ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 7.327

Volume 6, Issue 10, October 2018

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Botnets: A constant threat to Cyberspace

Jimut Bahan Pal[1]
Department of Computer Science
St. Xavier's College (Autonomous), 30 Park Street
Kolkata, India.

Dr. Asoke Nath[2]
Department of Computer Science
St. Xavier's College (Autonomous), 30 Park Street
Kolkata, India.

Abstract: Botnets are collection of compromised computers, which are very different from the traditional malwares; and can be controlled by the Botmasters remotely. Black hat hackers use Botnets for various kinds of attacks, ranging from Distributive Denial of Services to identity theft using phishing by sending spam emails all over the internet. These are done mainly to get attention, money, and show off their ego, causing financial loss to the naive users. Botnets are hard to detect since they remain hidden in the system, and only works when are instructed by the Botmaster. Botnets spread very rapidly, taking total control of the computer, without user's consent and knowledge. Botnets are evolving daily. It has become necessary to effectively research in this field to minimize financial loss and use botnet in a good way.

Keywords: Botnets; DDoS attacks; spam e-mail; phishing; financial loss.

I. INTRODUCTION

Botnets are a network of zombies, or compromised **[1]** computers. It is very different from the traditional malwares since, it is remotely controlled by group of attackers known as Bot masters, without the consent of the user. The name was first created when the researchers from the Sans Institute detected crypto-protected code in many windows computers in 1999. They were unaware of the purpose of the code as it was inactive. In 2000, the codes caused Distributive Denial of Service (DDoS) attack, which made eBay, Amazon and other e-commerce site down for a week. The term Botnet was created by joining Bot from "Robot" and Net, which comprised of a network of computers. The robot is the malicious code that is present in the infected or compromised computer. Since the security of the lower layers of the OSI models have been improved significantly, the attackers try to find out the applicative layer easier for intrusion in the system.

Several uses of botnets are causing DoS, and DDoS attacks, phishing, and sending enormous number of spam e-mails. It is also aimed at causing financial loss to an organization or a group of individual by collecting private information such as credit card number, passwords, valuable data, etc. The interesting fact about bots is the owner of the computer doesn't know whether the computer is infected or not since, bots are operated only when it receives orders from the master. The common communication channel for control of bot is Internet Relay Chat (IRC), because of its simplicity and functionality. The bots spread through various ways, they generally spread in the internet by looking for vulnerable and unprotected computers to infect. They send the status of the computer to the bot master on finding one, and stay hidden. The complexity of the robot determines whether the botnet is small or large. A botnet can be comprised of millions of compromised computers. Suppose a computer can upload at the speed of 150 bytes per second, so a network of a million computers can cause a network traffic bandwidth of 0.15 GB which is easy for any small e-commerce site to overload, and hence the server can be down.

This paper investigates the types of botnet, and some of the related works in this field. We focus on the ways by which botnet can be controlled or avoided, the possible communication channel that the botnet uses, and the future scope for the security of the internet.

II. Literature Review

Cybercrime is causing huge problems these days. There has been tremendous amount of research in the past few years to minimize cyber crimes. Network forensics is the science of analyzing network traffic and to use that data for detection and source **[2]** of future attacks. Stankovic **[1]** et al. has lighted upon the various strategies for defenses against modern botnets. There have been extensive study and research in the field of botnet detection and tracking. Kumar et al. **[3]** studied honey pot based detection and tracking of botnets**.** They have automated the tracking system by modifying the honeypots. Since botnets have been extensively used for spamming and phishing, Xu et al**. [4]** have studied on the harvesters collecting e-mail address for spamming. They have revealed social network of spammers by clustering them into behavior. The data needed for their research was collected through project honey pot. They found that the spammers within group exhibit coherent and similar IP addresses.

Kaur et al. **[2]** designed a generic framework for botnet detection, which provides guidelines and set rules for researchers to design their own botnet detection algorithm. Botnet is detected by honey pot based detection and analyzing the network traffic passively. A honeypot is an emulated network environment, which has vulnerabilities; attracts attackers to use those resources and fall into trap. After an attacker attacks the environment, researchers can monitor and log the interactions between botnets and attackers. Those data could be used for further future research. There are mainly three types of honeypots, low interaction honeypots, which collect minimal data and log files of interaction between the bots and the network environment. Production honeypots on the other side helps the organization to check their security issues and vulnerability. Research honeypots are used by the white hat (or the good hackers) to detect the bad guys (or black hat hackers). They have used Nepenthes **[3]**, a low interaction honeypot, which is used for malware collection with set of vulnerabilities. It can inform the system administrator about the intrusion. The system administrator can then take necessary actions after it has been informed, to tighten the security and further detect the source of intrusion. In that study, they enabled the Nepenthes in an enterprise network and made them active all the time. The reason for using honeypots for monitoring is for low interaction (low resource intensive) as well as high interaction (high resource intensive) honeypots, furthermore, honeypots can be configured and installed easily to any system. A honeywall is software used to monitor the activities and purpose of the bots. A collection or network of honeypots is called as honeynet. There are other techniques for monitoring of bots, including Intrusion Detection System (IDS) based detection, Domain Name System (DNS) based detection, and various data mining techniques.

Thakur et al. **[5]** proposed a novel approach to combat and detect bots. They have standalone algorithm and a network algorithm. The former runs independently on each node, whereas, the later analyses the conversations, to and from the network using transport layer records. The standalone algorithm analyses the processes in the node and tries to find out suspicious process by looking into the response time and output to input traffic ratio. If such a process has been found, then it triggers the network algorithm. The network algorithm also learns about the bot pattern and bot signature which can subsequently be used by the standalone algorithm to prevent bot processes and thus saving the system.

There are also studies which promote the development of botnets, one of them include OnionBot (**Fig. 1**). OnionBots subvert privacy infrastructure and cryptographic mechanisms. The tor project was successful in hiding user's identity and allowed to host services without revealing the location or identity of user in the internet. There has been tremendous improvement in crypto currency such as Etherium, Bitcoin, which are used for transactions in the underworld. Silk road, Zeus botnet, and the hosting of the Crypto locker ransomware using command and control centre and asking for money has emerged on the fact that privacy and cryptography would be the next tool to support botnets. The OnionBots carries traffic does not leak details of its destination, source or code. The communication in this first generation of non-trivial OnionBots is carried out through hidden services. No bots not even the Command and Control shows the IP addresses of the other bots. At a given time, a given bot is aware of the temporary address of a subset of bots.

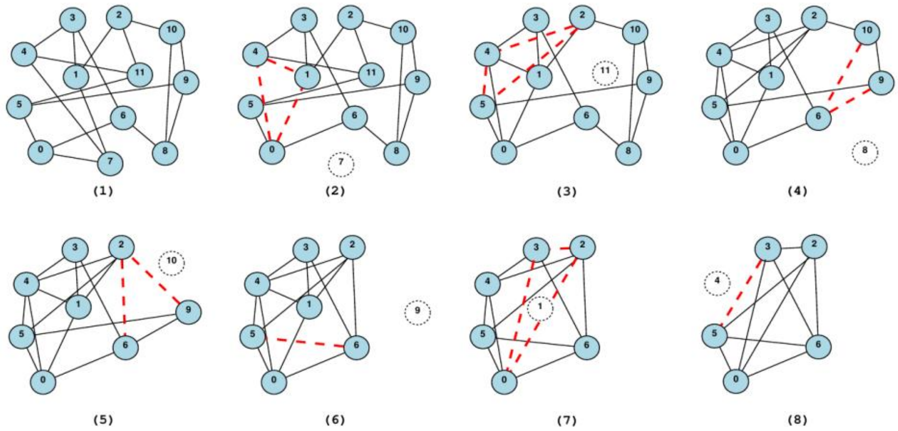


Fig. 1: A structure of Onion Bot, repairing itself. Picture Courtesy: Guevara Noubir.

There are various other ways to prevent bot from entering the computer. When a user suspects that their computer might have been infected, it is a good idea to permanently update the Operating system of the machine. Another way of avoiding bot is to check the address of the sender before downloading attachments in e-mail. Also, it is advisable to scan .vb, .js, .bat, .exe, .bin, .com, files using top rated protection software before its opening. To limit the user's right, and turning off the support for scripting languages in the browser can also protect against botnet, resulting in demotion of user experience.

Apart from these the system administrators can detect the activities of Botnet. They can monitor log files periodically. The study of IDS log files, Mail servers, IRC servers, Proxy servers, DHCP servers, etc. can show whether a bot is present in the machine. If there is change in traffic, then it is necessary to use appropriate tools for eliminating that subnet of computers. Sudden spike in network traffic also shows there might be presence of bot in the network.

Intrusion Prevention System (IPS) stays behind the firewall as shown in **Fig. 2**. It provides additional layer of analysis. It can monitor the network and detect anomalies in the network for alarming the system administrators. It can send an alarm to the administrator, can drop malicious packets, can reset the connection and block the traffic from the source address. This helps to avoid [**6**] degradation of network performance. Although it is similar to firewall, their way of analysing the traffic is different. The contents are differentiated in several ways; content based, rate based, and protocol analysis. The protocol analysis can decode the HTTP or FTP, application layer of the network. Rate based once are used to prevent DDoS attacks. They learn the normal behaviour of the traffic and compare with stored statistics. It can detect abnormal rates of certain type of traffic, such as UDP, TCP, or ARP. The attacks can be identified on exceeding thresholds. The use of Transport Layer Security (TLS), Secure Sockets Layer (SSL) provides encrypted and protected communication between the user and server. It helps to eliminate botnet sniffing of the traffic and results in reduced chances of information getting compromised. Updating the correct patches can also minimize the botnet attacks.

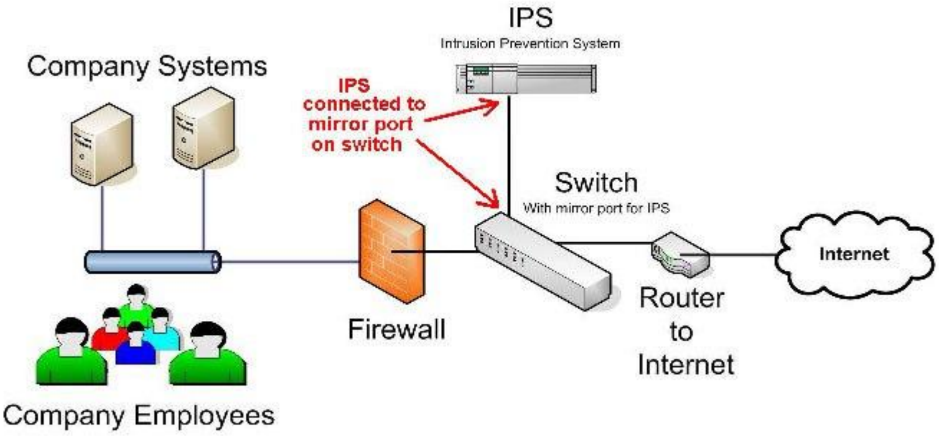


Fig. 2: The figure of an Intrusion Prevention System (IPS). Picture Courtesy: Balaji.

Sagirlar et al. **[7]** studied AutoBot catcher, which can dynamically analyse network of IoT devices, and detect the botnets. It exploits a Byzantine Fault Tolerance (BFT) blockchain. It helps to perform collaborative and dynamic botnet detection by analyzing the network traffic flows.

III. Materials and Methods

The motive of the authors is to study the communication protocols used by the Botnets. The computer is first infected by a worm or virus. Then the virus opens a TCP communication port. A Trojan program is then inserted into the computer without the consent of the user. This Trojan then hides in the user's computer and operates on receiving instructions from the Bot master. It may be used to spread in the local network where internet doesn't reach, maybe used to send enormous amount of spam e-mails. It maybe also used to perform DDoS attacks against some website or DNS server.

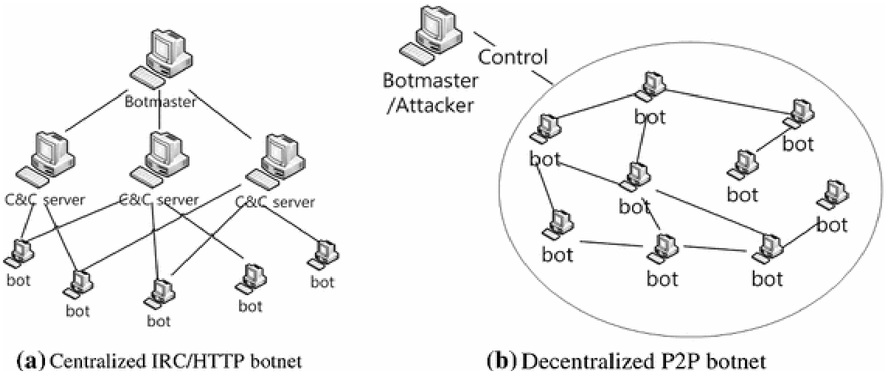
Bots mutually communicate with their owners by means of well defined network protocols. They use already existed Internet Relay Chat (IRC) protocol. Another type of communication protocol is peer-to-peer control, where there is no central controller. When the command regarding attack is sent by the Botmaster to the bots, they perform chain reaction. These botnets are also called as storm, since they carry out chain reaction like a storm. There are two types of communication done by the botmaster and the bots, one of them being pull-based, where bots make periodic queries to the C&C for commands. Another one is push-based, where the botmaster sends the command to the bots.

The most common type of communication protocol is IRC protocol [**8**] for the first generation of Botnets. The only problem with this centralized command centre (**Fig. 3(a)**) was that if it was detected, it could be disabled. This protocol was build to communicate in groups (many-to-many), for discussion in forums or channels; also it supports one to one communication by private messages. This is very useful to the BotMasters and attackers since it is very easy for them to send orders to a group or subset of computers. In most of the cases the bots are connected to the IRC channel which the Botmasters create and wait until instructions are received. Command and Control (C&C) protocol allows bots to receive commands and may even update the bot which makes it more powerful that added much of capabilities. The Central Server or C&C centre should be sufficiently robust to manage millions of bots distributed across the internet. It also has the capabilities to defend against any attempt to shut down the botnet, from the attacker's perspective. The plus point of this model is that it has small message latency. This helps the botmaster to launch attacks quickly. The disadvantage being, it is the critical point of the BotNet. IRC is flexible, easy to set up, use simple commands, have real time anonymous communication and it has low latency communication.

Though it is not mandatory for the Bot to use IRC protocol it can use the compromised server for accessing the web. Some ordinary web server is connected to the bot. Hyper Text Transfer Protocol (HTTP) is one of the most popular modes of communication for a bot and a botmaster in recent times. There are various reasons for using HTTP as a method of communication. Firstly, it can be hidden and encrypted in a better way than rest of the web traffic. Secondly, it is open to all communication channel and servers, so it can easily bypass the security rules. Lastly, it is difficult to detect botnet networks with HTTP protocol. This network interferes with the high capacity of the normal HTTP network traffic. They can easily bypass firewalls. But filters can classify between these kinds of traffic, so filters can be used to differentiate this types of traffic.

There are other types of protocols such as peer to peer (P2P) protocols (**Fig. 3(b)**), IM protocols etc. They generally use crypto implementation of P2P protocol for communication. They exchange private messages and files among a small group of parties. These are the newer generation of Botnets, that doesn't fail when a server is shut down, since there is no central server for command and control. It is much harder to discover and destroy botnets. If a number of bots gets destroyed, this will continue to perform its task well. Since there is no critical point, this is very hard to eliminate. Here a bot acts as both a client and a server. The advantage of this kind of communication is that the new bots knows some temporary address of the other bots. It can continue to operate when it is even offline. In this way the Botmaster can send commands which shall be executed when they come in contact with other bots that are online. The botmaster sends code to any node and is either broadcasted or accessed to certain nodes in the chain.

Some of the famous Botnets are - Agobot, Forbot, Phatbot, XtremBot. They are some of the best known bots, written in C++ programming language. It has root kit protection and more than 500 versions of it are already registered. It is easy to add some more modules to it since it is build and coded in modular way. Agobot uses other protocols along with IRC for communication purpose. Some of the most active group of IRC bots are OrBot, RBot, SDBot; written in C. It is inferior to Agobot. These are the most popular among the attackers, and characteristics are similar to AgoBot. There are also Global Threat (GT) bots, mIRC bots. There are varieties of these kinds of Bots, since mIRC is the IRC client for windows. Data Spy Network X (DSNX) bot is written in C++, and is one of the rare kinds of bots used for DDoS attack. It has got pulgins and it can spread rapidly over the internet. One of the bots for Linux platforms is Q8 bots. It is written in C, and has a dynamic update via HTTP protocol.



(a) Centralized IRC/HTTP botnet (b) Decentralized P2P botnet

Fig. 3: General structure of a Botnet; (a) centralized, and (b) decentralized. Picture Courtesy: Kyungsan Cho.

IV. Results and Discussions

The network of bots continues to threaten companies and individuals **[9]**. The fundamental reasons for setting and building botnets are financial gain. It is also because of the ego, social status, entertainment of the black hat hackers that they invest in such a thing. There has been research on the information about the stakeholders and the system. Putman et al. **[9]** researched on the business model of the botnets and determine the revenue stream of botnet owner. They studied the botnet lifecycle and determined the associated cost. They concluded that for building a cyber-army from scratch is very costly, whereas acquiring and developing previously build bots requires very little expenditure. They found that the total revenue generated is tremendous, compared to the set up cost of the bots. The first stage in **Fig. 4**, is the stage of research and development. The bot is tested and developed by top IT professionals. The patches are included to make the bot powerful to any kind of attacks by the white hat hackers. The bot is then tested and hosted by Pay Per Installation (PPI).

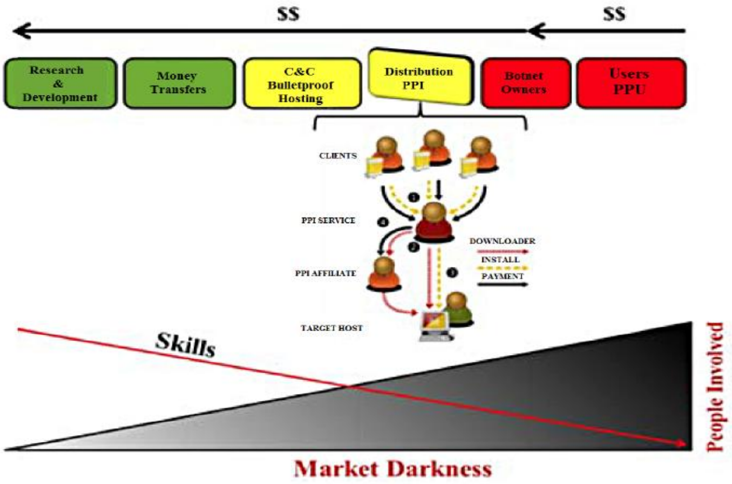


Fig. 4: A business model of a BotNet. Picture Courtesy: Cas G. J. Putman.

We now listed below some of the malicious uses of the botnet by the botmasters:

- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks: They are attacks caused by a network of zombie computers to choke the bandwidth of the target network. They are different from single point of attack since, in distributed system, there are a large number of computers, so it is easy for them to overload the communication channel as a whole. TCP and UDP flood are mostly used in this kind of attacks. This is used to attack almost any kind of web service available on the internet causing loss of service to the user.
- E-mail spamming: Using a large number of bots, the attacker can send enormous amount of spam emails. It is done by some bots which can open sockets v4/v5 proxy and generic proxy for TCP/IP networks. Apart from sending spam e-mails they are used for sending phishing e-mails.
- Botnet Spread: Bots mostly use spam and phishing email to spread themselves suo-motu. It can also take over files by FTP, and can spread through HTTP protocol.
- Traffic Monitoring and key logging: They are used to monitor, sniff network traffic, in order to intercept sensitive information. They can take passwords, usernames and other critical information which can cause a financial loss to the naive users. The bots can also detect other bots in the network by traffic monitoring. Some bots install key logger to the infected computer, they perform in such a way that when some passwords are typed, they store it and then send it to the Bot Master after collecting enormous amount of user sensitive data.
- Identity theft: The bots can spam a user to log into a site, which might seem original using phishing techniques. These can cause them to submit username and password to the false site hosted by the botnet and the user falls in the trap. That information can be sold to third parties who can do social engineering and demand money.
- Pay per click abuse: From the attacker's perspective, this is a good idea. Botnets can be used to automate enormous amount of clicks to a certain website without the user's consent. If the number of bots is relatively high then there will be a huge financial gain for the botmaster.
- Distribution of computation: Web browser has turned into a small but powerful operating system **[10]**. On visiting a website, the browser will run trusted code in which the browser has been given prior permission. The proliferation of recent JavaScript API has not only given user a good experience but also allows attackers to do malicious operations secretly without the user's consent. Papadopoulos et al. **[10]** investigated MarioNet (**Fig. 6** and **Fig. 7**); a framework that allows remote unauthorized access to a browser's computational resources even when the tab or window of the website is closed. There have been a vast number of sites that uses distributive browser's computational power to mine bitcoin and other crypto currencies. They can also use synchronised based password cracking. The MarioNet relies on HTML5 API, and it uses the computational power without using any additional plug-ins or installed software.

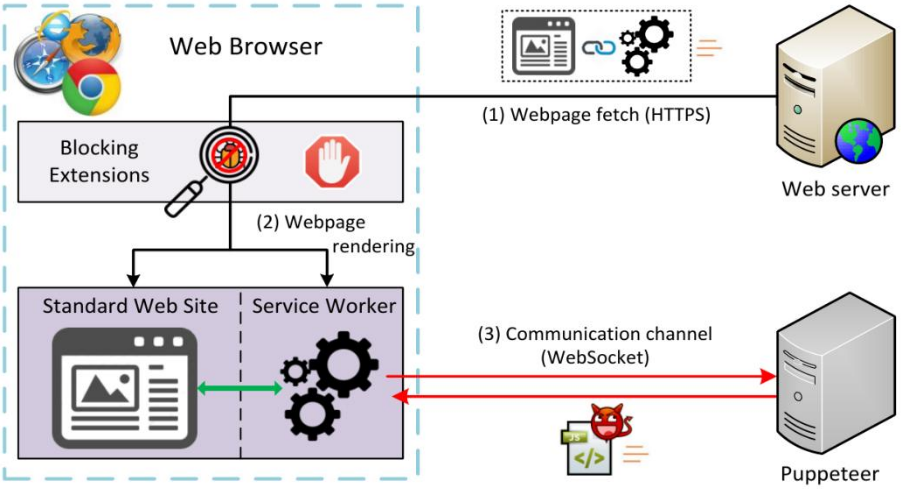


Fig. 6: High level overview of MarioNet. Picture Courtesy: Panagiotis Papadopoulos.

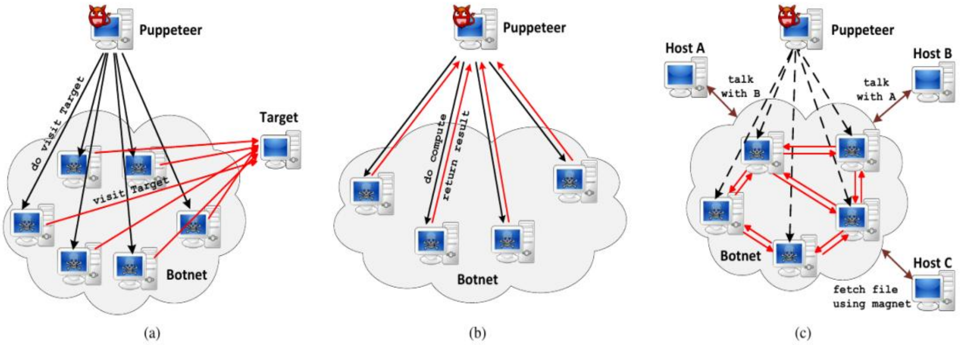


Fig. 7: Different use cases of MarioNet. Picture Courtesy: Panagiotis Papadopoulos.

So we have seen that there have been a large number of reasons that promote the development of botnets. It is necessary to take counter actions to save user's identity, computational resources, privacy etc.

V. Conclusion

In this paper we have investigated the various types of botnets, how it can operate maliciously in a network, and how it is more dangerous, different from the traditional malwares. It's a threat to the cyber space and can operate in different types of communication channels. It can also operate and spread itself suo-motu when offline. We found the reasons and the motivation for creating botnets. The power of distributive computing, the threat it poses to human life, identity, and resources. We have also found that it can cause DDoS attacks, spamming, phishing, and a huge financial loss to the naive users. Analysis shows that if it is used for good reasons it can cause huge financial gain for the BotMasters. There has been constant rise in the size of the network and the crime in the cyber space is rising tremendously. So measures should be taken to promote researches against the spread of BotNets and analysis and prevention of different malwares in the internet.

Acknowledgement

The authors greatly acknowledge the help received from, Dr. Jadab Kumar Pal, Deputy Chief Executive, Indian Statistical Institute, Kolkata for constantly helping and motivating to write this paper. The authors also acknowledge the help received from Cas G. J. Putman **[9]** of University of Twente; Balaji, Editor in Chief of GB Hackers [**11**]; Guevara Noubir of Northeastern university **[12]**; Panagiotis Papadopoulos of Greece, FORTH **[10]**; Kyungsan Cho [**13**] for contributing their pictures in this research. The authors are also grateful to Fr. Dr. Dominic Savio, Principal of St. Xavier's College(Autonomous), Kolkata for his constant encouragement to do research work in the field of Computer Science and Engineering.

References

1. Stankovic, S., & Simic, D. (2009). Defense Strategies Against Modern Botnets. arXiv:0906.3768[cs.CR]. https://arxiv.org/abs/0906.3768 accessed on 23.10.2018.
2. Kaur, S., & Verma, A (2013). Design of Generic Framework for Botnet Detection in Network Forensics. arXiv:1310.0569[cs.CR]. https://arxiv.org/abs/1310.0569 accessed on 23.10.2018.
3. Kumar , S., Sehgal, R., Singh, P., & Chaudhary, A.(2013).Nepenthes Honeypots based Botnet Detection. arXiv:1303.3071[cs.CR]. https://arxiv.org/abs/1303.3071 accessed on 23.10.2018.
4. Xu , S., K., Kliger, M., Chen, Y., Woolf , P. J., Hero III, A. O.(2013). Revealing social networks of spammers through spectral clustering. arXiv:1305.0051[cs.SI]. https://arxiv.org/abs/1305.0051 accessed on 23.10.2018.
5. Thakur, M. R., Khilnani, D. R., Gupta, K., Jain, S., Agarwal , V., Sane, S., Sanyal, S., & Dhekne, P. S. (2013). Detection and prevention of botnets and malware in an enterprise network. arXiv:1312.1629[cs.CR].https://arxiv.org/abs/1312.1629 accessed on 23.10.2018.
6. https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips, accessed on 30.10.2018.
7. Sagirlar, G., Carminati, B., & Ferrari, E. (2018). AutoBotCatcher: Blockchain-based P2P Botnet Detection for the Internet of Things. arXiv:1809.10775[cs.CR]. https://arxiv.org/abs/1809.10775 accessed on 23.10.2018.
8. https://en.wikipedia.org/wiki/Botnet, accessed on 30.10.2018.
9. Putman, C. G. J., Abhishta, Nieuwenhuis, L. J. M. (2018). Business Model of a Botnet. arXiv:1804.10848[cs.CY]. https://arxiv.org/abs/1804.10848 accessed on 23.10.2018.
10. Papadopoulos, P., Ilia, P., Polychronakis, M., Markatos, E. P., Ioannidis, S. & Vasiliadis, G. (2018). Master of Web Puppets: Abusing Web Browsers for Persistent and Stealthy Computation. arXiv:1810.00464[cs.CR]. https://arxiv.org/abs/1810.00464 accessed on 23.10.2018.
11. https://gbhackers.com/intrusion-prevention-systemips-and-its-detailed-funtion-socsiem/, accessed on 30.10.2018.
12. Sanatinia, A., & Noubir, G. (2015). OnionBots: Subverting Privacy Infrastructure for Cyber Attacks. arXiv:1501.03378[cs.CR]. https://arxiv.org/abs/1501.03378 accessed on 23.10.2018.
13. Ye,W., & Cho, K. (2017). Soft Computing 21: 1315. https://doi.org/10.1007/s00500-015-1863-6.

AUTHOR(S) PROFILE

Jimut Bahan Pal is a student of Dept. of Computer Science, St. Xavier’s College (Autonomous), Kolkata-700016. He is fluent in Python programming language, and has invented various scraping programs. He is also a member of various online learning communities like Coursera, Stanford Online, edX etc. Being a Machine Learning enthusiast, he has done various minor projects in Machine Learning area. He has also built various RPG games with Unity-3D, and Unity-2D game engines in association with MOOCs. Being a front end web developer, he has developed the website of Xavotsav 2018. He is an aspiring and curious researcher.

Dr. Asoke Nath, Ph.D., D.Litt., is working as Associate Professor in the Department of Computer Science, St. Xavier’s College (Autonomous), Kolkata. He is actively engaged in research work in the field of Cryptography and Network Security, Steganography, Green Computing, Big data analytics, Data Science, Quantum Computing, Li-Fi Technology, Mathematical modelling of Social Area Networks, MOOCs etc. He has published more than **232** research articles in different National and International Journals apart from conference proceedings.