Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

An Enhanced Approach for Botnet Path Monitoring

Sudhar Shankar .B*
School of Information Technology and Engineering
Vellore Institute of Technology
Vellore, India
shans512@gmail.com

Prof. Usha Devi .G
School of Information Technology and Engineering
Vellore Institute of Technology
Vellore, India
ushadevi.g@vit.ac.in

Abstract: Botnet is a network of compromised computers called bots that works under the dominance of botmaster (attacker). Botnet has become the major source of internet threats. Before stepping into the control process of its effects, it is important to have an advanced perception of its existing structure which helps the defender to protect the network by identifying the root cause of the malfunctions effectively.

Keywords: Botnet, Network, security, Peer-to-Peer, Monitoring.

I. INTRODUCTION

A Botnet is a network that consists of compromised computers (bots) and it is controlled by a botmaster (attacker). The compromised computers are responsible for most of the internet attacks like extortion to the network data through denial of service attack [5] and click fraud attacks [3]. It is not a sufficient approach to analyze on how to identify and defend against botnet for the future attacks through the current practices.

Therefore, it is important to have an advanced perception of its existing structure. This helps the defender to protect the network by identifying the root cause of the malfunctions effectively and in a better secured fashion. Botnet has also focused on recently encrypted channel like secure socket layer (SSL). The major protocols that are used by botmasters include Internet Relay Chat (IRC) protocol, Hypertext Transfer Protocol (HTTP) and Peer-to-Peer network protocols. Some of the examples of Bots are Sinit [1], Phatbot [2] and Slapper [7]. The Sinit uses public key cryptography which is used for authenticating updates and performs attacks. Phatbot uses cache servers for its bootstrap process and affects the network. Slapper uses a communication process by random probing and making more network traffic. All such processes has their own weakness to get caught by the defenders which leads to the factor of designing the advanced botnet structure which is helpful to guess the future attacks and control them.

The aim of this paper is to monitor the path of the botnet designed with advanced perspective structure and obtain the root cause of the attacks and prevents them with effective control measure.

This paper is organized as follows: Section II describes the related studies. Section III introduces the existing architecture and their effects. Section IV introduces an enhanced approach for botnet path monitoring and securing the network which involves the requirements for a new design of botnet and their advantages over the existing structure with the defense mechanism to be used in the proposal. Section V shows the result and discussions. Section VI concludes this paper along with the future scope of the project.

II. RELATED STUDY

The authors [6] represented a comprehensive study on monitoring the botnet activities in the internet by using honeypots to get into botnets. They have used Dynamic DNS service providers with a goal to remotely control the automated activities of the Denial of Service.

The authors of [4] represent a botnet monitoring system which is achieved by redirecting the DNS mapping of a C&C server to a botnet monitor. Here, a study of zombies i.e., victim machines (bots) that are controlled by an attacker are viewed with respect to time zones to understand how time and location affects malware spread dynamics.

The authors of [8] presented on how to use honeynet for botnet monitoring. Researches configure the network on how to capture a variety of useful data on attacks made on computer without compromising the other computers. A study is made on how the attackers used to initiate Distributed Denial of Service against Internet sites. The honeynet technology is relatively new, which is expected to be developed in the forth coming trends.

III. EXISTING ARCHITECTURE AND ITS EFFECTS

The major purpose of the botmaster is to monitor the network and perform attacks at weaker systems by shutting it down or hijacking. This is done with the existing command and control architecture shown in figure-1.

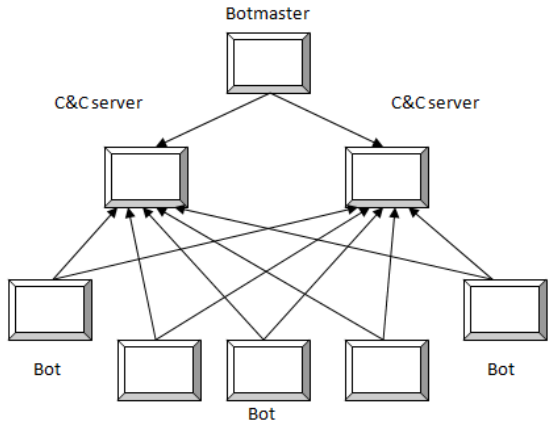


Fig. 1. Command & Control architecture of C&C botnet

The botmaster controls the botnet via the command and control architecture. There may be any number of bots in the network which is managed by an attacker. This is achieved through the C&C servers. The C&C servers issue the commands from the botmaster to the bots that are connected with it. According the botmaster, the C&C servers are the major foundation of the botnet operation. If a C&C server is caught by the defenders, the botmaster looses his control over the botnet and hence it is easy to obtain the root cause of the attacks by the defenders. The weak points of this structure are that C&C servers control more bots under them which leads to more traffic on the network. When a defender monitors the entire network then such traffic areas can be easily spotted.

The effects of botnet are the major problem in the current generation compared to other internet threats. In case of a large distributed network environment across the world it covers a wide network of bots on it and performs attacks that leads to a massive destruction and threat of confidential information.

Hence, it is most important to produce a control measure in an advanced fashion with more credits than the existing defense practices.

A. *Need for Constructing New Design Structure*

When the attacker attempts to remove the bootstrap procedure, a random probing is used to find bots of similar kind. At this time a large number of network traffic is created hence it is easier for defender to find the attacker my monitoring the origin of traffic. When attacker uses cache servers, it is possible for the defender to find the catch server and shutdown the system. In some botnet, attacker fails to use the encryption and command authentication hence leading to be easily hijacked.

Such facts are concerned to be major drawbacks of the existing botnet. Thereby, it is useful to create a robust botnet from the attacker's future design perspective and create control measures to secure the network.

B. *Monitoring of Botnet by the Botmaster*

The aim of the botmaster is to make the botnet hard to be monitored by the defenders. At the same instant it should be easier by the botmaster to monitor the entire botnet. The effectiveness of such a goal lies for the botmaster in conducting the attacks easily based on the size of the bots in the network and also maintaining the bots basic information on its identities such as IP addresses and on/off status etc. Another important factor is to protect the botnet from various counter actions by the defenders in the network.

Precisely the botmaster prevents the network bots from being shutdown, monitor or take control over the network by the defenders.

The botmaster focuses on vulnerability exploitation on the network and spreads viruses in emails, network share and other file based traditional viruses over the network.

IV. AN ENHANCED APPROACH FOR BOTNET PATH MONITORING AND SECURING THE NETWORK

A. *Requirements for the New Botnet Design*

The botmaster should be able to monitor the entire botnet and keep track of each bots in the network and maintains an account of the new bots that are added to the network and the bots that are removed from the network.

Constructing the botnet with peer-to-peer architecture ensures the following:

- Limited exposure of bots from each bot in the network, since each peer has its own index list of certain bots based on which it browses for its requirements.
- The peer-to-peer network has an advantage of serving as both as a server and a client, hence more efficient for the botmaster to acquire a network.

The botmaster should be able to protect the botnet even after some portion of the botnet is captured and shutdown by the defenders. Each bot in the botnet should be able to communicate with other bots with their own defined service port without any restriction.

B. *Proposed Architecture and its Advantages*

The proposed architecture is constructed based on peer-to-peer communication system illustrated in figure-2.

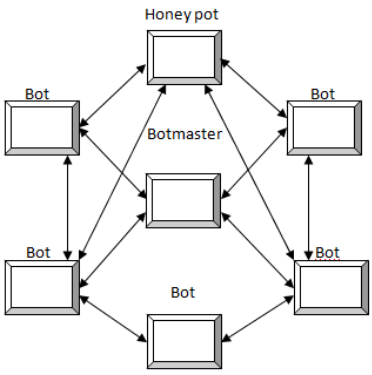


Fig. 2 . Proposed peer-to-peer Botnet with defense mechanism (Honey pot)

The bots in the network are constructed in such a way that each bot in the peer-to-peer botnet contains a peer list which has the information of certain other bots to which they

are communicating with. To check whether the connection is made between bots, the initial set of bots should contain some servant bots where its IP addresses are contained in the peer list of every other initial bots in the network.

When a new infection is spread from one bot to another and if the spreader is a servant bot, then the receiver bot adds its identity on its peer list. And if spreader comes to know that the receiver is also a servant bot, then the spreader includes the receiver's identity on its peer list. If a re-infection is made from the same spreader to the receiver, the receiver updates the spreader's identity on its peer list by replacing it on the list where there is an old communication identity if the peer list is full.

As the re-infection is continued, then it results in different interconnection of infections paths makes hard for the defenders to detect the infection time order among the bots in the acquired peer list. The updating of botlist by its botmaster is done by generating commands using different service ports by the servant bots which makes the monitoring of botnet difficult by the botmaster.

C. *Defense Approach using Honeypot Technique*

Botnets can be monitored and controlled by applying an effective and sufficient technique such as Honeypot technique. A significant factor to be concerned during botnet path monitoring is masking the visibility of the defenders counter action against the botmaster's activities. It would be difficult to provide such functionality by using common security enhancements.

A Honeypot is trap set for the detection of attempts made to interact with information systems by an illegal user or system. It is an early warning tool and closely observes the network to identify an illegal transaction. It joins any network by masking its original identity and shows the network as an open proxy.

An attacker may not be aware of its uniqueness and approaches the Honeypot system to perform attacks and will get trapped by the defenders and helps to provide an appropriate counter action against it.

D. *Defense Against the Proposed Botnet and Counter Measures by the Defenders*

Defender uses Honeypot technique to enter into the network. The Honeypot system monitors the entire network without the knowledge of the other nodes in the network. Whenever a new node enters the network the defender obtains the details of the node which includes the name of the node, IP address and the port number.

The honeypots are associated with a database that stores the details of the new nodes added. When the attacker makes a connection with the bots, the status of the transaction is monitored by the honeypot. The defender system acts as a traffic monitoring sensor host through which the network traffic is monitored.

According to the proposed botnet the major weak point is the process of updating of bots information by its botmaster. The servant bots are the responsible nodes for the command distribution from the botmaster to the other bots in the network. If a servant host makes a vast amount of traffic towards the bots it is easier for defenders to acquire the transaction and reduce a portion of the botnet population.

The major advantage in the above process is the removal of substantial portion of the botnet makes the workload of the other servant bots higher. Hence, it is made simple to find the largest traffic patterns.

There are possibilities to show honeypot system as a servant bot so that it may obtain a huge number of peer's communication towards it and obtains a fresh list of bots. This lets the opportunity to increase the honeypot systems to increase in the network by introducing more honeypot systems as servant bots. This makes the defenders task simple and manages the network safely.

The counter actions by the defenders include botnet monitoring, shutdown, hijack and detaching and recuing the network nodes and separate them from botmaster's control. Monitoring of the network is made easier through honeypot technique. The honeypot acts as an effective detection mechanism and helps the defenders to approach the identified bots with appropriate counter actions. The detection of the botmaster is made simple by reducing the overall botnet population and protects the network.

V. RESULTS AND DISCUSSIONS

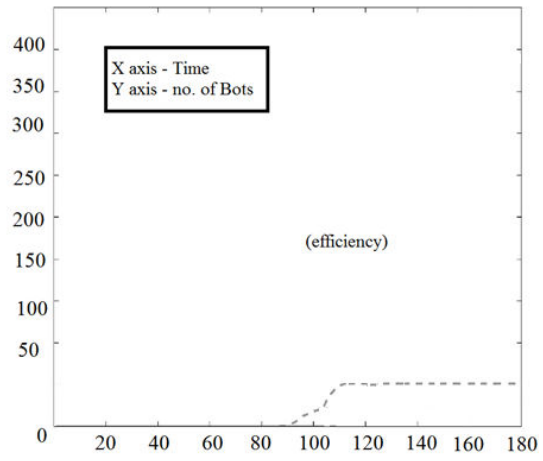
A. *Emerging Personification of the Enhanced Approach*

As a result of the new approach the botnet is made stronger than the existing methodology. The new concept implies the inclusion of the removed bot once again to enter the network while an attempt if made by the attacker. In the existent there is less probability of the reentry of the removed node into the network. Whereas in the proposed system the new peer that enters the network invokes a novel IP address. This makes the botnet harder than the client server approach.

In case of indirect attacks (attacker node makes use of an intermediate node to conduct attack over its target node) the honey pot can be utilized with a functionality of determining the root cause of the attack and to trigger appropriate counter actions.

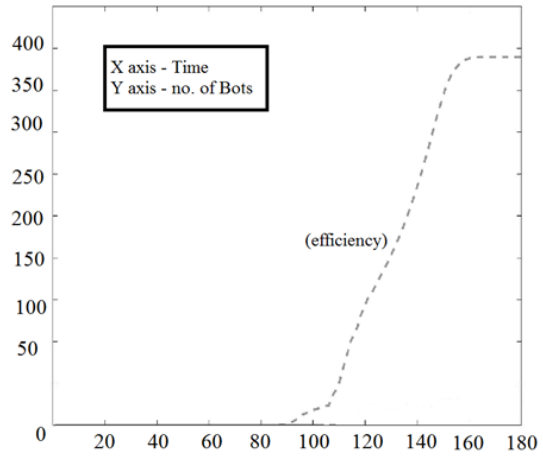
B. *Result Analysis*

The effectuation of the new approach serves following stages on the defender's perspective (using honeypot technique):



(A)

Figure (A) Honeypot performance in existing system.



(B)

Figure (B) Honeypot performance in proposed system.

Peer inclusion to the network: The new peer entry into the network follows a verification process where the user's specifications are examined comparing with the existing records. These components ensure that no duplicate entry of nodes is allowed.

Identifying bots: A bot can be tracked by both the defender as well as by another bot. This is performed when a bot is pursuing its attacks over another in the network. The defender is prompted with the type of attack to be conducted.

Detecting botmaster: Honey pot is used as a defense mechanism and helps detecting the botmaster. Honey pot system is intimated with the details of the botmaster when it tries to establish its control over the bots in the network either directly or via other bots.

Protecting network: Honey pot as a defense mechanism is facilitated with making counter actions while detecting the attacks by the botmaster. It first analyses with the type of attack going to be conducted. The options with this mechanism are enrolled with removing the botmaster from the entire network or to defend the attacks and rescue the affected node.

VI. CONCLUSION

The control measures against botnet attacks become more effective and efficient only when it prevents massive attacks and threats that are generated from complex botnet architecture. Thereby, it is important to construct a complex botnet design with a perception of advancement over the existing botnet architecture. Peer-to-Peer networks are sufficient for the botmasters to maintain control over the botnet while compared to common client server architecture. The major advantage is that a botmaster can still maintain a control over the botnet even after a substantial portion of the botnet population is affected by the defenders.

A. *Future scope:*

Honeypot is a technique used to counteract the new botnet's attacks. This is an effective technique which is applicable to oppose the activities of botnet regardless of its negative effects. Therefore, it is of the great significance to conduct researches on honeypot and its operations from being exposed by the attackers.

VII. REFERENCES

[1] Sinit P2P Trojan Analysis, http://www.lurhq.com/sinit.html, 2008.
[2] Phatbot Trojan Analysis, http://www.lurhq.com/phatbot.html, 2008.
[3] C.T. News, Expert: Botnets No. 1 Emerging Internet Threat, http://www.cnn.com/2006/TECH/internet/01/31/furst/, 2006.
[4] D. Dagon, C. Zou, and W. Lee, "Modeling Botnet Propagation Using Time Zones," Proc. 13th Ann. Network and Distributed System Security Symp. (NDSS '06), pp. 235-249, Feb. 2006.
[5] S. Kandula, D. Katabi, M. Jacob, and A. Berger, "Botz-4-Sale: Surviving Organized DDOS Attacks That Mimic Flash Crowds," Proc. Second Symp. Networked Systems Design and Implementation (NSDI '05), May 2005.
[6] F. Freiling, T. Holz, and G. Wicherski, "Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks," Technical Report AIB-2005-07, CS Dept. RWTH Aachen Univ., Apr. 2005.
[7] I. Arce and E. Levy, "An Analysis of the Slapper Worm," IEEE Security & Privacy Magazine, vol. 1, no. 1, pp. 82-87, Jan.-Feb. 2003.
[8] B. McCarty, "Botnets: Big and Bigger," IEEE Security & Privacy Magazine, vol. 1, no. 4, pp. 87-90, July-Aug. 2003.