IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Botnets : A Survey

Ankur Singh Bist
Govind Ballabh Pant University of Agriculture And Technology,Panthnagar, India
ankur1990bist@gmail.com

Abstract

Botnet is a network of machines infected by malware support the command and control structure that makes it different from other malicious codes . In this paper our motto is to study various issues related to evolution and detection of botnets as well as to study about botnet tracking tools .

Keywords- Botnet , Command and Control.

Introduction

Malicious codes are very dangerous for computer security . Malicious codes in form of spyware , malware , metamorphic and polymorphic viruses are present to create harmful scenario . Botnets is another name that is much powerful and have capability to take over large number hosts and have this intention also which is provided by their designers .

Initially the command and control infrastructure adopted by botnets are not made for harmful purpose but it get used . In 1993 , bot named Eggdrop come into existence that has IRC as its architectural features and was made for UNIX/LINUX operating system . After that various bots got arise like gtbot ,netbus ,!a , backorifice2k ,sdbot ,gaobot ,slapper , agobot ,spybot ,sinit ,rbot ,bagle ,phatbot ,polybot ,mytob ,rustok ,nugache , torjan.peacomm ,srizbi , storm and many more bots are detected . Most of them are made for windows operating system and used IRC , P2P ,HTTP as their architectural features. These all bots are mainly responsible for DDOS attacks . Mainly IRC channel get used by Botnets for their working . Various techniques like data mining techniques are used for botnet detection but still lot of work is to be done to defend the attacks of botnets .

Various Issues Of Botnets

Bot can be defined as an executable file and it contains the capability of performing various functions on getting triggered by specific command . Victim machine , IRC server , control channel are the important elements used in botnet .

The life cycle of botnet includes various phases [2] :----

1. Botmaster create the infection sequence using bot through various modes like attachment in mail .
2. After that command and control channel get used by bot .
3. IRC , HTTP etc . get used by Botmaster .
4. There are various army bots to make control from main central point .

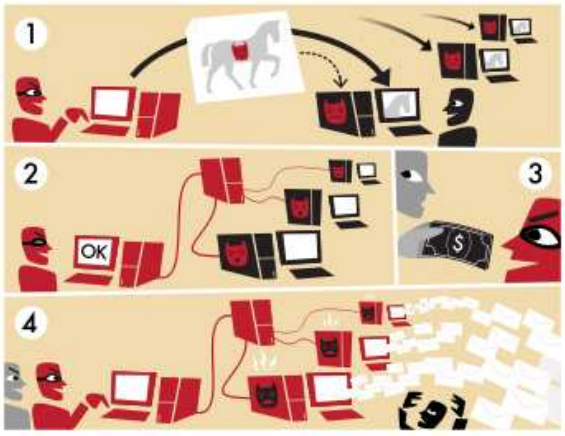

Figure . botnet is created and used to send email spam [1]

Torpig is malicious program that refer to a type of bot to retrieve various information from victim . Brett Stone-Gross , Marco Cova , Lorenzo Cavallaro , Bob Gilbert , Martin Szydlowski , Richard Kemmerer in their paper explained the Torpig network infrastructure that contain various elements[3] :--

1. Vulnerable web server
2. Victim client
3. Mebroot driven by download server
4. Torpig command and control server
5. Injection server

Mebroot does not contain any malicious activity intention but it provides a platform that can be used by other modules to perform their malicious actions . Torpig utilizes different procedures to locate command and control server which is called domain

flux .With the help of domain flux domain generation algorithm is used by bot to obtain a list of domain names . Finally various analysis get made by authors[3]:-------

1. Evaluation of botnet size based on cont of different IPs yields grossly overestimated result .
2. The victims use poor password that can be guessed easily , this problem is treated as cultural problem .

Botnet classification is done in different ways[2] :----

1. According to communication topology
   - 1.1 Centralized model
   - 1.2 Decentralized model
   - 1.3 Unstructured command and control model

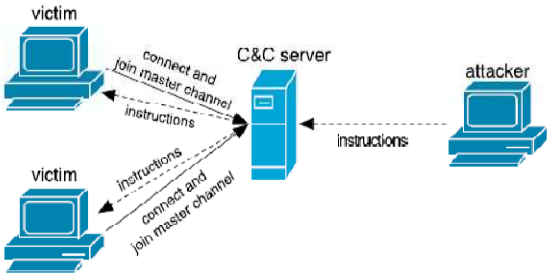

Figure 2. Communication flow in botnet[5]

2. According to network protocols
   - 2.1 IRC oriented
   - 2.2 Instant messaging oriented
   - 2.3 Web oriented

Botnet detection is done in different ways[2] :----

1. Using Honeynet based approach
2. Passive techniques
   - 2.1 Signature based detection
   - 2.2 Behavior based detection
   - 2.3 Anomaly based detection
   - 2.4 Domain name system based detection
   - 2.5 Detection based on data mining techniques

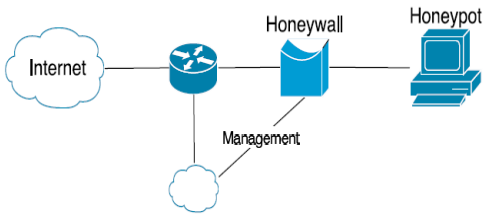

Figure 3. Botnet tracking setup[5]

In the centralized model the dependency is on some specific servers but it is not the case of decentralized models . They use various protocols IRC ,P2P , HTTP to communicate all have various strength and weakness associated with them but they are very dangerous when used by botnet in encrypted forms . distributed denial of service , Fast flux that tries to details of main servers , Sniffing , Adware , Spamming are various attacks that are chosen by botnets . Various techniques that are used for detection includes Honeypot based methods that includes end host that is not resist to attacks and can be used for various analysis , further the signature based approach based on past available data but as usual like the case of simple viruses this technique is not good for new viruses due to this other methods are used that adopt various analysis based on network behavior and other defined analysis . Data mining including other elements like neural network , supported vector machine , expert systems , genetic algorithms are used for some better analysis . Now hybrid approaches are also used that contain the combination of behavioral approaches and data mining approaches to overcome this problem .

Tools For Botnet Analysis

There are three main goals of tracking botnet[4]:----

1. Malware sample collection
2. Study the behavioural intension of botnet designers
3. Forensic uses

Arbor botnet tracking project mainly focuses on various observations done on the various distributed denial of service attacks .Finally this project lead to obtain various important results[4] .

Nepenthes platform that is a simulation tool is widely used to get the various efficient observation regarding botnets . Nepenthes sensor is capable to classify payloads into their protocols and family and then determine if they represent known attack . Which botnet to track and analyse is another problem . Dynamic analysis of malware includes the activity of malware sandbox. Python is a secure language for writing a script to monitors botnets and after this malicious activities get filtered . Now various growing malwares contains anti sand box method that is they contain the logic to identify reverse engineering . Such code can be listed from Phatcode codebase . Various executable packer like Themida packer is used in these situations[4] .

Conclusion

In this paper firstly we discuss about the evolution of botnet and give example of different botnet with their way of expansion , platform and detection mode. We give a summarised look on classification and various detection method of botnets . Finally we discuss various botnet tracking tools .

Future Research Work

Future research includes the creation of data repository for known botnets for the improvement in

detection algorithms . It is also needed to develop an efficient antibot application with the strong analysis parameter of botnet behaviour in network like " what will be the behaviour of botnet when some of related nodes get detected " are needed to be focused in ternm of further development .

References

[1] www.wikipedia.com
[2] Amit kumar Tyagi , G. Aghila , "A wide scale survey on botnet " , international journal of computer application " .
[3] Brett stone gross , Marco cova , Lorenzo cavallaro, Your botnet is my botnet :Analysis of botnet takeover
[4] Dr. Jose Nazario ,"Botnet tracking :tools ,techniques , and lessons learned".
[5] Rwth Aachen ," Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks ".