International Journal of Computer and Communication Technology

Volume 8 | Issue 1 Article 9

January 2017

A New Generation Peer-to-Peer Advanced Botnet

Roshan Mathew
Dept. of CSE, Viswajyothi College of Engineering and Technology, India, roshmathan@gmail.com

Follow this and additional works at: https://www.interscience.in/ijcct

Recommended Citation
Mathew, Roshan (2017) "A New Generation Peer-to-Peer Advanced Botnet," *International Journal of Computer and Communication Technology*: Vol. 8 : Iss. 1 , Article 9.
DOI: 10.47893/IJCCT.2017.1398
Available at: https://www.interscience.in/ijcct/vol8/iss1/9

This Article is brought to you for free and open access by the Interscience Journals at Interscience Research Network. It has been accepted for inclusion in International Journal of Computer and Communication Technology by an authorized editor of Interscience Research Network. For more information, please contact sritampatnaik@gmail.com.

A New Generation Peer-to-Peer Advanced Botnet

Roshan Mathew

Dept. of CSE, Viswajyothi College of Engineering and Technology, India
E-mail: roshmathan@gmail.com

Abstract **-** A botnet is a network of compromised computers that are infected with code that allows an unauthorized user to control them via the Internet. Botnets are one of the most serious threats to today’s Internet. Most current botnets have centralized command and control (C&C) architecture. However, peer-to-peer (P2P) structured botnets have gradually emerged as a new advanced form of botnets. Without central C&C servers, P2P botnets are more resilient to defenses and countermeasures .Compared with current botnets, the proposed botnet is harder to be shut down, monitored, and hijacked. It provides robust network connectivity, limited botnet exposure by each bot, and easy monitoring and recovery by its botmaster and more trustfull.

Keywords *- Botmaster, Peer-to-peer, Symmetric key.*

I. INTRODUCTION

Botnet is recognized as one of the most serious security threats of today. A botnet consists of a network of compromised computers connected to the internet that is controlled by a remote attacker or botmaster. Botnets have become a significant threat to network communications and applications, as they increases the efficiency of network attacks such as denial-of –service (DoS) attacks, scanning, phishing, Email spam, identity theft, click fraud, and espionage . This capability of a botnet is attributed to the large number of hosts that it controls, which ranges from hundreds to thousands that work together in carrying out an attack, as opposed to when only a few number of hosts carry out attack.

Today, centralized botnets are still widely used[4, 5]. In a centralized botnet, bots are connected to several servers (called C&C servers) to obtain commands. This architecture is easy to construct and efficient in distributing botmaster’s commands; however, it has a weak link - the C&C servers. Shutting down those servers would cause all the bots lose contact with their botmaster. An entire botnet may be exposed once a C&C server in the botnet is hijacked or captured by defenders. In addition, defenders can easily monitor the botnet by creating a decoy to join a specified C&C channel. Also defenders could easily obtain the identities (e.g., IP addresses) of all C&C servers based on their service traffic to a large number of bots, or simply from one single captured bot (which contains the list of C&C servers).

In a P2P botnet, there is no central server, and bots are connected to each other and act as both C&C server and client. P2P botnets have shown advantages over traditional centralized botnets. The proposed improved peer-to-peer botnets are more resilient to defenses and countermeasures. Compared with current botnets, the proposed botnet is harder to be shut down, monitored, and hijacked. It provides robust network connectivity, limited botnet exposure by each bot, and easy monitoring and recovery by its botmaster. As the next generation of botnets, they are more robust and difficult for security community to defend.

II. RELATED WORKS

The evolving and evasive nature of botnets requires researchers to anticipate possible topologies. Grizzard et al. [1] provided a history and overview of P2P botnets. Holz et al. [2] presented a case study on Storm including its system-level and network-level behaviors. Kanich et al. [3] tried to present a more accurate estimation for the size of Storm botnet by taking various types of noise (e.g. protocol aliasing, adversarial aliasing, and temporal dynamics) into consideration.

Wang et al. [4] summarized the disadvantages of centralized and P2P botnets and proposed a hybrid structured botnet that overcame those disadvantages. The C&C communication model proposed by them had an undirected graph topology for command forwarding as shown in Fig.1. In this model, a botmaster injects her commands to any bot(s) in the botnet. Both client and servent bots periodically connect to the servent bots in their peer lists in order to retrieve commands issued by their botmaster. When a bot receives a new command that it has never seen before (e.g., each command has a unique ID), it immediately forwards the command to all servent bots in its peer list. In addition, if itself is a servent bot, it will also forward the command to any bots connecting to it. The drawback with this approach is that , as the command is injected directly to either the client bot or to the servent bot by the botmaster, there is a weak control in the command flow. Also, it is difficult for the botmaster to keep track the attack status in the botnet. Our proposed model for command communication will overcome this drawback with a directed command forwarding in breadth first fashion in the C&C architecture of P2P botnet.

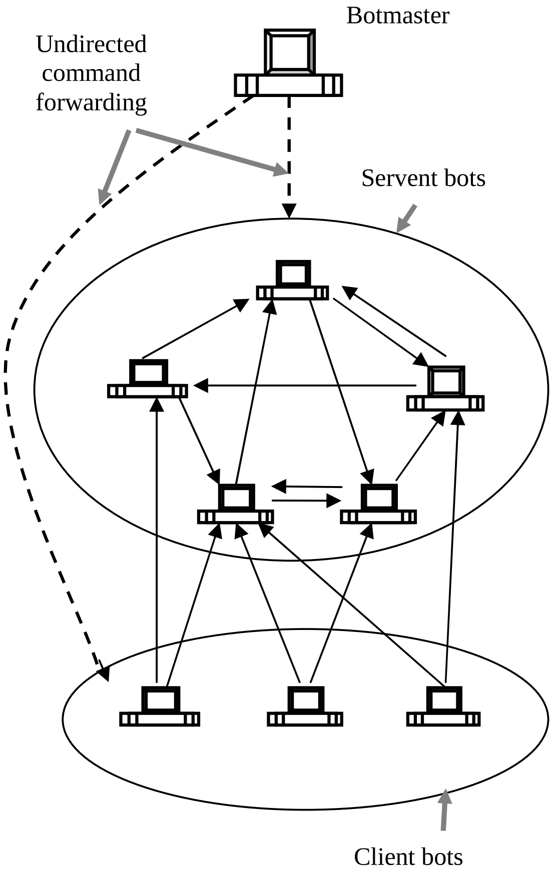

Fig. 1 : Undirected command forwarding in hybrid peer-to-peer botnet.

III. NEW GENERATION PEER-TO-PEER BOTNET

A. Implementing hybrid Botnet p2p structure

The bots in the proposed P2P botnet are also classified into two groups as in the hybrid peer-to-peer botnet [4]. The first group contains bots that have static, nonprivate IP addresses and are accessible from the global Internet. Bots in the first group are called servant bots since they behave as both clients and servers.2 The second group contains the remaining bots, including 1) bots with dynamically allocated IP addresses, 2) bots with private IP addresses, and 3) bots behind firewalls such that they cannot be connected from the global Internet. The second group of bots is called client bots since they will not accept incoming connections. Only servent bots are candidates in peer lists. All bots, including both client bots and servent bots, actively contact the servent bots in their peer lists to retrieve commands.

B. Development of Botnet command and control

In our proposed model, the botmaster directly sends the command to the servent bots only. And this is send in breadth first order as shown in Fig. 2. So the command will reach the servent bots in the order A,B,C,D,E. The servent bots will then forward the commands to the client bots which are connected to it. This benefits the botmaster in controlling the command flow. For example, if only a certain number of servent bots need to be participate in an attack, botmaster can launch the attack in that way. Another advantage of our proposed model is that, with the botmaster not sending command to the client bots but only to the servernt bots, it decreases the chances of the botmaster being detected by honeypot client bots thus improving the stealthiness of the botnet in continuing the attacks. Also, servent bots normally do not change their IP addresses, this design increases the network stability of a botnet Thus it is more trustfull and robust.The proposed botnet is harder to be shut down, monitored, and hijacked.

The botmaster generates a pair of public/private keys, $h(K^+,K^-)$, and hard codes the public key K^+ into the bot program before releasing and building the botnet. There is no need for key distribution because the public key is hard-coded in bot program. Later, the command messages sent from the botmaster could be digitally signed by the private key K^- to ensure their authentication and integrity.

In the existing botnet, each servent bot i randomly generates its symmetric encryption key K^i . Suppose the peer list on bot A is denoted by LA. It will not only contain the IP addresses of M servent bots, but also the symmetric keys used by these servent bots. Thus, the peer list on bot A is LA={(IP_{i1} ,K_{i1}); (IP $_{i2}$;K_{i2});. ….. ; (IP_{im} ;K_{im})} where (IP_{ij} , K $_{ij}$) are the IP address and symmetric key used by servent bot ij. With such a peer list design, each servent bot uses its own symmetric key for incoming connections from any other bot. This is applicable because if bot B connects to a servent bot A, bot B must have (IPA;KA) in its peer list. This individualized encryption guarantees that if defenders capture one bot, they only obtain keys used by M servent bots in the captured bot’s peer list. Thus, the encryption among the remaining botnet will not be compromised.

C. Botnet monitoring by its Botmaster

The peer-list-based architecture enabled the botnet to disperse its communication traffic in terms of service port. Since a servent bot needs to accept connections from other bots, it must run a server process listening on a service port. The service port number on servent bot i, denoted by Pi, and could be picked by the bot, either randomly or selectively.

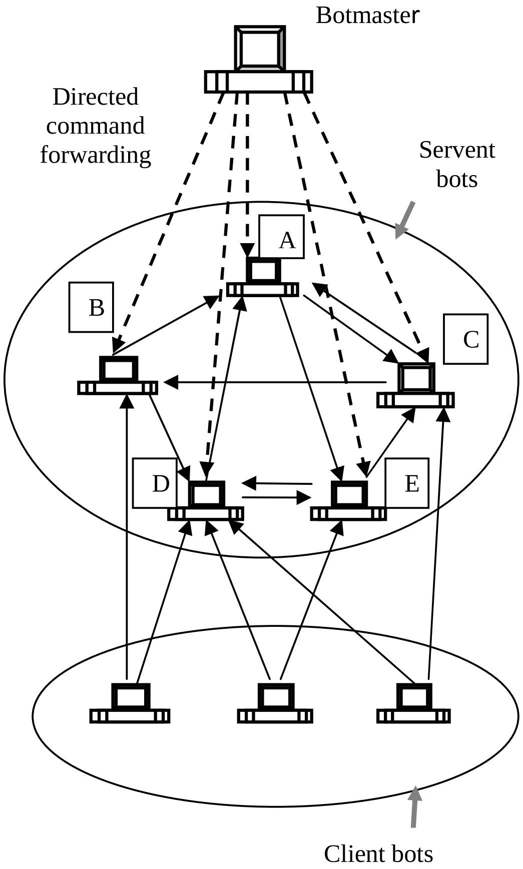

Fig..2 : Directed command forwarding in hybrid peer-to-peer botnet

Considering this, a peer list needs to contain the service port information as well. For example, the peer list on bot A is

$$LA= \{(IP_{i1},K_{i1} ,Pi1) ; . . . \{(IP_{iM},K_{iM} ,P_{iM}) ;\}$$

With the new peer list LA shown above, bot a can connect to any servants bot in its peer list using the correct service port without any difficulty.

D. Setting priority for the commands send by botmaster.

A priority is set to the command messages send by the botmaster which enables botmaster to give preferences to attack commands. So, the priority number is also included into the peer list. For example, the peer list on bot A is

$$LA= \{(IP_{i1},K_{i1} ,Pi1, PR_{i1}) ; . . . \{(IP_{iM},K_{iM} ,P_{iM,}PR_{iM}) ;\}$$

With the new peer list LA as shown above, if PR=1, the bot will perform the command once. If PR=2, the bot will perform the same command twice. If PR=3. The bot will perform the same command thrice and so on. In this way, the botmaster will control and monitor preferences to commands.

IV. CONCLUSIONS

Botnet is a network of compromised hosts or bots, under the control of a human attacker known as the botmaster. Botnets are used to perform malicious actions, such as launching DDoS attacks, sending spam or phishing emails and so on. Thus, botnets have emerged as a threat to internet community. Peer to Peer (P2P) is a relatively new architecture of botnets.

Botnets present significant new challenges for researchers. In this paper, we presented the design of a new generation peer-to-peer botnet in which the command communication model of the p2p architecture is improved by a directed command forwarding. In this, the botmaster will send command to the servent bots only and that too in breadth first order . Compared with current botnets, the proposed botnet is harder to be shut down, monitored, and hijacked. It provides robust network connectivity, limited botnet exposure by each bot, and easy monitoring and recovery by its botmaster and more trustful.

REFERENCES

[1] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. Kang, and D. Dagon. Peer-to-Peer Botnets: Overview and case study. In First Workshop on Hot Topics in Understanding Botnets (HotBots'07), Cambridge, MA, April 2007.

[2] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling. Measurements and Mitigation of Peer-to-Peer-based Botnets: A case study on storm worm. In First UsenixWorkshopon Large-scale Exploits and Emergent Threats (LEET'08), San Francisco, CA, April 2008. C.

[3] Kanich, K. Lechenko, B. Enright, G. M. Voelker, and S. Savage. The Heisenbot Uncertainty Problem: Challenges in separating bots from chaff. In First Usenix Workshop on Large-scale

Exploits and Emergent Threats (LEET’08), San Francisco, CA, April 2008.

[4] Ping Wang, Sherri Sparks, and Cliff C. Zou, “An Advanced Hybrid Peer-to-Peer Botnet “,IEEE Transactions on Dependable and Secure computing, Vol.7, No.2 , Aprill-June 2010.

[5] Tao Wang and Shun-Zheng Yu, “Centralized Botnet Detection by Traffic Aggregation “, IEEE International Symposium on Parallel and Distributed Processing with Applications, 2009.

❑❑❑