2011 2nd International Conference on Networking and Information Technology
IPCSIT vol.17 (2011) © (2011) IACSIT Press, Singapore

IRC Botnet Major Issues and Solutions

Arash Habibi Lashkari[1], Seyedeh Ghazal Ghalebandi[2], Shahab Alizadeh[3] and Rohini Devi[3]

[1]Faculty of Computer Science, Binary University College, Puchong, Malaysia

[2]Faculty of Computer Science, University of Malaya (UM), Kuala Lumpur, Malaysia

[3]Faculty of Computer Science, Binary University College, Puchong, Malaysia

a_habibi_l@hotmail.com,gazelle.ghalebandi.it@gmail.com,shabi1200@yahoo.com,rohinids@binary.edu.my

Abstract. The sharing of information during communication has been the main driver behind the research into criminal activities such as identity theft, phishing, and spam. Behind most of these activities are little programs that infect the users' system without the user's knowledge, or Botnets. The severity of such infections depends on the system's level of security, user awareness and the system's degree of vulnerability. There is a lot of paper that represent problem and detection methods, but the area of study is vast, hence this paper is deduced based on reviewed papers about this topic and clarified some problems and existing common solutions in a simple classification. Finally, paper tries to find the best solution for each problem regarding to related researches and resources.

Keywords-Botnet, Botnet Detection, IRC Botnet

1. Introduction

The term used for many types automated software is "bot" (from the word "robot"). A type of bot that allows attackers to have full access and control over the user's computer is called a malware [21].

A botnet is a common controller that affects several machines. Bots are typically different from viruses or worms. Instead of just removing an infected node, bots can only be taken down via the whole botnet.

The initial stage of botnet begins with the downloading of a software program. These malicious software will then compromise the machines and use it for criminal purpose. The threat botnet is very real. They are evolving at an alarming rate and the severity of the problems caused is still not properly understood. The best way of dealing with botnets is to tackle the problem at the C&C server side. Being highly dynamic with the ability to adapt and avoid security defence means that botnet is almost close to impossible to being detected.

In regards to bot detection, there are several collaborations intended to takedown bots and botnets in infected systems, especially the C&C servers. By using sophisticated heuristic methods and analysis techniques found in AV scanners and spam filters, plus other techniques, are used to increase detection rate of bots. It is obvious that the primary threat to system security in the Internet today is botnets. Here are several common botnet related tasks that are carried out:

- Self-propagation through the distribution of malware
- Spam dissemination through the establishment of SMTP relays and open proxies
- Denial of Service (DoS) attacks
- Click Fraud

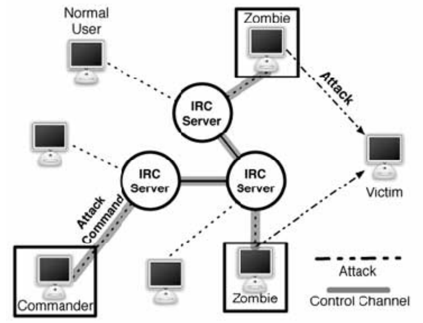

Figure 1. BotNet Detection

2. Problems

In this part, we explain twenty articles from botnet detection based on IRC botnets by focusing on problems:

- The lack of necessary and mutual cooperation between ISPs plus the lack of speed to tackle the botnet evolution within the current technology found in many countries [1].
- There are still weaknesses present in the current detection designs that are unable to discover collaborative botnets [2].
- The methods of detecting botnets require a lot of computational power and memory resources. Complex algorithms are used to run small set of flows. The cost is too high to identify botnet flow presence as well as the current analysis method of machine learning and flow correlation. It becomes a statistical problem to run large scale sets of chat identification traffic flow. [3]
- Even by intercepting network traffic, it is difficult to observe botnets [6].
- Delivering messages is unreliable and spam has become a nuisance to users. These messages can contain malicious software that phish personal information from users as well as containing dangerous executable files. The hidden communication channels that are present in emails and spam mail provides an opportunity for botnet to control. The messages containing the botnet command can and will affect the internet operation beyond the bandwidth and storage used by spam [6].
- Major threats existed thanks to a large number of botnets spam [8].
- It is hard to take down botnets when legitimate IRC servers are used to command the bots [4].
- Attacks are made by coordinated servers [15].
- The attackers are able to convincingly mimic legitimate users' behaviour. One of the major threat of botnet are DDos attacks [16].
- The Storm botnet issue [20].
- The communications from C&C servers are being obfuscated by the botmasters to avoid detection [17].
- The leakage of information about botnets' behaviour that has never been studied extensively. It is mostly a mystery how prevalent botnet is in the internet. Capturing the botnets' behaviour and impact from different point of views [12].
- Identify the indistinct chat-like command and control communication (C&C) of bonnets. They are unrecognisable from human-to-human communications that uses a traditional method of signature based techniques [18].
- Attackers are able to access personal computers running the latest operating system and send malicious codes through software that is installed onto the system. Computers that do not have proper detection software are open to hackers' tools. Anyone with access to the Internet are easily located and automatically compromised [13].
- The issue of the matter is content filtering technology's high false rate. If only the filter on content is built without the pattern analysis on parameters, misjudge can happen [5].
- Bandwidth receives unfair vertical limitations. It is still achievable for Dos/DDoS flooding to occur using drones and zombies with such bandwidth restrictions. One of these threats are the ICMP flood based attacks [14].
- IP spoofing are one of the attacks involved. It has become a tedious task to detect infected PCs using pattern-based IDS and AV due to the large number of unknown bots generated with codes that are continuously updated [11].
- Bots bringing down email servers via large quantities of unwanted content. User's mailbox is filled with enormous volumes of spam [9].

- Computer viruses and phishing can be considered as threats to information security. It is difficult to monitor botnet activities [10].

3. Summarize Major Problems

Major problems are classified in 8 groups as follows:

- Spam and Email Botnets
- Botnet activities or Malicious behaviour and difficulties to detection
- Lunching malicious code by downloading software from internet
- ICMP flood based attacks
- Botnet DDOS attack
- Obscure Botnet C&C communications
- Storm botnet
- Large-scale & statistical problem & expensive computational on traffic flows

4. Solutions

Here we have classified solutions are used so far in current problem in field of IRC botnet detection:

4.1 International sharing of information

It is important that the analysis of structure and distribution is enabled among the ISPs. It is also crucial to understand botnets' behaviour based on whatever information that is gathered. The function of monitoring and controlling the network is available to every ISP but can be exploited. The network monitoring and controlling is done through Security Authority (SA) via collecting and analysing intrusions and attack information on ISPs. Bot zombies bypass the ISP using a DNS sinkhole that accepts command/control traffic. However, traffic data can be collected from these sinkholes and analysed to be shared internationally. These traffic data collected at the gateway interfacing LAN and backbone is then sent to the detection module [1].

4.2 Hierarchical collaborative models

It shares information and cooperates in the three levels of information, feature, and decision-making and then extracts the essential features of botnet from a variety of data [2].

4.3 network-based observation and filtering unlikely flows

Most computationally intensive detection of botnet coordination is done on a dramatically reduced traffic set. Filtering flows to reduce the botnet search space. Characterize IRC flows (which are also brief and interactive) to identify how we can separate the C2 channel from other Internet traffic. For data reduction, they convert the sequence of packets into flow summaries, and then identify a suspect infrastructure. Collect and analyse forensic archive of packet-level of data [3].

4.4 Email shape detection

Botnet detection mechanism can be based on the neither email “shape” neither analysis that relies on neither content nor reputation analysis. Email can be characterized by mimicking human visual inspection. A set of email shapes are derived and then they used to generate a botnet signature. Detect the presence of the spamming botnet that sent the email [4].

4.5 Analyze email client interaction

Email has the ability to provide a stealthy C&C channel. Messages can be cleverly crafted to include a botnet mechanism that can run without user interaction at their email clients and is invisible to detection mechanism. To evaluate the ability of botmasters, two C&C channels are designed to employ encoded commands in emails. Subsequent communications over email communication channels between bots and botmasters permits access without identification or blockage [6].

4.6 spam filter by analyzing the mail header

Extracting the structure of mail header, (just sender IP and sender email address), and classifying spams by comparing the locations of these elements could reduce traffic bandwidth and space used by spam [8].

4.7separating IRC and non-IRC traffic

The method of detection distinguishes traffic from standard IRC or botnet-based IRC. To group the activities of the same bot, a traffic flow correlation is used. First, a basic filtering method is used followed by aggregating flows into communication flows. Any related features are then extracted from these flows and the relationship can be established based on the information received. The normal traffic collected from the campus network is injected with the flow data from the testbed [4].

4.8Detecting behavior of downloads and the port-scans.

The detection process is automated in the proposed decision tree consisting of statistics. Clarify typical behaviour of botnet from the observation of CCC (cyber clean centre) DATA set. Identify the type of the port scans into fourth octet changed one by one [15].

4.9Turing test

A large percentage of legitimate traffic passes through an ISP's edge router. A method used by Google TM to identify and separate legitimate human user and bot programs is by directing users that plans to access an attacked website to a group of nodes. These nodes will then perform an authentication procedure where users are required to successfully complete a Turing test before gaining access to the website. Google TM can then help identify traffic that was referred to by valid search engines.

4.10 reroute or disrupt "real" C&C traffic

Disrupting the communication between the bots by inserting themselves in the peer lists of "regular" bots, and eventually. Another one is mounting the practical Sybil attacks on the Storm botnet. The number of Sybils necessary to achieve the desired level of disruption, with respect to the net growth rate of the botnet. Capturing key features of the Overnet P2P is overlay network [20].

4.11 Analysing properties of IP address aliasing and Node-ID

Identifying storm bots is achieved by collecting location information from all participants [19].

4.12 Bayesian approach

Assume at least one bot in a botnet is known, using a Bayesian approach, find other hosts with similar DNS traffic. DNS traffic of infected hosts can be collected [17].

4.13 capture botnet binaries

In order to track unique IRC botnet infections ranging from different sizes and several infected end host, a multifaceted and distributed infrastructure must be created. This will result in a comprehensive analysis of measurement regarding the structure and behavioural aspects of botnet which is important. Botnet binaries are captured using a distributed malware collection points. In order to gain an insider perspective of the live botnets behaviour, the unique IRC is tracked. How globally prevalent is the botnets can be assessed by analysing the DNS cache [12].

4.14 BotProbe

An algorithmic framework uses hypothesis testing to separate botnet C&C dialogs from human-human conversations with desired accuracy. Implement a prototype system called BotProbe. a hypothesis testing framework that enables network administrators to tune the level of expected interference with detection rates. to avoid disturbing known critical/legitimate programs/sessions can also be used to reduce potential interference [18].

4.15 BLOBOT

Blobot is a tool for detection botnets in real time at originator side, namely at the user side. Filter user outgoing connection. BLOBOT analyses the traffic generated by a single user. It tries to detect anomalies that reveal the presence of a botnet. It detects both IRC-based and HTTP-based C&C networks. It Reduces amount of very specific traffic and thus becoming able to effectively detect botnets in real-time [13].

4.16 Technology on gateway firewall layer

It distinguishes legitimate mail and spam. a classification filtrate mechanism based on user's behavior. For each e-mail characteristic, its IP address, content length, delivery time, sending frequency and content type are focused on [5].

4.17 Tracking from a victim PC to a bot and from the bot to a C&C server

Evaluate the tracking success ratio of the bot process on the infected PC. Collect bot access records and depict the botnet topology that suggests active C&C servers [11].

4.18 Traffic control mechanism detects

It delays the traffic of suspicious senders and bots. Grouping spammers based on their behavior and transmission patterns. Traffic shaping techniques are a pre-filtering analysis to avoid use of automated machines (Bots) to spam a particular domain. Real-time filtering techniques can be used without the risk of false positives [9].

4.19 Honeypot system

Capturing malware and tracking botnets. Developed honeypot system is used for capturing malware based on honeypot technology. Malware analysis system consists of MD5 hush database [10].

5. Summarize solution

In this section, we summarized and categorized all solution taken of our paper [22] as best solutions known for major problems that had been argued above in IRC botnet detection (Table 1).

Spam and Email Botnets problem are take attraction in so many ways. As we mentioned in our paper [22], there are few ways to mitigate spams, but we studied and found the grouping spammers based on behaviour and trans- mission pattern Real time filtering works in better way to help spam mitigation [6][7][8][9].

Botnet activities or malicious behaviour and difficulties to detection problem in have been described by related solutions, but Flow correlation for grouping same activity, identify normal IRC behaviour and Identify behavioral pattern have place in more satisfy level among detection techniques[22] [4] [5].

Lunching malicious code by downloading software from internet are mentioned in [22] introduced some solutions. But we have found Filtering the user outgoing packet could help in better way [13][14].

ICMP flood based attacks problems could be mitigated in best way if the Identify type of port scan is being used as a solution [22] [15].

Botnet DDOS attack problems have their own best solution known as Authentication to distinguish between human client and bot client [22] [16].

Obscure Botnet C&C communications problems used Hypothesis testing to separate botnet C&C dialog [22] [18].

Storm botnet problem are mitigated through Inserting bots in the peer list of regular bots & reroute real C&C traffic [22] [20].

Large-scale & statistical problem & expensive computational on traffic flows problems is used eextract clues from network-based evidence to detect presence of botnet [22] [3].

TABLE I. SUMMARY OF STUDY IN EIGHT CATEGORIES

Row	Problem	Solution(s)
01	Spam and EmailBotnets	Grouping spammers based on behavior and trans- mission pattern
02	Botnet activities or Malicious behaviour and difficulties to detection	Identify behavioral pattern [5]
03	Lunching malicious code by downloading software from internet	Filter user outgoing
04	ICMP flood based attacks	Identify type of port scan

05	Botnet DDOS attack	Authentication to distinguish between human client and bot client [16]
06	Obscure Botnet C&C communications	Hypothesis testing to separate botnet C&C dialog
07	Storm botnet	Inserting bots in the peer list of regular bots & reroute real C&C traffic [20]
08	Large-scale & statistical problem & expensive computational on traffic flows	Extract clues from network-based evidence to detect presence of botnet

6. Conclusions

Over 20 papers within this classification of bots and botnets being reviewed, there are 8 major problems highlighted in this paper along with solutions in each section. The most common issues here are botnets and malware behaviour, as shown in the table. There are several solutions being developed by researchers to deal with this problem, which this paper has mentioned and classified based on available resources and researches. In short, we look at the methods of capturing and tracking channels after which the flow is analysed and filtered to identify the patterns meant further assessment. However, the bots and botnet numbers will continue to grow. Therefore, it is necessary to classify them and utilise sophisticated techniques to mitigate and face them head on.

7. References

[1] eungGoo Ji, ChaeTae Im, MiJoo Kim, HyunCheol Jeong, Botnet Detection and Response Architecture for offering secure internet services, Korea Information Security Agency, Seoul, Korea, 2008

[2] Hailong Wang, Chang Sha, Hu Nan, Zhenghu Gong, Collaboration-based Botnet Detection Architecture, School of Computer National University of Defense Technology, China, 2009

[3] Robert Walsh, David Lapsley, and W. Timothy Strayer, Effective Flow Filtering for Botnet Search Space Reduction, BBN Technologies, 10 Moulton Street, Cambridge, USA, 2009 IEEE

[4] Hsiao-Chung Lin Chia-Mei Chen Jui-Yu Tzeng, Flow Based Botnet Detection, Fourth International Conference on Innovative Computing, Information and Control

[5] WANG Chun-dong, LI Ting, WANG Huai-bin, Botnet Detection Based on Analysis of Mail Flow, Key Laboratory of Computer Vision and System, Ministry of Education, Tianjin, China, 2009 IEEE

[6] Paul Sroufe, Santi Phithakkitnukoon, Ram Dantu, and João Cangussu , Email Shape Analysis for Spam Botnet Detection, Department of Computer Science & Engineering, University of North Texas, Denton, USA, 2009 IEEE

[7] Kapil Singh Abhinav Srivastava Jonathon Giffin Wenke Lee, Evaluating Email's Feasibility for Botnet Command and Control, International Conference on Dependable Systems &Networks: Anchorage, Alaska, June 24-27 2008.

[8] Kobkiat Saraubon Benchaphon Limthanmaphon, Fast Effective Botnet Spam Detection, Fourth International Conference on Computer Sciences and Convergence Information Technology, 2009.

[9] Husain Husna, Santi Phithakkitnukoon,and Ram Dantu, Traffic Shaping of Spam Botnets, University of North Texas, Denton, USA, 2010.

[10] Katsumi Ono, Isamu Kawaishi, Toshihiko Kamon, Trend of Botnet Activities, High-tech Crime Technology Division National Police Agency of Japan, 2007 IEEE

[11] Keisuke TAKEMORI, Masahiko FUJINAGA, Toshiya SAYAMA, Masakatsu NISHIGAKI, Host-based traceback; Tracking bot and C&C server , KDDI R&D Laboratories Inc, Japan, 2009 ACM.

[12] Moheeb Abu Rajab Jay Zarfoss Fabian Monrose Andreas Terzis, A Multifaceted Approach to Understanding the Botnet Phenomenon, Johns Hopkins University, Baltimore, Maryland, USA, 2006 ACM.

[13] Gianluca Dini and Isidoro S. La Porta, BLOBOT: BLOcking BOTs at the Doorstep, Fourth International Multi-Conference on Computing in the Global Information Technology, 2009, Italy

[14] J.Udhayan', R.Anitha, Demystifying and Rate Limiting ICMP hosted DoS/DDoS Flooding Attacks with Attack Productivity Analysis, 2009 IEEE International Advance Computing Conference , Patiala, India, 6-7 March 2009

[15] Kazuya Kuwabara, Hiroaki Kikuchi, Masato Terada, Masashi Fujiwara, Heuristics for Detecting Botnet Coordinated Attacks, International Conference on Availability, Reliability and Security.

[16] Basheer Al-Duwairi, G. Manimaran, JUST-Google: A Search Engine-based Defense Against Botnet-based DDoS Attacks, Department of Electrical and Computer Engineering Iowa State University, USA, IEEE ICC 2009 proceedings.

[17] Ricardo Villamarín-Salomón, José Carlos Brustoloni, Bayesian Bot Detection Based on DNS Traffic Similarity, University of Pittsburgh, Pittsburgh, USA, 2009 ACM.

[18] Guofei Gu, Vinod Yegneswaran, Phillip Porras, Jennifer Stoll, Wenke Lee, Active Botnet Probing to Identify Obscure Command and Control Channels, Annual Computer Security Applications Conference

[19] Binbin Wang, Zhitang Li, Hao Tu, Zhengbing Hu, Jun Hu, Actively Measuring Bots in Peer-to-Peer Networks, 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing

[20] Carlton R. Davis, Jos´e M. Fernandez, Stephen Neville, John McHugh, Sybil attacks as a mitigation strategy against the Storm botnet, ´ Ecole Polytechnique de Montr´eal, University of Victoria, Dalhousie University, 2008 IEEE.

[21] Tony Bradley, “Essential Computer Security”, Syngress 2006.

[22] Seyedeh Ghazal Ghalebandi, Arash Habibi Lashkari , Rohini Devi, Shahab Alizadeh, “A wide survey on IRC Botnet Detection”, 4th International Conference on Computer and Electrical Engineering (ICCEE 2011), published by ASME, Singapore, 2011