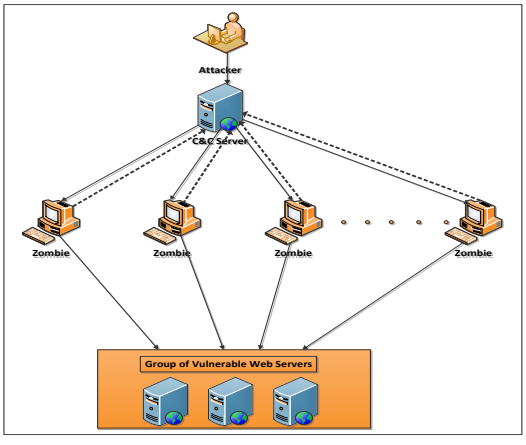

Figure 1. HTTP-based Botnet Structure

IV. Famous HTTP Botnets used for HTTP flooding DDoS attacks

This section will discuss some of the famous HTTP Botnets (e.g. Black Energy v.1.8 Bot and Zemra bot) used to perform HTTP flooding DDoS attacks.

A. *Black Energy v.1.8 Bot*

Black Energy v.1.8 is a Web-based botnet which is used to perform variety of Distributed Denial of Service (DDoS) attacks. It is developed by Russian hacker which previously had tied with Russian cyber crime organizations during the period started from 2007 to 2009. During this period, two versions of it were released in underground community such as Black Energy v.1.7 which was analysed by [21] and Black Energy v.1.8 which was analysed by [22]. Each Black Energy bot can create a set of instructions when implanted inside the victim such as injection, service creation and concession escalation in order to determine persistence on a victim system. Meanwhile, most Black Energy C&C systems are seen in Malaysia and in Russia, where Russian sites being the first. One of the main features that Black Energy bot advertise in forums is the ability to target more than one IP address per host name. This tool continues to be used to deny services from commercial Websites [23-25].

B. *Zemra bot*

Zemra bot is another type of HTTP-bot which has a C&C hosted in a remote server. Zemra botnet is mainly used to perform Distributed Denial of Service attacks and can perform two types of DDoS attacks such as HTTP flood and SYN flood attacks. A brief of additional functionalities of Zemra bot is listed below:

- Using AES encryption algorithm, 256 bits of traffic from the bot to the server
- USB Spread (spread through flash drives)
- Can use victim's pc as proxy by using SOCKS plug-in

V. Existing Botnet Testbeds

There are a lot of security test-beds such as Emulab [25], and Deter [26] are created to facilitate researchers for performing various experiments. These test-beds are heavily used for both research and application testing in security fields. These also offer the researchers and practitioners the only viable platforms to test their ideas and application beyond custom built corporate clusters. Although a step forward, current test-bed platforms fall short in terms of testing botnets by two issues:

- The testing when it comes to scale to ten or even hundreds thousands of application or service instances.
- The expecting danger when testing botnets on the wired test-bed especially the Distributed Denial of Service (DDoS) attacks scenarios where it needs a huge number of machines to perform the attack [27].

To address this shortcoming and to allow existing test-bed infrastructure to scale even further, researchers have turned to Virtualization Technologies.

VI. Overview of Proposed Test-bed Setup and Design

For test-bed users, there is need of a test-bed which includes a repository of attack traffic generators, monitoring tools, topology generators, and other tools, and work is underway to integrate these tools into an experimenters' workbench which will simplify the task of getting new experiments up and running. Test-bed consists of hardware (i.e. a set of high-end PCs as experimental nodes) and extensive control software. Flexibility and usability of the control software is very important in fulfilling the needs of test-bed users.

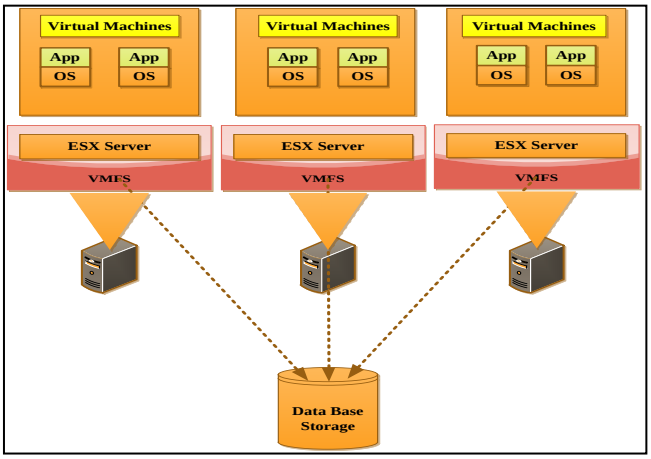

Figure 2. Virtual Machine System

Our proposed test-bed is setup using VMware server infrastructure as shown in Figure 2. It uses client-server model by allowing remote access to virtual machines, the description of the VMware server is as below:

- Dell Blade Chasis M100OC with Power Edge M 610 Server.
- Dual Quad Core Processor / 16 GB / 600 GB MDD.
-

TABLE 1. Virtual Machine Descriptions

Number of Machines	Operating System	H/W Details	Purpose
30	XP2	2G HD, 128MG RAM	Zombies
10	Win-7	10G HD, 1G RAM	Zombies
1	Win-7	10G HD, 1G RAM	Monitoring
1	XP3	5G HD, 256MG RAM	Command & Control Server + Attacker
1	Ubuntu 12.04	10G HD, 1G RAM	Target Web Server (Victim)

A. HTTP Botnet Test-bed Description

In order to present the HTTP botnet scenario that is used to launch Distributed Denial of Service (DDoS) attacks, we have created 43 VMware machines and the details of these machines is shown in the Table 1. The completed scenario of the HTTP botnet is illustrated in Figure 3.

B. Botnet Test-bed Network Architecture

The test-bed network consists of 43 interconnected Windows workstations. The Windows operating systems is chosen so that it could meet the requirements of the botnet. Thirty workstations were installed with Windows XP SP2, ten workstations with Windows 7, and one workstation with SP3. As shown in Figure 3, switch is configured in such a manner that all the nodes are connected to it. The command and control server (C&C) (192.168.171.50) is responsible for controlling the zombies by given commands. Target Web Server (192.168.171.20) is responsible for delivering the target Website and monitoring workstation (192.168.171.144) monitor all the traffic in the network.

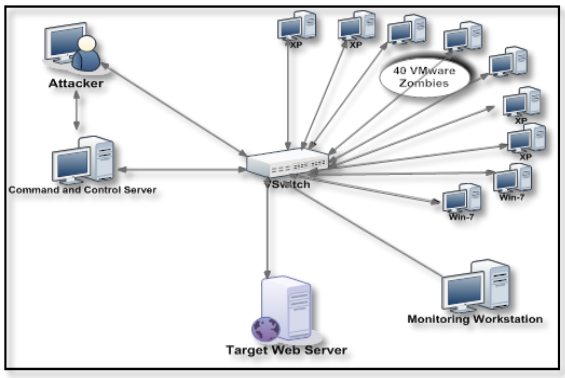

Figure 3. HTTP Botnet VMware Testbed Structure

C. Sample HTTP Botnet Trace file

In network security field, the researchers need malicious trace files for evaluation and validation of their system. Therefore, in this section, we present sample results which are generated from HTTP-based botnet (HBB) test-bed in the form of trace file of HTTP-based botnet when launching HTTP-based flooding Distributed Denial of Service (DDoS) attacks. Figure 4 depicts a snapshot of web access log with botnet trace file generated using HTTP-Based Botnet (HBB) test-bed with more than one signature.

```
192.168.1.3 - - [17/Nov/2013:20:30:38 +0800] "GET /robots.txt  HTTP/1.1" 302 304 "-"
"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"
192.168.1.4 - - [17/Nov/2013:20:30:39 +0800] "GET /index.php HTTP/1.1" 200 76 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)"
192.168.1.5 - - [17/Nov/2013:20:30:39 +0800] "GET
/Publication/download/mosleh.A%20NEW%20TRANSPORT%20PROTOCOL%20%20F
OR%20VOIP%20APPLICATIONS.pdf
HTTP/1.1" 304 - "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X)
AppleWebKit/536.26 (KHTML, like Gecko) Version/6.0 Mobile/10A5376e Safari/8536.25
(compatible; Googlebot-Mobile/2.1; +http://www.google.com/bot.html)"
192.168.1.6 - - [17/Nov/2013:20:30:39 +0800] "GET /index.php HTTP/1.1" 200 76 "-"
"Mozilla/5.0 (Windows; U; Windows NT 5.1; ru; rv:1.8.1.1) Gecko/20061204
Firefox/2.0.0.1"
```

Figure 4. Sample HTTP botnet trace file

VII. CONCLUSIONS

In this paper, we have outlined various challenges and drawbacks of current test-beds and datasets available to study the behaviour of HTTP-based botnet as well as to evaluate different solutions proposed to detect HTTP-based botnet by various researchers. In addition, we discussed how we can overcome the shortcomings of existing test-beds by designing and implementing a real time test-bed for botnet researchers. HTTP-bots are installed and used to perform HTTP flood DDoS attacks against target Web server to HTTP-bot traces. In future, we will work to install other types of botnets such as IRC, P2P botnets, etc.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper. This original research was supported by the RUT grant of University Science Malaysia (USM) (Grant No. 1001/PANY/857001).

REFERENCES

[1]. A. J. Aviv and A. Haeberlen, "Challenges in experimenting with botnet detection systems," in USENIX 4th CSET Workshop, San Francisco, CA, 2011.

[2]. Z. Zhu, G. Lu, Y. Chen, Z. J. Fu, P. Roberts, and K. Han, "Botnet research survey," in Computer Software and Applications, 2008. COMPSAC'08. 32nd Annual IEEE International, 2008, pp. 967-972.

[3] A. ALmomani, T.-C. Wan, B. B. Gupta, A. Altaher, E. A. Lmomani and S. Ramadass, "A Survey of Phishing Email Filtering Techniques," IEEE Communications Surveys & Tutorials, 15 (4), pp. 2070-2090, 2013.

[4] J. Calvet, C. R. Davis, J. M. Fernandez, W. Guizani, M. Kaczmarek, J.-Y. Marion, and P.-L. St-Onge, "Isolated virtualised clusters: testbeds for high-risk security experimentation and training," in Proceedings of the 3rd international conference on Cyber security experimentation and test (Berkeley, CA, USA, 2010), CSET, 2010, pp. 1-8.

[5] University of California. KDD Cup 1999 data, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html; 2011.

[6] Lincoln Laboratory MIT. DARPA intrusion detection evaluation, http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/index.html; 2011.

[7] Lawrence Berkeley National Laboratory and ICSI. LBNL/ICSI enterprise tracing project. www.icir.org/enterprise-tracing/.

[8] The Shmoo Group. Defcon, http://cctf.shmoo.com/; 2011.

[9] CAIDA. The cooperative association for internet data analysis, http://www.caida.org/; 2011.

[10] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln Laboratory," ACM transactions on Information and system Security, vol. 3, pp. 262-294, 2000.

[11] http://iscx.ca/datasets.

[12] B. B. Gupta, R. C. Joshi and M. Misra, "Defending against Distributed Denial of Service Attacks: Issues and Challenges," Information Security Journal: A Global Perspective, Vol. 18, No. 5, 2009, pp. 224-247.

[13] Y. Emre, "A Literature Survey About Recent Botnet Trends," 2011.

[14] A. Karasaridis, B. Rexroad, and D. Hoeflin, "Wide-scale botnet detection and characterization," in Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, 2007.

[15] A. Mishra, B. B. Gupta and R. C. Joshi, "A Comparative Study of Distributed Denial of Service Attacks, Intrusion Tolerance and Mitigation Techniques," European Intelligence and Security Informatics Conference, EISIC 2011, 12-14 September 2011, pp. 286, 289.

[16] A. Srivastava, B. B. Gupta, A. Tyagi, A. Sharma and A. Mishra, "A Recent Survey on DDoS Attacks and Defense Mechanisms," Proceedings of the First International Conference on Parallel, Distributed Computing Technologies and Applications (PDCTA-2011), Tirunelveli, 23-25 September 2011, pp. 570-580.

[17] B. B. Gupta, M. Misra, R. C. Joshi, "FVBA: A Combined Statistical Approach for Low Rate Degrading and High Bandwidth Disruptive DDoS Attacks Detection in ISP Domain, ‖ in the proceedings of 16th IEEE International Conference on Networks (ICON-2008), New Delhi, India, 2008.

[18] J. Nazario, "Blackenergy ddos bot analysis," Arbor, 2007.

[19] http://www.hackreports.com/2012/07/download-zemra-botnet-ddos-attack.html.

[20] N. Maheshwari, "Botnets—Secret Puppetry with Computers."

[21] B. B. Gupta, N. Jamali, "Predicting Number of Zombies in a DDoS Attacks Using Isotonic Regression," Mining Social Networks and Security Informatics, Springer, pp. 145-159, 2013.

[22] Black Energy DDoS Bot Analysis http://atlaspublic.ec2.arbor.net/docs/BlackEnergy+DDoS+Bot+Analysis.pdf .

[23] E. Alomari, S. Manickam, B. Gupta, S. Karuppayah, and R. Alfaris, "Botnet-based Distributed Denial of Service (DDoS) Attacks on Web Servers: Classification and Art," arXiv preprint arXiv: 1208.0403, 2012.

[24] http://media.blackhat.com/bh-us-12/Briefings/Jones/BH_US_12_Jones_State_Web_Exploits_Slides.pdf

[25] M. Hibler, R. Ricci, L. Stoller, J. Duerig, S. Guruprasad, T. Stack, K. Webb, and J. Lepreau, "Large-scale Virtualization in the Emulab Network Testbed," in USENIX Annual Technical Conference, 2008, pp. 113-128.

[26] L. Li, P. Liu, Y. Jhi, and G. Kesidis, "Evaluation of collaborative worm containment on the DETER testbed," Proc. DETER Community Work. on Cyber Security Experimentation and Test (CSET).(August 2007), 2007.

[27] Gupta, B., R. Joshi, and M. Misra, Prediction of Number of Zombies in a DDoS Attack using Polynomial Regression Model. Journal of Advances in Information Technology, 2011. 2(1): p. 57-62.

Esraa Alomari has done a Bachelor in Computer Science from computer collage- Al-anbar University-IRAQ in 2003 and received her MSc. Degree in Computer Science from University of Technology-IRAQ in 2006. Currently, she is a PhD student in National Advanced Center of Excellence (Nav6) in University Sains Malaysia (USM). Her research interest includes Advances internet security and monitoring, Botnet and Cyber attacks. She is member of the IPv6 Forum Global Education where she plays a role in the validation of IPv6 engineers, trainers and courses worldwide. In addition, she is actively involved in conducting professional courses on IPv6, including Certified IPv6 Network Engineer (CNE6) Level 1&2.

Selvakumar Manickam is Deputy Director at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. He received his Bachelor of Computer Science and Master of Computer Science in 1999 and 2002, respectively. He has published more than 80 papers in journals, conference proceedings, book reviews, and technical reports. He has also given several key note speeches as well as dozens of invited lectures and workshops at conferences, international universities and for industry. He has given talks on IPv6, Internet Security, Green ICT and Open Source technologies at various organizations and seminars. Currently, he spearheads a number of key clusters under National Advanced IPv6 Centre, namely Internet Security, Cloud Computing, Android and Open Source Technology, focusing on conducting scientific research in respective areas. He manages two teams, network and system support team and the software and web application team. He holds various research grants in the university at national and international level. Due

to his proven expertise in Internet Security, he has also been given the responsibility to lead the Internet Security Working Group of the Malaysian Research and Education Network (MYREN) to facilitate collaboration among researchers and other security enthusiasts nationwide. He is an Executive Council member of Internet Society (ISOC) Malaysian Chapter. He is also an appointed core member of the IPv6 Forum Global Education where he plays a role in the validation of IPv6 engineers, trainers and courses worldwide. He is involved with International Telecommunication Union (ITU) in which he runs online trainings on IPv6 topics. Apart from that, as senior trainer, he is actively involved in conducting professional courses on Android, Web Application Development and IPv6, including Certified IPv6 Network Engineer (CNE6) Level 1&2 and Certified IPv6 Security Engineer (CSE6). He is also involved in the development of next generation network monitoring platform and plays the role of project manager and an avid ANSI C programmer.

B. B. Gupta (gupta.brij@gmail.com) received PhD degree from Indian Institute of Technology Roorkee, India. In 2009, he was selected for Canadian Commonwealth Scholarship and awarded by Government of Canada award. He has published more than 45 research papers in International Journals and Conferences of high repute. Dr Gupta is also holding position of editor of various International Journals and magazines. He also worked as a post doctoral research fellow in UNB, Canada. His research interest includes Information security, Cyber Security, Intrusion detection, Computer networks and Phishing.

Parminder Singh is a visiting researcher at National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia and Principle Consultant at DCS1 Enterprise Solutions private Limited. He is a skilled and result oriented professional with 15+ years of experience in the IT industry and working in key managerial and technical positions. He has an edge over technical aspects such as ethical hacking, operating systems, scripting and databases. He is leading the teams of Internet Security, Cloud Computing and Open Source Technology, and focusing on conducting scientific research in respective areas. He is also an active Member of Internet Security Working Group of the Malaysian Research and Education Network (MYREN). He is member of the IPv6 Forum Global Education where he plays a role in the validation of IPv6 engineers, trainers and courses worldwide. In addition, he is actively involved in conducting professional courses on IPv6, including Certified IPv6 Network Engineer (CNE6) Level 1&2 and Certified IPv6 Security Engineer (CSE6).

Mohammed Anbar is a Post Doctoral Fellow in National Advanced IPv6 Centre of Excellence (NAV6) at Universiti Sains Malaysia (USM), Malaysia. He holds a PhD in the area of Advanced Computer Networks, M.Sc. in Information Technology, and B.Sc. in Computer System Engineering. His research interest includes Malware Detection, Web Security, Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and network monitoring.