International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 1, March-May, 2017 | Pages 37-44

LARGE SCALE BOTNET SPAMMING DETECTION AND PREVENTION

Vinit. K[1], S.Shruthi[2], D.Aravind[3], V.Rakesh[4]
[1]Assistant Professor, [2,3,4]UG Scholars, Computer Science and Engineering
SRM University,Vadapalani Campus, Chennai, Tamil Nadu, India

Abstract: Botnets are mostly used for cyber-criminal activity. It is used for spamming, phishing attacks, denial of service attacks and etc. Botnet can be defined as the range of computers that are controlled by a bot master. They can also be defined as software robots that are controlled by a large entity called the botmaster. In this paper we detect the botnet using a new technique that is based on detecting the anomalies in a network. Depending upon the anomalies that are detected in the network, we detect the botnets using the Coarse Grained algorithm which identifies the bots that are written in a normal file and sent to the users by the servant bots. The botnets have created a huge loss in many businesses and organisations. Because of these losses the botnet crimes has received some attention. Therefore in order to reduce the cyber crimes due to bots we propose this paper and provide a better solution than the other methods.

Keywords – Botnets, Anomalies, Cyber Crimes, Social Network, Spams, Botmaster.

I. INTRODUCTION

Botnets can be defined as net hosts that have fallen under the control of a bot master or are network of compromised hosts[3].The functions of these botnets are penetration, enumeration and propagation. During the process of controlling the host computers, the bot master usually targets random ip addresses and use as their slave for performing the service attacks [5]. This bot master uses a technique known as horizontal scanning method that checks the vulnerability of the system and uses a code called worm code that exploits a system that is going to be used as target machine. The cyber crimes that are usually created by these bots are very infectious and causes harm to a company. The intrusion detection technique is a little ineffective in preventing the bot nets from being formed. Earlier methods that involved bot detection used Bot hunter and Bot Magnifier which were not successful in detecting all the bots and were less effective in its functions. In our paper we observe the network for anomalies and bots and we also create a traffic filter and a system protection status display that haves an updated condition of the system and its components from being attacked by the harmful bots. In general spam bots and other bots cannot be detected easily by the already existing methods [6].

II. EXISTING SYSTEM

For the existing detection method, in the network the bot may not be detected by the firewall as the firewall usually identifies a virus contained file’s extension and blocks the file if it is infected. In such cases the file is not completely scanned and therefore the file infects the computer. It is mainly due to the fact that the traffic profile of a bot-compromised host might be completely distorted. The existing system is less effective to detect the bots that are shared from one peer to another. This does not promote wide scale botnet detection [1].As the drawbacks in existing system the command and control channel that is used as communication component in the nodes is ineffective and it completely distorts the peer to peer connection. Several methods were used as an alternative approach to detect the harmful bots but despite these methodologies the bots were not identified with correctness and were not judged whether the files were really infected or not.

III. PROPOSED SYSTEM

In the proposed system, using the clustering algorithm or using the coarse grained algorithm technique we detect the bot files that are shared among the users, using a scanner that is fed in the system. The scanner scans the content of each file that is shared between two users by regulating the protection status of the scanner. The scanner is active when the protection status is left on and when in “OFF” state the scanner doesn’t scan the files that are being shared. When the scanner of the system is kept in “ON” state the file which is shared can be scanned completely and if the file is a bot file, the scanner scans it and blocks the whole file and also finds the ip address of the system from which the malware file was shared to another system. So when the ip address is detected, the same is sent to the admin for observation and that ip address is permanently blocked from sharing any type of file to another user. By doing this the system remains malware free and also keeps a check of the blocked ip addresses.

IV. METHODOLOGIES

MODULE NAMES

This project having the following five modules

1. User Interface
2. Coarse Grained Peer to Peer Detection
3. BOT Detection
4. Botnet elimination using behavior clustering
5. Blocking attackers IP address

A. USER INTERFACE

We create windows which is used for sending files from one user to another. Using the Swing package available in Java we design the User Interface. Swing is a widget toolkit for Java. It is part of Sun Microsystems Java Foundation Classes an API for providing a graphical user interface for Java programs.

B. COARSE GRAINED PEER TO PEER DETECTION

This detects the peer to peer clients by analyzing network flows after the Traffic Filter component. For each host *h* within the monitored network we identify two flow sets, denoted as *Stcp(h)* and *Sudp(h)*, which contain the flows related to successful outgoing TCP and UDP connection, respectively [2]. SYN, SYN/ACK, ACK handshake, and those UDP connections for which there was at least one “request” packet and a consequent response packet.

C. BOT DETECTION

When a bot is shared from one user to another the bot is detected using the scanner that is installed in the system. The scanner detects the bot or the botnet and the traffic filter is used for monitoring the process that is being carried out [4]. by completely reading the file that is infected by a virus that is disguised as a normal text file or a document. Since bots are malicious programs used to perform profitable malicious activities, they represent valuable assets for the bot master, who will intuitively try to maximize utilization of bots. This is particularly true for P2P bots because in order to have a functional overlay network a sufficient number of peers needs to be always online. In other words, the active time of a bot should be comparable with the active time of the underlying compromised system.

D. BOT ELIMINATION

Once a bot is detected by the coarse grained algorithm technique it also finds the ip address which is related to the bot which was being shared between the peers. The ip address is identified and using the clustering algorithm the ip address is grouped, blocked and sent to the admin for observation and is stored in a memory as a bot. Once if the bots are detected

E.BLOCKING ATTACKERS IP ADDRESS

Once the ip address is detected, it is sent to the admin and blocked by the server to avoid further sharing of bot files.

V. ALGORITHM USED:

Coarse-Grained Detection of P2P Bots:

The coarse grained algorithm technique is responsible for detecting the peer to peer clients by analyzing network flow using the traffic filter component. It is a method used for sharing the file from one user to another in a network. A peer to peer network of pivotal nodes are created and document files or text files are shared amongst the two users. When a virus file is fed into a normal text file an antivirus fails to scan the file completely. In such case, using a scanner that is built based on the coarse grained technique will be used in order to check the virus content that is hidden in a normal file. Coarse Grained is basically used to hold the important or the related data, or in other words splitting up into smaller pivotal units that are related to the process.

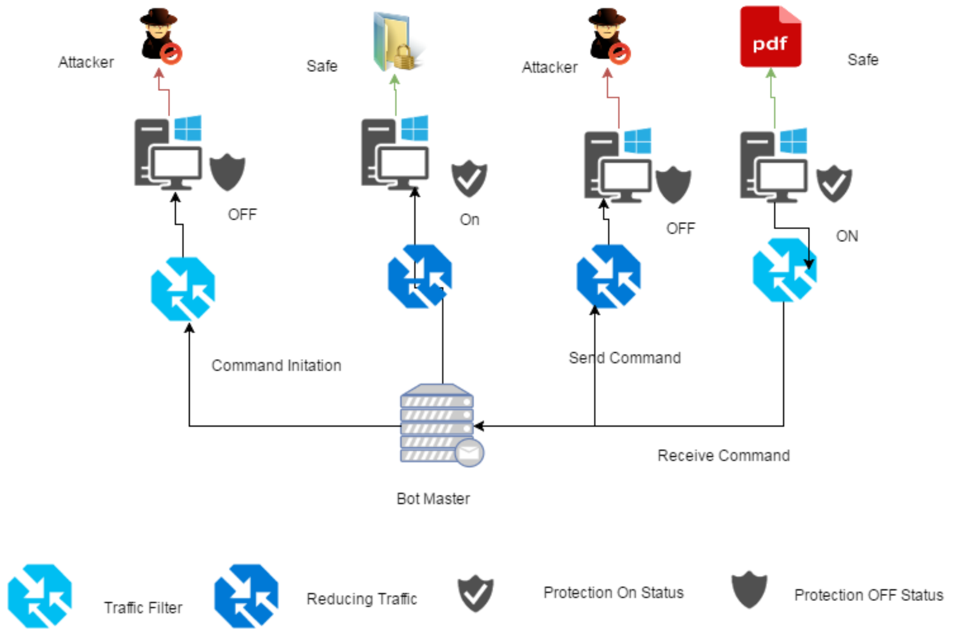
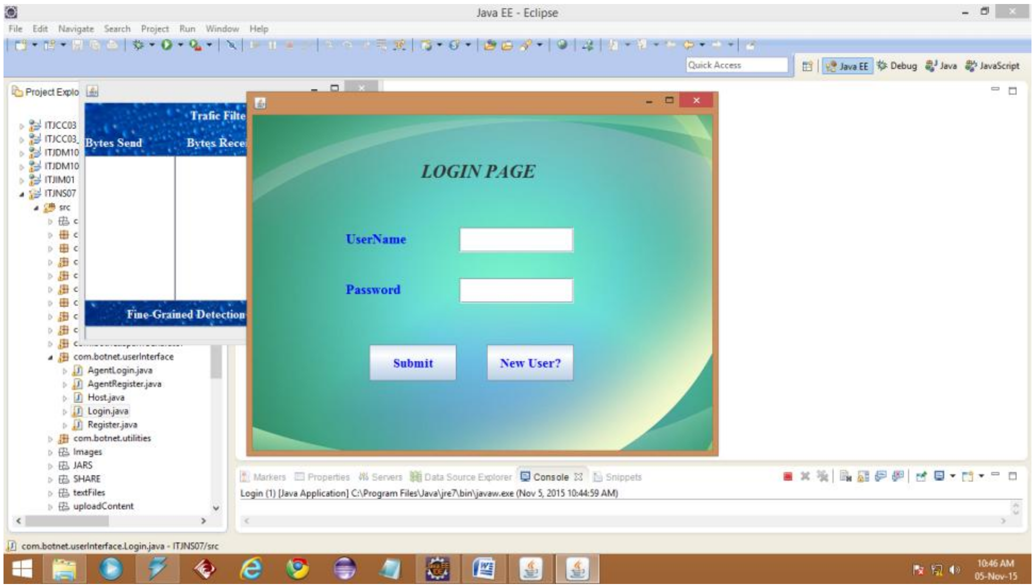


Fig 3 - System Architecture

As in Fig3, the systems architect establishes the basic structure of the system, defining the essential core design features and elements that provide the framework. The systems architect provides the architects view of the users' vision. Above diagram user first login to the account then he can upload or download a file which are available in server.

VI. RESULTS



LOGIN PAGE

UserName

Password

```
Login (1) [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Nov 5, 2015 10:44:59 AM)
```

Fig. 4 - User Given Input Interface Design

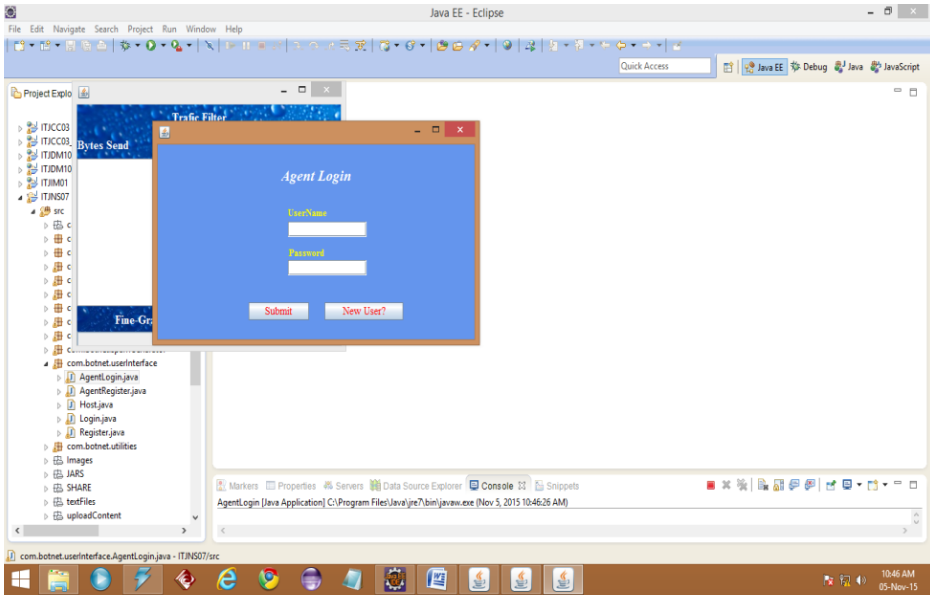
Input:

Ip address Port number

Output:

User window

Authentication-Admin:



AgentLogin [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Nov 5, 2015 10:46:26 AM)

Fig. 4 - Design for sender authentication page

Input: Username and password

Output: valid or invalid

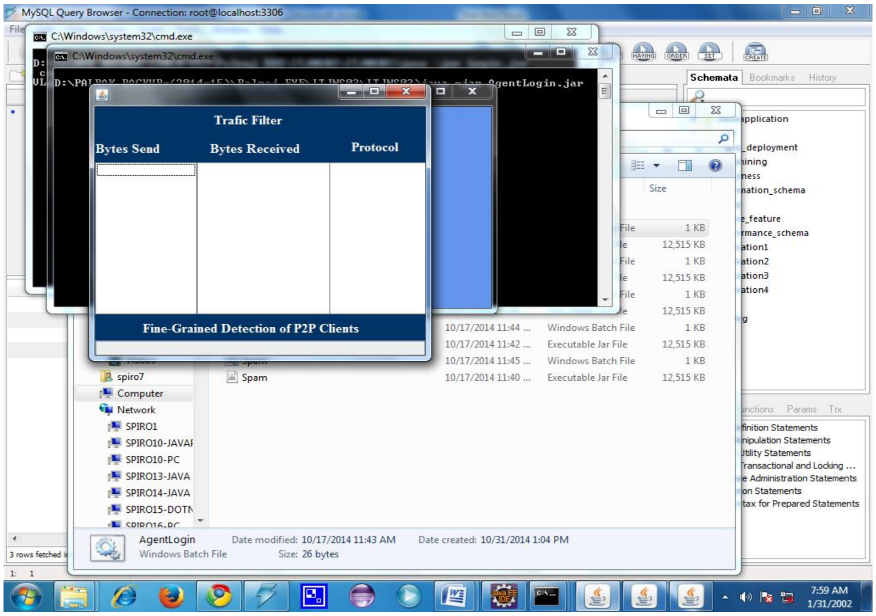
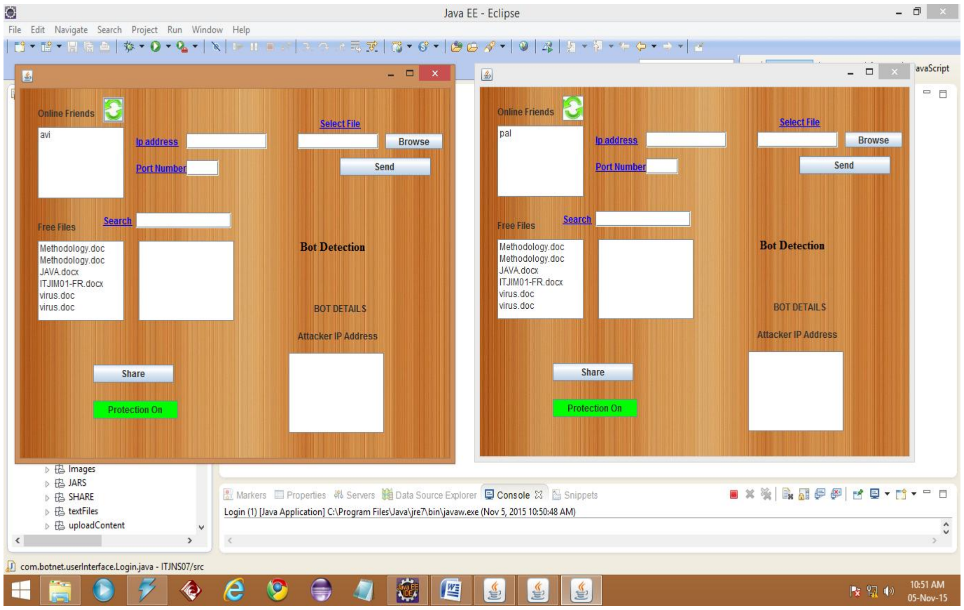

MySQL Query Browser - Connection: root@localhost:3306
C:\Windows\system32\cmd.exe
Trafic Filter
Bytes Send
Bytes Received
Protocol
Fine-Grained Detection of P2P Clients
Schemata
Bookmarks
History
Computer
Network
AgentLogin
Windows Batch File

Fig.6: Traffic Filter which monitors and checks the network traffic simultaneously



avi

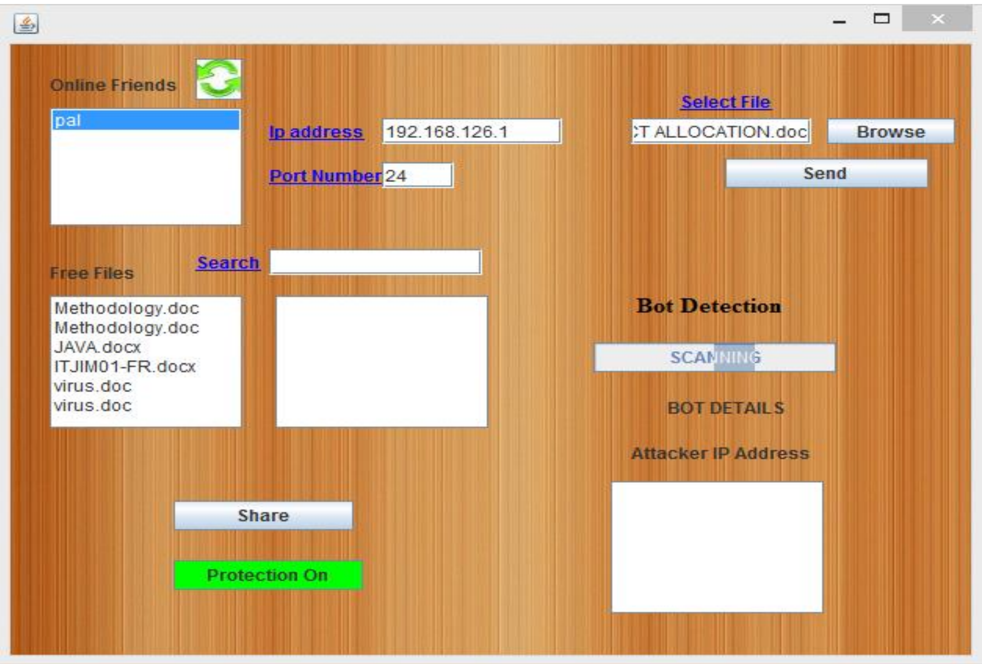
pal

Methodology.doc
Methodology.doc
JAVA.docx
ITJIM01-FR.docx
virus.doc
virus.doc

```
Login (1) [Java Application] C:\Program Files\Java\jre7\bin\javaw.exe (Nov 5, 2015 10:50:48 AM)
```

Fig.7- One user selects the file to be sent to another and it is noted that the protection status of the system remains in "ON" state

Input: File Upload Output: File Sending



pal

Ip address 192.168.126.1

Port Number 24

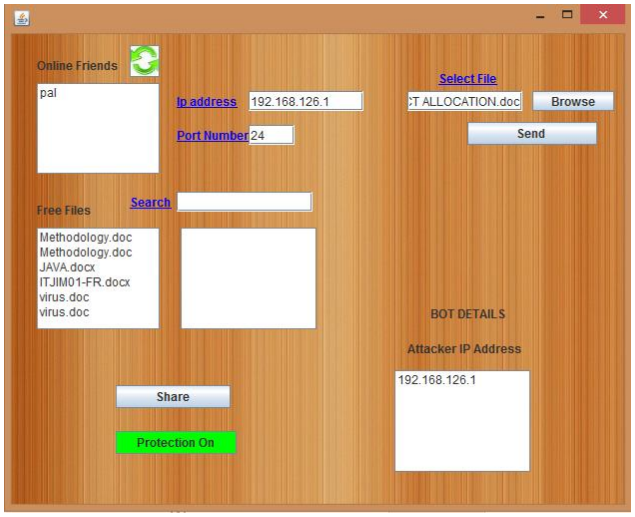
:T ALLOCATION.doc

Methodology.doc
Methodology.doc
JAVA.docx
ITJIM01-FR.docx
virus.doc
virus.doc

Fig 8 Shows that whenever a file is being shared between the users, the in-built scanner checks the content of the file.

Input: File Sent

Output: File Scanning Done



Online Friends: pal

Ip address: 192.168.126.1

Port Number: 24

Select File: :T ALLOCATION.doc

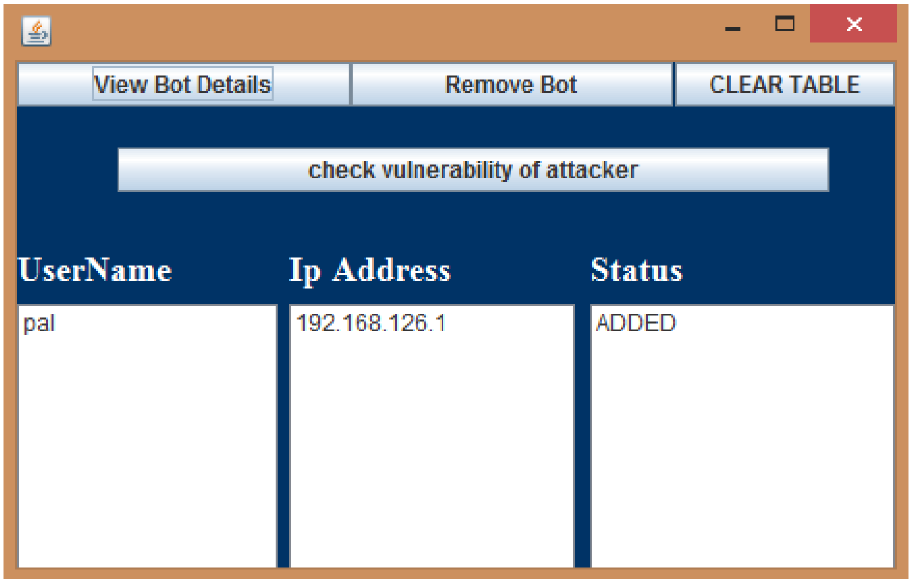
Free Files:
Methodology.doc
Methodology.doc
JAVA.docx
ITJIM01-FR.docx
virus.doc
virus.doc

Attacker IP Address: 192.168.126.1

Fig.9 - An example that displays the IP address of the attacker for the user's observation

As mentioned earlier, once when a virus fed document is shared by the user, the scanner detects the file, blocks the file and displays the Ip address of the attacker for the user's observation. The above given fig 9, is an example of such a process.

Input: 1st Phase Detection results
Output: Attacker's Ip address



UserName	Ip Address	Status
pal	192.168.126.1	ADDED

Fig.9 – Attackers information stored as a blocked content

So finally, the attackers information will be stored as a blocked content in the admin's memory where that particular user is not allowed to share files to other users anymore.
Input: 1st phase Detection results
Output: Ip address

VII. CONCLUSION

In this paper, we presented a botnet detection using behaviour clustering system that is able to identify stealthy P2P botnets, whose malicious activities are tracked, controlled and blocked.

VIII. FUTURE SCOPE

To summarize, although our system greatly enhances and complements the capabilities of existing P2P botnet detection systems, it is not perfect. We should definitely strive to develop more robust defense techniques, where the aforementioned discussion outlines the potential improvements of our system. Botnet developers are constantly improving their development in order to produce more and more stealthy malware for all kinds of attacks to make profit. While various approaches have been studied or used for botnet attacks, the risk of exploiting widely used browser extensions and their automatic browser extension update mechanisms for command and control channel has not been practically investigated. In this study, we show that it is not difficult to construct stealthy botnet via browser extensions

REFERENCES

[1] “Wide scale botnet detection and characterization” 2016 http://www.engpaper.com/botnet-2016.htm

[2] Jing Wang and Ioannis Ch. Paschalidis “ botnet crimes has received attention” on IEEE paper, 2016

[3] Shahid Anwar, Jasni Binti Mohamad Zain, Mohamad Fadli Bin Zulkipli, Zakira Inayat - A review paper on botnet and botnet detection in cloud computing “botnets are network of compromised hosts” https://www.researchgate.net/publication/283257776_A_Review_Paper_on_Botnet_and_Botnet_Detection_Techniques_in_Cloud_Computing

[4] Shehar bano “botnet detection and traffic” 2012 A study of Botnets on http://www.cl.cam.ac.uk/~sk766/publications/ms_thesis_sheharbano.pdf

[5] Michael Bailey, Evan Cooke, yunjing xu, Manish Karir “botnet attackers choose random victim computers” http://nsrg.eecs.umich.edu/publications/catch09_botnets_final.pdf 2009

[6] Zhaosheng Zhu ; Guohan Lu ; Yan Chen ; Zhi Judy Fu ; Phil Roberts Keesook Han “botnets are collection of software robots” http://ieeexplore.ieee.org/document/4591703/?reload=true