ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

ANOMALY- BASED BOTNETS DETECTION FRAMEWORK TO PREVENT FINANCIAL FRAUD

M.D. Amala Dhaya,
Assistant Professor,
Department of Computer Science and Engineering,
Loyola Institute of Technology of Science

Dr. R. Ravi
Professor & Research Centre Head,
Department of Computer Science and Engineering
Francis Xavier Engineering College,
Tirunelveli - 627003, Tamil Nadu State, India.
fxhodcse@gmail.com

ABSTRACT

Financial fraud has become very serious in today's world; as a result various solutions are adopted to overcome it. Administrators in financial sector need to be updated with the latest advancements in hardware and software system in financial sector to protect their systems as well as the user's data. The architecture of the financial process can be modified to prevent these attacks. This paper develops an automatic categorization system to detect the phishing websites and malware samples with the use of cluster ensemble. By aggregating the clustering solution generated by different clustering solution we detect the phishing websites and malware samples to Prevent Financial Fraud using resilient identity. The network can be differentiated into comprised systems and un-comprised systems. Here we detect the un-comprised systems.

Keyword- Botnets, Anomaly, phishing websites

1. INTRODUCTION

Financial botnets are targeted to carry out financial fraud; which is a well-known threat for banking organizations all around the globe. Botnets are responsible for targeting huge money losses or for conducting money laundering operations. Botnets are the base for many network crimes in recent years. New Bots use advanced P2P protocols to establish command and control system based on user behavior. Banks are implementing advanced security measures and policies, and fraudsters are very much motivated to respond by changing their operations. Cyber security measures must be advanced on detection of cyber attacks and preventing the cyber criminals from accessing valuable key assets. It means applying internal solutions that will help to detect and contain intrusions quickly. The challenge for financial operations in executing such valuable authentication method will be in forwarding it across many different channels. As these fraud shifts take place, financial sectors should look for a central fraud observatory setup or hub that can track different trends across channels and lines of

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

enterprise business [1-4]. This will enable organizations to track and react as financial fraudsters look for new vulnerabilities. The important attacks are listed in the below,

Types of attack:

Attack is defined as an action that comprises the security of information owned by the organization

Passive Attack

The opponent wants to obtain the information that is being transmitted in bank and involves no alteration

Active Attack

Active attack involve alteration to the data

Phishing Attack

Through phishing attack the hacker creates a false web page that looks like a popular site of a bank or exactly like paypal. The phishing part of the attack happens that the botnet sends an e-mail like a hacker sending a message trying to deceive the user to activate by clicking a link that leads the users to the fake site. When the user tries to log on into their account details, the hacker records the username and authentication then tries the collected information on the real website [5-8].

2. EXISTING SYSTEM AND LIMITATION

Methods / Approaches:

- Host analyzer
- Network analyzer
- Correlation engine
- IP reputation system
- Discrete Time Series Analysis

Limitations:

- Traffic Volume may be low
- Does not violate network protocol rule
- Traffic communication might be encrypted
- May have a less number of botnets in the monitoring network
- Due to the stealthy - difficult to identify and complex to analyze
- Difficult and unlawful to collect the IP addresses of compromised computers
- Organizations are unwilling to give the intelligence information about cybercrime
- Lack of supporting framework to track and taking down financial botnets
- Most detection technique functions at the network level
- Requires the analysis of packets' payload
- It raises privacy concerns
- It incurs large computational overheads.

3. PROBLEM IDENTIFICATION

The existing system contains the following drawbacks:

- Traffic Volume may be low
- Does not violate network protocol rule
- Traffic communication might be encrypted
- May have a less number of botnets in the monitoring network
- Due to the stealthy - difficult to identify and complex to analyze
- Difficult and unlawful to gather the IP addresses of compromised computers
- Organizations are unwilling to share secret information about cybercrime

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

- Lack of supporting framework to track and taking down financial botnets
- Most detection technique functions at the network level
- Requires the analysis of packets' payload
- It raises privacy concerns
- It incurs large computational overheads.

4. PROPOSED SYSTEM

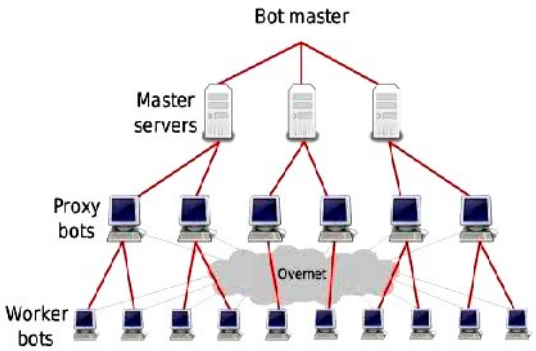


Figure 1 Botnet Architecture

Figure 1 shows the general Botnet Architecture of the proposed scheme. Attacking Behaviors are Distributed Denial-of-Service Attacks, Spamming, Sniffing Traffic, Key logging, Spreading new malware, Installing Advertisement Addons and Google AdSense abuse.

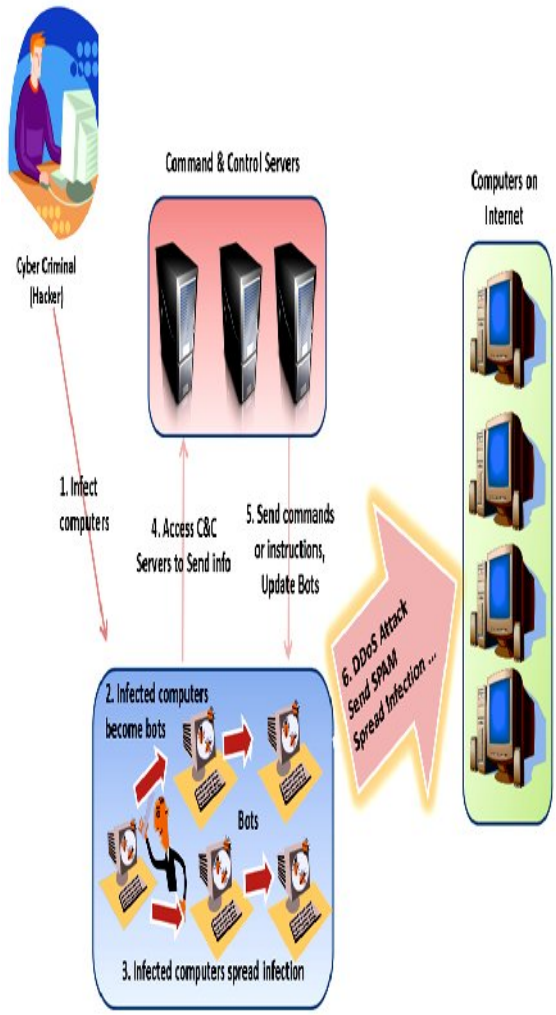


Figure 2 Botnet Operation

Figure 2 shows the Botnet Operation.

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

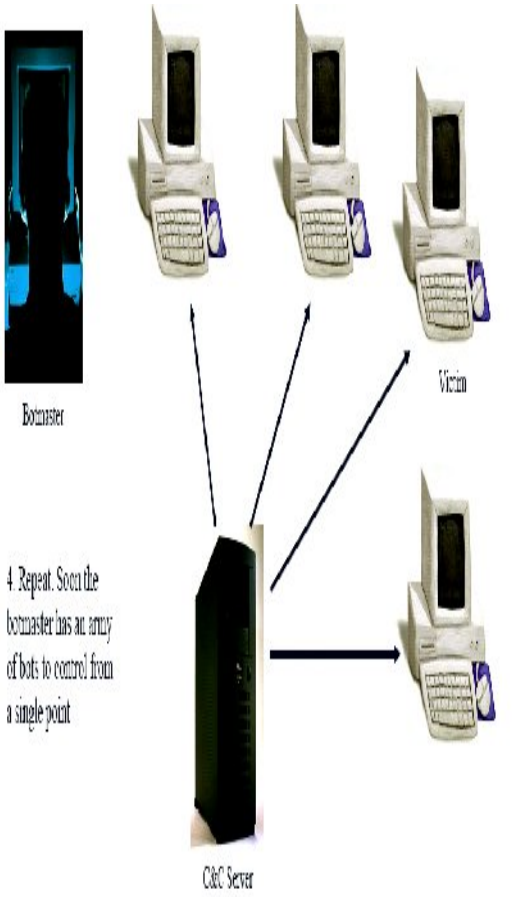


Figure 3 Botnet Propagation

Figure 3 shows the Botnet Propagation between the devices.

5. RESULT AND DISCUSSION

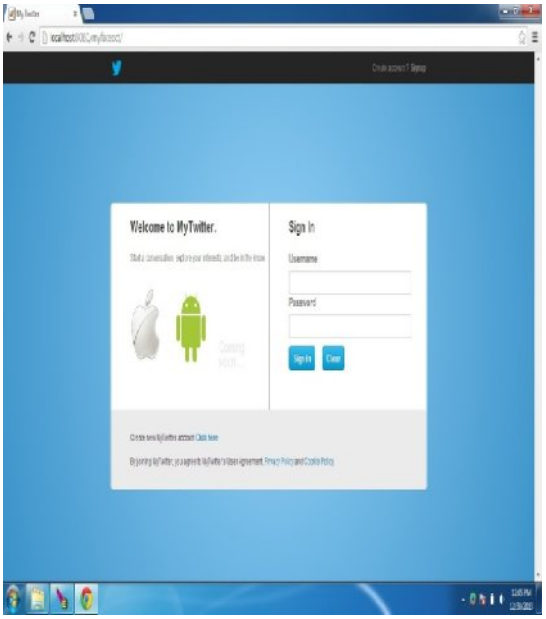
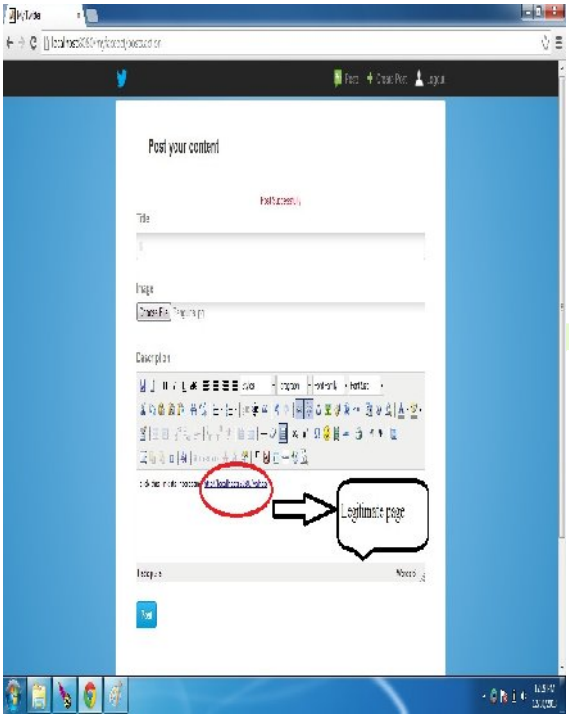


Figure 4 Front page

Figure 4 shows the Front page of the website.



ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

Figure 5 Legitimate Page

Figure 5 shows the Legitimate Page of the website.

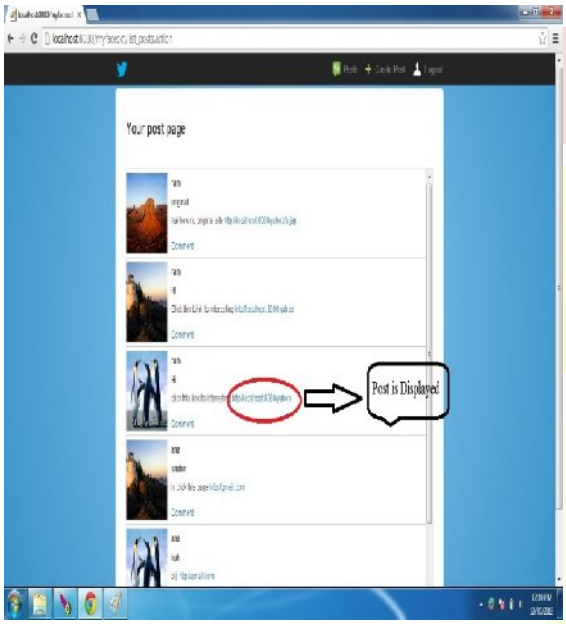


Figure 6 Post is Displayed

Figure 6 shows the Post is displayed in the website.

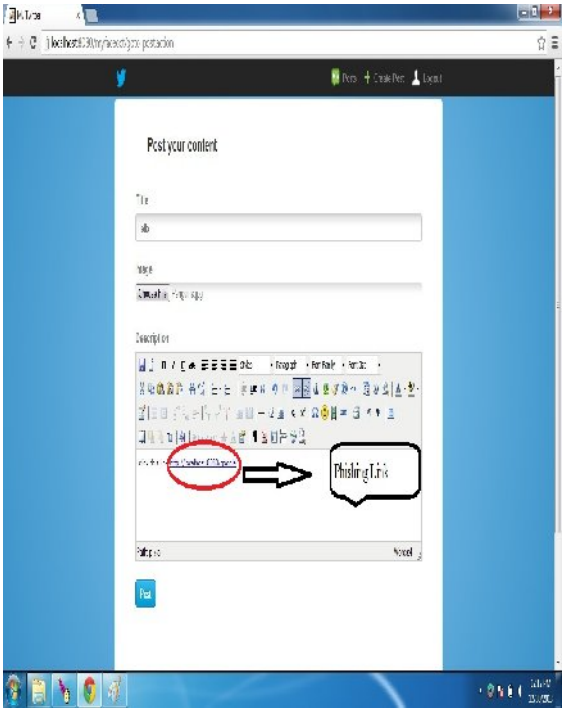


Figure 7 Phishing Link

Figure 7 shows the Phishing Link in the website.

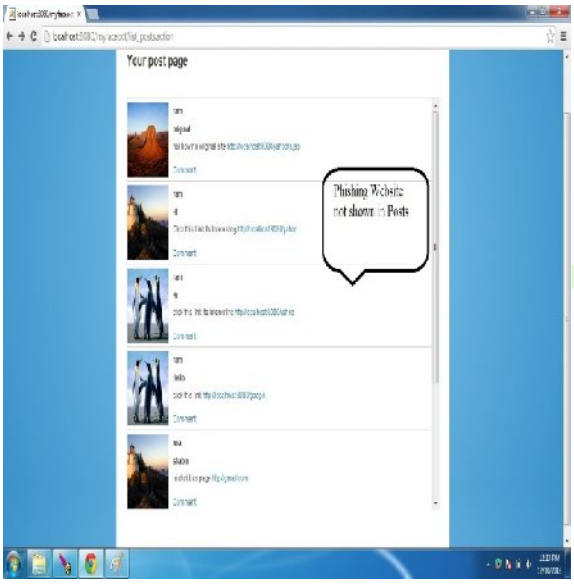


Figure 8 Phishing Website not Shown in Post

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

Figure 8 shows the Phishing Website not Shown in Post of the proposed scheme.

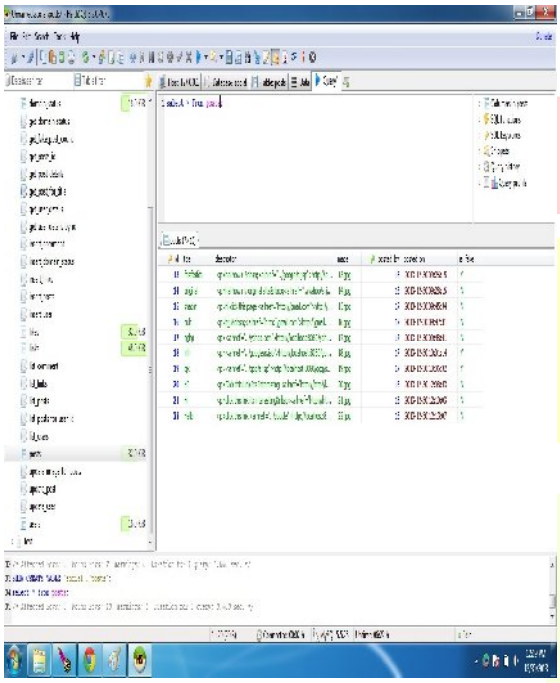


Figure 9 User Database

Figure 9 shows the User Database of the proposed method.

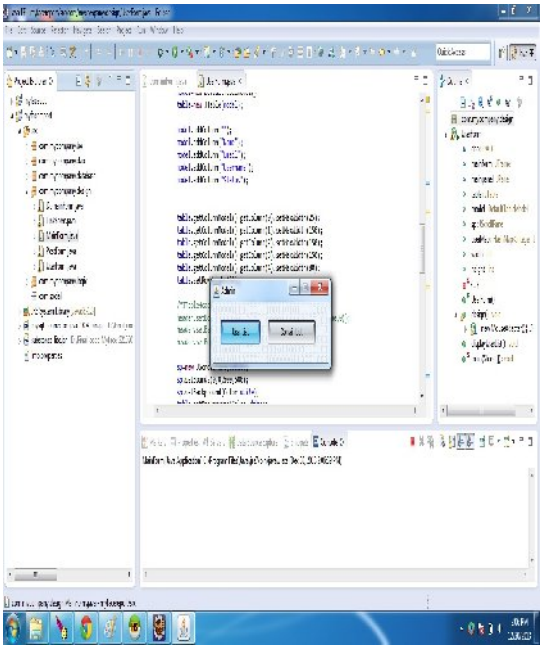


Figure 10 User List

Figure 10 shows the User List of the planned technique.

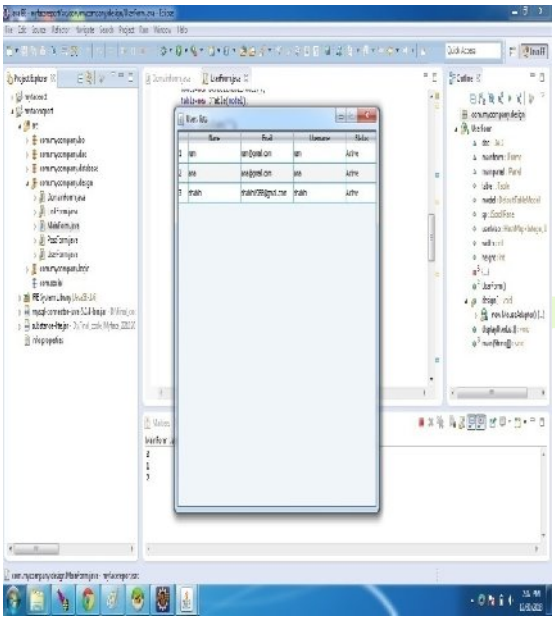


Figure 11 User Details

ISSN (ONLINE) : 2395-695X
ISSN (PRINT) : 2395-695X
Available online at www.ijarbest.com
International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST)
Vol. 1, Issue 4, July 2015

Figure 11 shows the User Details of the proposed scheme. Detect based on traffic movement anomalies such as High Network Latency, Huge Volumes of Traffic, Traffic on unusual ports and strange System Behavior.

6. CONCLUSION

As internet has become a huge part of our daily life, the need of bank security has also increased exponentially from the last decade. As more and more users connect to the bank it attracts a lot of criminals. Botnet research that can be categorized into three areas, i.e. understanding botnet, detecting & tracking botnets, and countering against botnets. In understanding botnet research, it is proposed to learn botnet behaviors and characteristics through source code analysis, binary analysis or wide area measurement. Using clustering techniques like hierarchical clustering and K-means clustering provides efficient results in real time categorization and also in malware instruction extraction. It provides a very good result.

7. REFERENCES

[1] P. Wurzinger, L. Bilge, T. Holz, J. Goebel, C. Kruegel, and E. Kirda, "Automatically generating models for botnet detection", In 14th European Symposium on Research in Computer Security (ESORICS'09), 2009.

[2] S. Gianvecchio, M. Xie, Z. Wu, and H. Wang, "Measurement and classification of humans and bots in internet chat", In Proceedings of the 17th USENIX Security Symposium (Security'08), 2008.

[3] Yuanyuan Zeng, Xin Hu, Kang G. Shin, Detection of Botnets Using Combined Host- and Network-Level Information, IEEEIIFIP International Conference on Dependable Systems & Networks (DSN), 2010

[4] J. R. Binkley and S. Singh. An algorithm for anomaly-based botnet detection. In Proceedings of the 2nd conference on Steps to Reducing Unwanted Traffic on the Internet, 2006. 978-1-4244-7501-8/10/$26.00 ©2010 IEEE

[5] J. Goebel and T. Holz. Rishi: Identify bot contaminated hosts by irc nickname evaluation. In HotBots'07: Proceedings of the first conference on First Workshop on Hot Topics in Understanding Botnets, 2007.

[6] G. Gu, J. Zhang, and W. Lee. Botsniffer: Detecting botnet command and control channels in network traffic. In Proc. of the 15th Annual Network and Distributed System Security Symposium (NDSS), 2008.

[7] Karasaridis, B. Rexroad, and D. Hoefiin. Wide-scale botnet detection and characterization. In HotBots'07, 2007.

[8] C. Livadas, R. Walsh, D. Lapsley, and W. Strayer. Using machine learning techniques to identify botnet traffic. In Proceedings of the 2nd IEEE LCN Workshop, Nov, 2006.