Volume 5, Issue 9, September 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

HTTP Header File Image Plantation Mechanism

Rishikesh C Gaikwad
Computer & Savitribai Phule, Pune University,
Maharashtra, India

Abstract— The amount of Botnet is increasing day by day across the world in recent years. If we are not able to find any solution on this process then such type of issues will create more dangerous attack in future. HTTP Botnet use one of the important protocols while transmitting malicious code and that is HTTP protocol with port 80.The attack becomes so easy that neither firewall nor Intrusion detection system can stop it. Proposed system uses "Repeatability Standard Deviation" method so as to detect the interconnection of malicious Botnets within HTTP protocol. After this, one system uses the JXT A P2P network to share the detected results, and users can compare the packets of traffic with lists of the filtering mechanism. The technique Peer to Peer which is to exchange the information we can detect, those end users who are getting infected can find the connection of HTTP Botnet servers and uninfected users will able to use this information as a comparison sample, once they get new packets. End users will use it for determining whether the connections are infected or not, and this will help to make their system more defensive. The peer to peer technique will decrease the cost of implementation, and will make the network more resilient.

Keywords—HTTP Botnet, Malicious threats, DDoS attack, Standard Deviation Method, Network Behavior Analysis

I. INTRODUCTION

Botnet are attacking one computer in a network and attacking other computers or nodes in the same network with the help of HTTP protocol. It is appearing on Internet since 1990 and developed to Peer-to-peer bots after 2000. Most recently, it has developed HTTP bots. The Kraken, a part of HTTP botnets, becomes a malicious network with more than 400 thousand bots. According to internal Microsoft network environment, we find that there are at least more than 220 computers, reduced to a fixed control Botnet virus host, as hackers attack the springboard for a particular object. We can simply change the criteria of sending address in the HTTP header by an image. As our earlier methodology is using sender and receivers IP address in the header file of the HTTP protocol, we should be sending it in a image format so that it cannot be edited. The observation says that the HTTP header file is hampered by attackers and then the packets are sent across, while having image as the address in the header file the same cannot be overwritten or hampered.
PGRP is used to reduce brute force and dictionary attack and this protocol is not having any significant impact on usability. Internet worm infection continues to be one of top security threats and has been widely used by botnets to recruit new bots. It is also called as Worm tree infection.

II. LITERATURE SURVEY

Existing System

In the centralized architecture, bots in the botnet connect directly to some special hosts or target hosts called command and control servers ("C & C" servers).These C&C servers receive commands from their botmaster and forward them to the other hosts in the network with the help of header file address mentioned in HTTP Protocol. It also spreads to some of the peer-to-peer botnets like Slapper, Sinit, and Phatbot.

HTTP Header File Format.

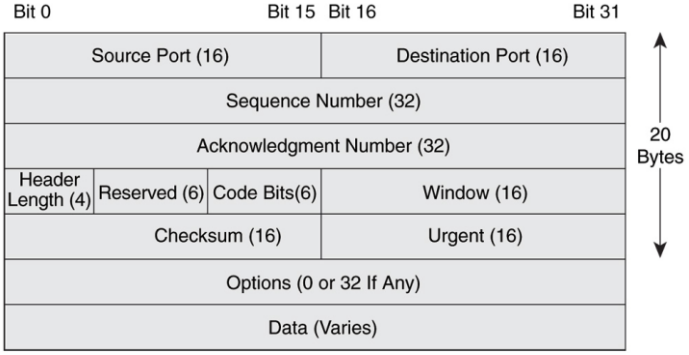

Fig. 1: HTTP Protocol Format

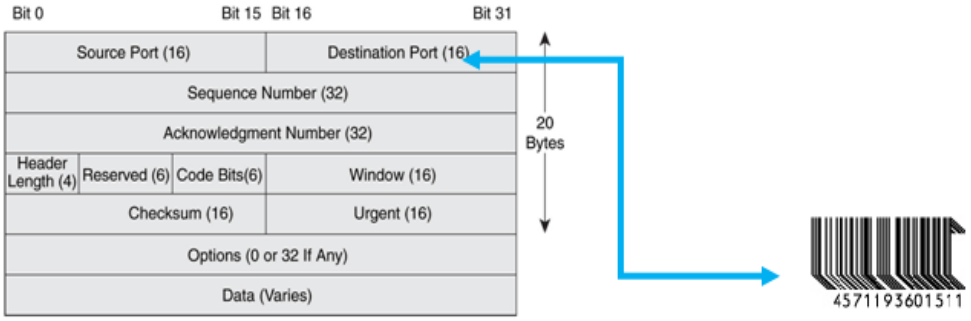

Fig 2: Image Replacement of for Destination address

Bar code generator will generate image randomly at both ends (senders and receivers) and will cross verify at both ends. Botmaster will not able to edit the image and will help to prevent botnet attack. We can elaborate botnet event as a group of coordinated bots which makes the target network with the same goal. Here in this case the same goal means the probes are using the same protocol(s).We define a session as a set of connections between a pair of hosts with a specific purpose , perhaps involving multiple application protocols.

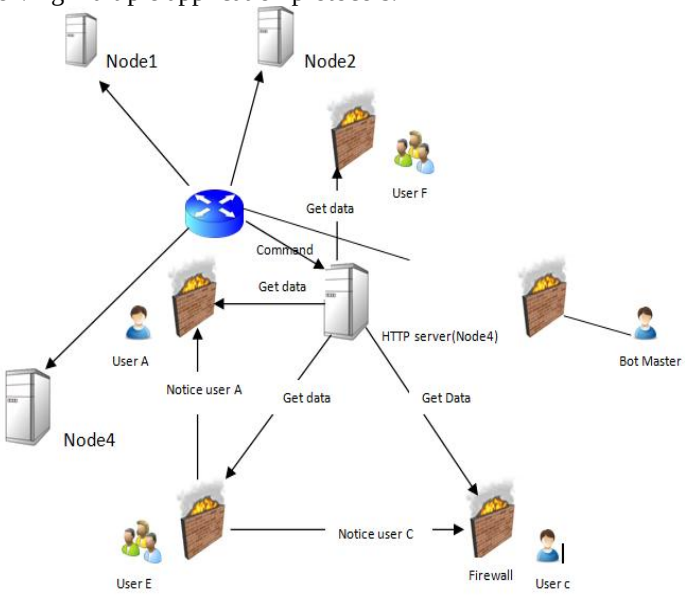

Fig.3. C&C architecture of a C&C botnet

Botnet Analysis

We need to launch Denial of service attacks and stealing personal data has a sophisticated word which is called as Torpig. All bots communicate with the Torpid C&C through HTTP post requests, using the URL that contains the hexadecimal representation of the bot identifier and a submission header.

DNS resources records

The DNS system allows a name server administrator to associate different types of data with either a fully qualified domain name or an IP address. To send a message to a bot; an adversary can store data in any one of these types of records:

1. A record specifies an IP address for a given host name.
2. CNAME and MX records can point to textual data representing the alias or mailing host of a particular host name.TXT records are designed to store arbitrary textual data up to 255 characters.
3. EDNS0 record allows storing up to a 1,280-byte payload. EDNS0 was introduced in RFC261 to extend the DNS protocol. When a capable server or client encounters this field, it can decode the packets, allowing several improvements to the basic DNS protocol. These features include larger UDP packet size, a list of attribute value pairs, and several extra bytes for commonly used flags.

Proposed Work:

In the proposed System, it presents the design of Dynamic bots monitoring in peer-to-peer botnet. Compared with current botnets, the proposed botnet is harder to be shut down, monitored, and hijacked. It provides robust network connectivity, individualized encryption and control traffic dispersion. The botnet requires no bootstrap procedure. The botnet communicates via the peer list contained in each bot. A botmaster could easily monitor the entire botnet by issuing a report command. This command instructs all (or partial) bots to report to a compromised machine (which is called a sensor host) that is controlled by the botmaster. The IP address of the sensor host, which is specified in the report

command, will change every time a report command is issued to prevent defenders from capturing or blocking the sensor host beforehand. After a report command has been sent out by a botmaster, it is possible that defenders could quickly know the identity of the sensor host (e.g., through honeypot joining the botnet and then either shut it down or monitor the sensor host.

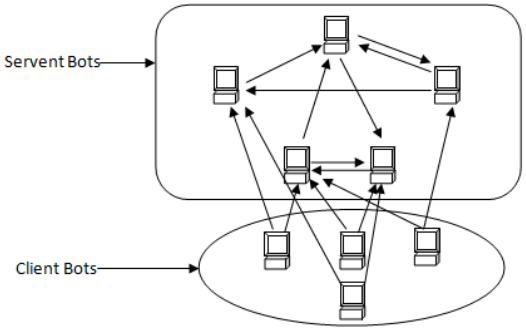

Fig.4: C&C architecture of the proposed hybrid P2P botnet

IMPLEMENTATION DETAILS PLAN

Techniques and Approaches

Network behaviour analysis technique and Degree of periodic repeatability is used to figure out the attacked computer system available in the network.

Detection technique:

Repeat first calculates the standard deviation of a standard deviation of each Bi, and then uses every Bi, repeat the standard deviation calculation. T for the Bi sample number, then take the square of a Bi, after accumulation divided by T, you can repeat the standard deviation calculated.

$$B_l = \sqrt{\frac{\sum(Y_{lm}-\overline{Y_l})^2}{(F-1)}} \quad \text{---------- (1)}$$

l to 1- F, B_i for every standard deviation, Y_l for the time, Y_{lm} as the time difference which l_i to Y_{l+1} , X_l as the average which Y_l to Y_l

$$B_r = \sqrt{\sum_{l=1}^{T} B_l^{\,2} / T} \quad \text{---------- (2)}$$

B_r for Repeat the standard deviation, B_i for each standard Deviation, T for the sample number.

MATHEMATICAL MODEL -

- Switch is denoted by S_w
- Router is denoted by R
- Hub is denoted by H
- Network cable or patch cable is denoted by N_c
- C= (C1,C2,C3,…..,C_n)
- N =(R ,S_w,N_c,H)
- S = (C,W,N)
- Size of the botnet peer list is denoted by M, then as per Fig.3 each bot has at least M venues.
- Public key is denoted by K^+ and private key is denoted by K^-
- Botmaster which generates a pair of public/private keys, (K^+ or K^-), and hard codes the public key K^+ into the bot program before releasing and building the botnet is denoted by A
- The peer list on bot A is denoted by L_A
- Encryption key is denoted by K_i
- IP address and symmetric key used by servant bot i_j is denoted by IP_{ij}
- Symmetric key used by servant bot i_j is denoted by K_{ij}
- IP address of B system is denoted by $IP_{A.}$
- Encryption key of B system is denoted by K_A
- There is no need for key distribution because the public key is hard-coded in bot program. The command messages sent from the botmaster could be digitally signed by the private key K^- to ensure their authentication and integrity.
- In the proposed botnet, each servant bot i randomly generates its symmetric encryption key K_i. Suppose the peer list on bot A is denoted by L_A.
- It will not only contain the IP addresses of M servant bots, but also the symmetric keys used by these servant bots. Thus, the peer list on bot A is L_A = {(IP_{i1}, K_{i1}), (IP_{i2}, Ki2) . . . (IP_{iM}, K_{iM})}, where (IP_{ij}, K_{ij}) are the IP address and symmetric key used by servant bot i_j. With such a peer list design, each servant bot uses its own symmetric key for incoming connections from any other bot.

- This is applicable because if bot B connects to a servant bot A, bot B must have (IP_A, K_A) in its peer list.
- The communication traffic happens through service port since the servant bots needs to accept connections from other bots; it must run a server process listening on a service port. The service port number on servant bot i, denoted by P_i could be picked by the bot either randomly or selectively. Considering this a peer list needs to contain the service port information as well.
- e.g. The peer list on bot A is
- LA = {IPi1, Ki1, Pi1). . . (IPiM, KiM, PiM) }. With the new peer list L_A bot A can connect to any servant bot.
- Let C (p) denotes the connected ratio and D (p) denote the degree ratio.
- C (p) and D (p) are defined as

$$C(p) = \frac{\text{\# of bots in the largest connected graph}}{\text{\# of remaining bots}}$$

$$D(p) = \frac{\text{Average degree of the largest connected graph}}{\text{Average degree of the original botnet}}$$

Hardware Requirement

1. Three Desktop Systems(Min RAM 512 MB, Min 80 GB HDD ,Min 1 MB cache)
2. LAN cards
3. HUB/Switches
4. Networking cable

Software Requirement

1. C# Language
2. SQL 2003
3. Windows 7 or XP Desktop OS
4. Windows 2003 server (Operating System)
5. VMware WorkStation 8.0

III. RESULTS

By applying standard deviation formula as a logic while implementing bot detection software the network behaviour analysis method will show performance statistics of the entire network to point out the packet which is corrupted or the system which is infected and working as a C&C centre to send confidential information outside the network to botmaster. We can then determine what all the PCs are getting affected and how it can be reduced.

IV. CONCLUSIONS

Bot can attack n number of nodes, networks and organizations and can spread very rapidly. By using image insertion method Botmaster will never able to edit the image to send the bot along with the HTTP and even if edits the HTTP header image will never get matched at the destination address so will not get delivered. HTTP protocol is used for web communication but the bot is carried on its head only and this bot cannot be blocked because HTTP itself cannot be blocked by any firewall as it is a disadvantage of HTTP. By using this system one can early detect the suspicious activities of bots and block them at early stage. By using the Image replacement Technique, our system can easily monitor the network behavior of the computers and detect the activities. The network of botnet is unbreakable but our system gives a way to block the activities on individual level.

ACKNOWLEDGMENT

With immense pleasure, I am presenting this Paper on HTTP Header File Image plantation mechanism as part of the curriculum of M.E. Computer Engineering. Inspiration and guidance are invaluable in every aspect of life especially in the field of academics, which I have received from our respected Ms. Arti Mohanpurkar: Head of Computer Department, I would also like to thank all my colleagues who have directly or indirectly guided and helped me in the preparation of this seminar and also for giving me an unending support right from the stage this idea was conceived. I also acknowledge the research work done by all the researchers in this field.

REFERENCES

[1] Anup Goyal, Yan Chen, Zhichun Li, and Vern Paxson, *"Towards Situational Awareness of Large-Scale Botnet Probing Events"* IEEE Transactions on Information Forensics and Security, Vol. 6, No. 1, pp 176 March 2011

[2] Brett Stone-Gross, Marco Cova, BobGilbert, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna, *"Analysis of a Botnet Takeover "* IEEE Journal Paper ,January 2011

[3] Chao Yang, Robert Harkreader, and Guofei Gu*, "Empirical Evaluation and New Design for Fighting Evolving Twitter Spammers*", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 8, August 2013

[4] Guofei Gu, Narasimha Reddy, Fellow, Seungwon Shin and Christopher P. Lee, *"A Large-Scale Empirical Study of Conficker* ", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, April 2012

[5] Jérôme François, Issam Aib, and Raouf Boutaba, Fellow *," FireCol A Collaborative Protection Network for the Detection of Flooding DDoS Attacks "*IEEE/ACM Transactions on Networking, Vol. 20, No. 6, December 2012

[6] Katerina Argyraki and David R. Cheriton*," Scalable Network-Layer Defense against Internet Bandwidth-Flooding Attacks "*IEEE/ACM Transactions on Networking, vol. 17, No. 4, pp 1286, August 2009

[7] Mansour Alsaleh, Mohammad Mannan, and P.C. van Oorschot*, "Revisiting Defenses against Large-Scale Online Password Guessing Attacks* ", IEEE Transactions on Dependable And Secure Computing, Vol. 9, No. 1, pp 130 January/February 2012

[8] MyungKeun Yoon, *"Using Whitelisting to Mitigate DDoS Attacks on Critical Internet Sites "*IEEE Communications Magazine, July 2010

[9] Ping Wang, Sherri Sparks, and Cliff C. Zou, *"Advanced Hybrid Peer-to-Peer Botnet*, IEEE Transactions on Dependable and Secure Computing, vol. 7, no. 2, April-June 2010

[10] Patrick Butler, Sudip Saha, and Danfeng (Daphne) Yao, Kui Xu, *"DNS for Massive-Scale Command and Control* ", IEEE Transactions on Dependable and Secure Computing, Vol. 10, No. 3, May/June 2013

[11] Qian Wang, Zesheng Chen, and Chao Chen, *"On the Characteristics of the Worm Infection family tree",* IEEE Transactions On Information Forensics And Security, Vol. 7, No. 5, October 2012

[12] Meisam Eslahi, "*Improving HTTP based Botnet Detection by using Network Behavior Analysis System*", University of Malaysia, 2010.

[13] Tung-Ming Koo, Hung-Chang Chang, Guo-Quan Wei "*Construction P2P Firewall HTTP-Botnet defense Mechanism*", IEEE National Yunlin University, 2011

