A Survey on Botnet: Classification, Attacks and Detection

Shaishav D.Shukla, Mr. Keyur Shah
Computer Engineering, Silver Oak College of Engineering and Technology
Ahmedabad, Gujarat, India

***Abstract*- Botnet becomes root cause of cyber attacks. Botnets are well recognized and persistent threat to all internet user. Recently the owner of some botnet, such as strom worm, zeus, torping and conflicker are employing fluxing techniques to evade detection. Botnet can be used for sniffing packets, starting DDOS attack, spamming, phishing and stealing data. Extensive used botnet is peer to peer botnet it is also advance form of botnet. There has been not extensive work and focus on defence technology. This paper presents the some technique that is used by botnet. Also classify the botnet types, its attacks and some well known detection techniques.**

***Index Terms* –Botnet, Evade, Peer to Peer Botnet, HTTP Botnet, Spamming, Phishing**

I. INTRODUCTION

In recent years, cyber attacks have evolved, becoming more profit-centered and better organized. Emails spams, click frauds, and social phishing are becoming more and more popular. Botnet, which consists of a network of compromised computers connecting to the Internet and controlled by a remote attacker, are for all of these problems. A botmaster can drive numerous compromised computers to attack the target at the same time. Therefore, as an attack platform, a botnet can cause serious damage and is very hard to defend against. Compare to other attack vectors, the essential component of a botnet is its control and command channel. A C&C is used to update the bot program, distribute commands from the botmasters, and collect victims' private information, such as bank accounts and identifying information. Once a C&C is broken down, the botnet degrades to discrete, unorganized infections, which are easy to be eliminated using host-based cleanup technology.

1.1 MOTIVATION

Among all media of communications, Internet is most vulnerable to attacks owing to its public nature and virtually without centralized control. With the growing financial dealings and dependence of businesses on Internet, these attacks have even more increased. Whereas previously hackers would satisfy themselves by breaking into someone's system, in today's world hackers' work under an organized crime plan to obtain illicit financial gains. Various attacks than include spamming, phishing, click fraud, distributed denial of services, hosting illegal material, key logging, etc. are being carried out by hackers using botnets.
Botnet attacker always one step ahead in attack formation than antivirus vendors and defender or security researcher. It requires a concentration for prevention and mitigation.

1.2 BOTNET LIFECYCLE[1]

(A)Infection: initial installation of botnet malware on target host. this is done by tricking users into running executables to attached to email. By exploiting their browser weakness or exploiting the presence of security holes.

(B)Bootstrapping and Maintenance: each node has to perform a set of actions to detect the presence of other nodes and connect to them, bot controller must be able to counteract when its associated nodes leave the botnets. Such maintenance operation have a fundamental role in ensuring robustness.

(C)Command & Control: botmaster and controller have the necessity of reliably distributing their command (e.g. by sending the command start ddos target=192.133.0.10 or send spam mail templates bot software updates) to their controlled nodes. that in turn to send associated results, or current status into back to bot master.

(D)Command Execution: running the received command on each individual bot.

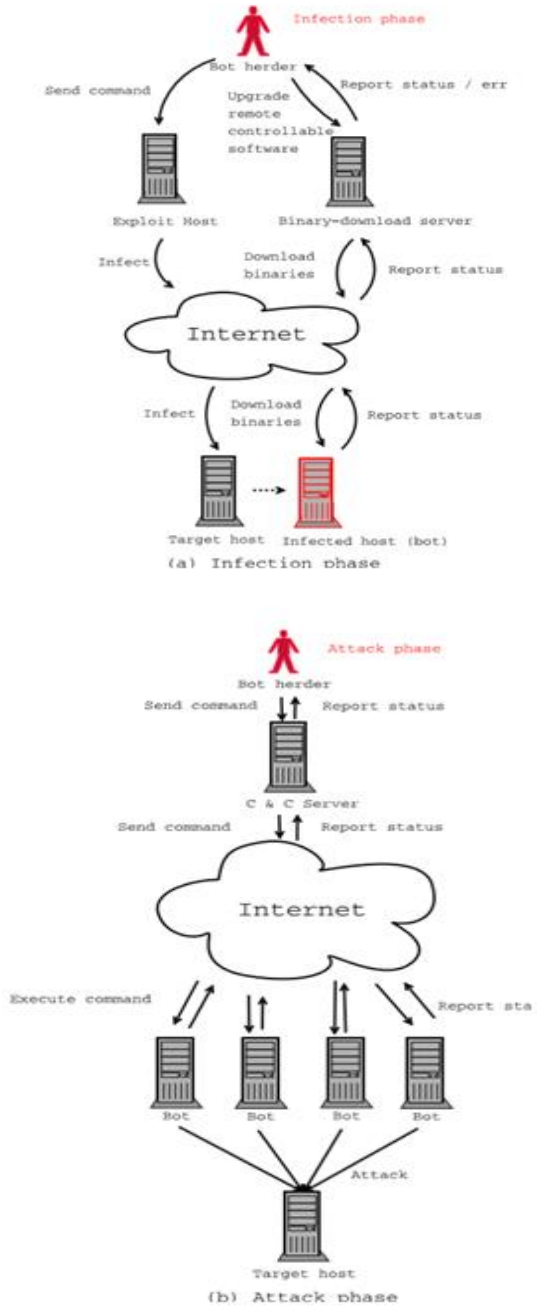

Figure 1: Botnet working scenario the infection and attack phase [2]

1.3 COMMAND & CONTROL ARCHITECTURE[3]

A core problem for botnet attackers is how to communicate with each bot instance. Most attackers would like the ability to rapidly send instructions to bots but also do not want that communication to be detected or the source of the those commands to be revealed.

A) Centralized: A centralized topology is characterized by a central point that forwards messages between clients. Messages sent in a centralized system tend to have low latency as they only need to transit a few well-known hops. From the perspective of an attacker, centralized systems have two major weaknesses: they can be easier to detect since many clients connect the same point, and the discovery of the central location can compromise the whole system.

B) P2P: Peer-to-peer (P2P) botnet communication has several important advantages over centralized networks. First, a P2P communication system is much harder to disrupt. This means that the compromise of a single bot does not necessarily mean the loss of the entire botnet. However, the design of P2P systems is more complex and there are typically no guarantees on message delivery or latency.

C) Unstructured: A botnet communication system could also take the P2P concept to the extreme and be based on the principle that no single bot would know about any more than one other bot. In such, a topology a bot or controller that wanted to send a message would encrypt it and then randomly scan the Internet and pass along the message when it detected another bot. The design of such a system would be relatively simple and the detection of a single bot would never compromise the full botnet. However, the message latency would be extremely high, with no guarantee of delivery.

1.4 TECHNIQUES IN BOTNET TO EVADE DETECTION[4]

(A)Fast Flux (FF): A mechanism that a set of IP addresses change frequently corresponding to a unique domain name.

(B)Domain Flux (DF): A mechanism that a set of domain names are generated automatically and periodically corresponding to a unique IP address.

The rest of the paper is dividing as follows in section II, we focus on different botnet attacks. Following that we introduce how recent approaches were developed to detect botnet in section III. In section IV, we briefly introduce the Defense and takedown techniques. At last, in section V provide the conclusion.

II. BOTNET ATTACKS[5]

(A) Attacking IRC Networks: Botnets are used for attacking IRC networks. The victim is flooded

by service request from thousands of Bots and thus victim IRC network is brought down.

(B) Distributed Denial of Services (DDoS): DDoS is a attack on a computer system or network that causes a loss of services/network to users by consuming the bandwidth of the victim network. The resource path is exhausted if the DDoS- attack causes many packets per second (PPS). The DDoS attacks are not limited to Web servers, virtually any service available on the internet can be target of such an attack. Higher level protocols can be misused to increase the load even more effectively by using very specific attacks such as such as running exhausting search queries on bulletin boards or recursive HTTP-floods on the victim's website called spidering.

(C) Key Logging: With the help of a key logger it is very easy for an attacker to retrieve sensitive information. There exists filtering mechanism that aid in stealing secret data.

(D) Sniffing Traffic: Bots can also use a packet sniffer to watch for clear text data passing by compromised machine. The sniffers are used to retrieve sensitive information such as usernames and passwords.

(E) Spamming: Some bots can open a SOCKS v4/v5 proxy—a generic proxy protocol for TCP/IP-based networking applications—on a compromised machine. After having enabled the SOCKS proxy, this machine can then be used for nefarious tasks such as spamming. With the aid of Botnet, an attacker can then send massive amounts of bulk e-mail (spam). Some Bots also harvest e-mail addresses (by opening a SOCKS v4/v5 proxy).

(F) Advertisement Installation: Botnets setup a fake web site with some advertisements. The operator of this website negotiates a deal with some hosting companies that pay for clicks on ads. With the help of Botnet, these clicks can be 'automated' so that instantly a few thousands Bots clicks on the pop-ups, hijacks the start page of a compromise machine so that the 'clicks' are executed each time the victim uses the browser.

(G) Spreading New Malware: This is easy since all Bots implement mechanisms to download and execute a file via HTTP or FTP. Thus, spreading virus via e-mail is very easy using a Botnet.

(H) Manipulating Online Polls or Games: These are very easy to manipulate due to high attention. Since every Bot has a distinct IP address and do the manipulation. Every vote will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way.

(I) Mass Identity Theft: By combining above different functions, they are used for large scale identity theft which is one of the fastest growing crimes on the internet. Bogus e- mails that pretend to be legitimate (such as banking e-mail) ask their internet victims to go on line and submit their private information. The fake e-mail are generated and sent by Bots via their spamming mechanism. These Bots can also host multiple fake web sites and as and when one of these fake sites is shut down, another one can pop up. In addition, key logging and sniffing of traffic can also be used for identity theft.

III. BOTNET DETECTION

3.1Analysis of network traffic

The network traffic monitoring and analysis approach is useful to identify the existence of botnet in the networks. A collection of the signatures and behaviours of existing botnets was made, to build a common botnet model, which is independent of botnet protocol and structure. This model can be used to detect botnets. With this model, botnets based on several network traffic anomalies such as high network latency, high volumes of traffic, traffic on unusual ports can be monitored. Even some unusual system behavior that could indicate presence of malicious bots in the network may also be detected. With the common botnet model, defenders can identify the hosts that share both similar communication patterns and similar malicious activity patterns. Although, this technique is powerful for detection of known botnets, it's not effective as we think, in detecting new botnets, especially in monitoring encrypted C&C traffic.

3.2 Host based Detection

Host based detection is simple but effective technology .signature based malware detection and behaviour based detection both fall into this category. signature based malware detection is effective and still widely used. But botmasters may deploy polymorphic technology to defend against signature detection. Luckily, the bots behaviour wont change much. Security defenders could analyze the behaviour of sample bot, such as registry logging, secondary downloading, and

service registering, etc, combined with other information gained from reverse engineering; security defenders could make a custom detection toolkit.

IV. BOTNET DEFENSE[6]

4.1 Honeypot-Based Monitoring

Botnet monitoring helps defenders understand its working patterns, find design vulnerability, and spy on plain command text. honeypot monitoring has been widely used in monitoring botnet activities. Defenders could configure a honeypot to serve as a servant and join the botnet. Because our proposed botnet can delete inactive servants from its peer-list, the honey pot should act as a real servant in order to monitor the botnet as long as possible. in this way, defenders have opportunities to obtain the plain text of commands. Defense against Domain flux Domain flux technology has three important features

1) bots send out a lot of Dns resolution requests to a DNS server in a short time

2) most requested DNS have common substrings; and

3) most requested DNS will receive empty A-records because the requested DNS has not registered .Considering these three features, we can detect Domain flux network flow at the gateway of LAN. First, collect DNS request information including the requested DNS, timestamp, end the source IP address from where the request is sent out. Also, the response from the DNS server should be recorded, including the request DNS, destination IP address and responding A-record. Combining the above results, we will know exactly which ip address send out a DNS request at a specific time and the response is also known. In a time window, calculate the longest common substring of all the requested DNS sent out in the while. If the number of requested DNS which have the longest common substring and have an empty A-record exceeds threshold representing a normal web application. We can determine that the host is in domain flux programs. Subsequent DNS requests containing the lognest common substring could be blocked to cut off the communication between bots and command server.

4.2 The index Poisoning

index poisoning attack is done by inserting massive numbers of bogus records into the index of P2P file sharing system[5]. It is used to prevent illegal distribution of copyrighted content in P2P networks. The same technique can also be used to mitigate P2P botnets, because most P2P botnets make use of the indexes in P2P networks to implement their C&C mechanism, such as Stormnet and Peacomm botnet. With the help of honeypots and reverse engineering techniques, defenders are able to analyze behaviors of bot programs and find out the index which is related to the command of botmaster. Because of the limited of index that is used for command distribution, in some sense, the C&C architecture of P2P botnets is similar to that of the traditional centralized botnets. Index-based P2P botnets logically rely on predefined indexes, just like traditional botnets physically rely on central points or communication. And in most of the P2P networks, there is no central authority to manage the index. Therefore, any node no matter benign or malicious is able to insert records into the index. And in the past, there is no algorithm to authenticate the identity of the node and content of the records. That is why P2P botnets are vulnerable to index poisoning attack.

4.3 Fluxing Mitigation

Automatic identify FF that recorded in domain blacklist. Blacklist can be used to stop FF by collaboration from domain name registrar. Registrar had authority to shut down a domain this effectively taking down scam. Automatic black list of FF domain can quickly notify registrar about fraudulent domains.ISP can use such a blacklist to protect its cline from FFSN, blacklist derived from DSNBL. Domain blacklist can be used for spam filtering.

V. CONCLUSION

Botnet are growing and evolving fast but there are some things we can expect. They will be easily extended and upgraded. They will traverse multiple types of network and protocols. Their master will not be easily found since not even the bot knows where to find him. They wont be easily hijacked as they only accept digitally signed commands. They will be able to directly change transactions made by users on websites and online banks, without needing to steal credentials. They will use as communication vectors protocols that can’t be easily blocked without causing harm, like http.

Despite of above mitigation method botnet owner continuously evaluate sound botnet so for the combating against them security researcher and antivirus vendor require continues monitoring to

exploit new botnet features and develop mitigation technique.

REFERENCES

[1] Aniello castiglione, Robert De Priso, Alfredo De Santis, Ugo Flore, Francesco Palmieri, "A botnet based command and control approach relying on swarm intelligence", Journal of Network and Computer Application.

[2] Kuchen Wang, Chun-ying huang, Shang-Jyh lin, Ying-Dar-Lin."A Fuzzy pattern based filtering algorithm for botnet detection", Journal of Compute Network.

[3] Michael Bailey,Evan Cook,Farnam Jahanian,Yunjing Xu,Manish Karir"A Survey On Botnet Technology and Defensed",University of Michigan.

[4] Lei Zhang, Shui Yu, Di Wu, Paul Watters, "A Survey On Lateset Botnet Attack and Defense", Deakin University, University of Ballarat.

[5] Jivsh Govil, Jivika Govil, "Criminology of Botnets and their Detection and Defense Methods",IEEE EIT 2007.

[6] C.Czosseck, E. Tyugu, T. wingfield, "On the arms race around botnets-setting up and taking down botnets",2011 3rd international conference on cyber conflict.