Journal of Engineering and Applied Sciences 14 (12): 4089-4096, 2019
ISSN: 1816-949X

Survey: Botnet Impact on Cyber Net

[1]Vanakamamidi Rama Krishna and [2]R. Subhashini
[1]Sathyabama Institute of Science and Technology, Department of Computer Science, Chennai, India
[2]Sathyabama Institute of Science and Technology, Department of Computer Science,
Sathyabama University, Chennai, India

Abstract: Bot is a malware installed in a network device. The word bot was derived from 'robot' an automated process used to interact with other services. Botnet is a collection of bots (devises) receiving and responding to commands from bot master. Bot master takes control of bots to perpetrate various activities such as DDoS attacks information theft (username, passwords, financial information), spam camping using emails, acting as other identity and causing network congestion. The attacked network device may not be aware of the bot, bot will be running in the background. Bot will perform the activities instructed by bot master. As per the surveys around 25% of the effected network devices are due to botnet. The attackers are tending towards botnets because it is less expensive and easy to propagate the attack. Symantec botnet intended to advertisement able to create 10,000 bots with just us $15. The intention of this survey is to look at the botnet, architecture and its impact on cyber world. It was getting developed. We want to bring all these details in one study.

Key words: Botnet, botnet architecture, botnet impact, background, advertisement, information

INTRODUCTION

Botnet overview: Bot is a malware program installed in a vulnerable device. A botnet is a collection of compromised devises (bots) receiving and responding to commands from bot master. The attacker (the bot master) takes control of the devises (the bots) to perpetrate various criminal activities such as information and identity theft, denial of service attacks (Paxton *et al*., 2007; Choi *et al*., 2009). Botnet and their impact on cyber networks huge as per surveys in 2017 different origination claims the existence of bots (Fig. 1).

Facebook claims over 1000,000 bots on Messenger Twitter may have 48 million bot accounts, almost 15% of their accounts (Ianelli and Hackworth, 2005) Kik Management team says it has 20,000 bots on its platform. Microsoft Bot Frame claims more than 20,000 bots (Fossi *et al*., 2011).

Cyber criminals finding botnet is the easy way to attack the websites and many services in the internet. Bots are inexpensive and can be easily propagated the average botnet size is now about 20,000 devises. The number of bots is extending in the cyber net rapidly. The large number of botnets present in the cyber world makes attackers attractive (Choi *et al*., 2009). In large scale bot traffic is flowing in the cyber net, over half of the traffic is

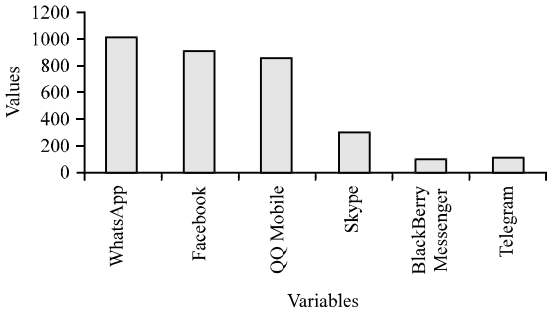

Fig. 1: Bots present in web application; Active bots in application (Bacher *et al*., 2008)

getting originated from bots. It is very important to know about the bots. There are two kinds of bots good bot and bad bot. Bots with malicious intents are classified as bad bots. Botnet initially started for good purpose it was used in Internet Relay Chat (IRC), a text-based chat-system that organizes communication. Bots used to interrupt commands, provide administration support and used to offer services to users. They mainly used to retrieve information like operating system, login details and email related information. Community researchers, law enforcement directives feel botnet is the biggest threat to cyber world (Anonymous, 2010a-d). Attacking behavior of botnet can be classified (Fig. 2).

Corresponding Author: Vanakamamidi Rama Krishna, Sathyabama Institute of Science and Technology,
Department of Computer Science, Chennai, India

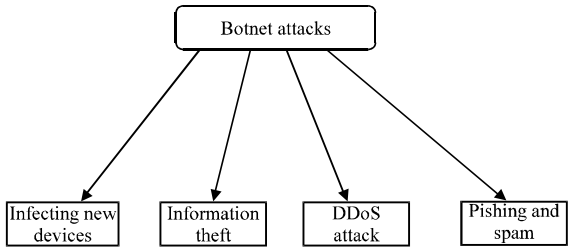

Fig. 2: Classification based on attacking behavior

Infecting new devices: Spreading the malicious information to the multiple devices. Generally, by using emails and through chat bots will spread program to new devises.

Stealing use full information: This kind of bots used to steal interesting information that can help to attack. They also can be used to steal the personal information of the users. These kind of bots identify less secured (or) compromised system and uses tools like key logger, sniffers to spy the user activities in the network. After collecting the information, they can prepare personal statistics of the user. Example:Zyklon.

Distributed Denial of Service (DDoS): DDoS attack is multiple devises targeting server (or) machine with packets. Botnet is most popular way to do this attack. Bots can make multiple instances and can start attack on network (or) server. This will bring down the services and caused network outage. By using botnet both kinds of DDoS attacks like application layer DDoS attack like HTTP floods and network layer attacks like Syn and UDP flood are performed. Example:Leet

Phishing and spam proxy: The botnet owner steals the data and will sell it and can be used for attacks (or) personal gains, this activity comes under Phishing type of attack. For example, bot used can retrieve email addresses in address book (or) can retrieve server ip' ports running in the network. Popular Phishing botnet was Agobot. Spam Proxy uses on demand proxy server by using HTTP, SOCKS protocols passes malicious traffic by using control server ports malicious traffic will be flown. This proxy server will be controlled by bot master. Bot master can aim specified target and can flood with traffic. Necurs is an example of spam proxy.

MATERIALS AND METHODS

Botnets and their effects on cyber world: The first well known bot was developed on IRC named Egg drop in

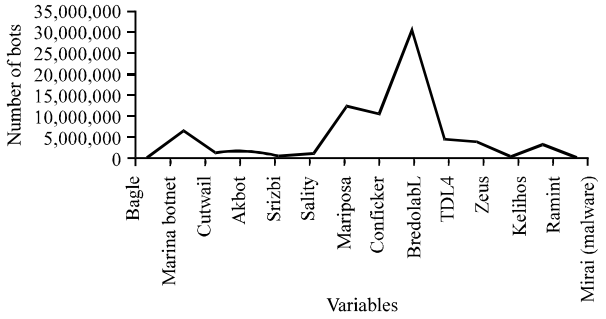

Fig. 3: Number of bots present in cyber world; Estimated No. of bots

1993. Initial days bots were developed to attack other users and IRC server (Markoff, 2009). Later attackers started using bots for DoS then they upgraded them for DDoS. As time and technology grows bots became more complex, bot are injected in to different protocols and day by day they becoming more power full. They can be made as worms, viruses and can do distributed attacks in very large scale (Fig. 3).

Egg drop: This is one of the first popular IRC bot developed in 1993, it was free bot written using C and TCL. This was originally developed to protect channel from takeover attempts. Extra feature can be easily added to this bot and can be extended. This had features of botnet. This botnet supports multiple channel, default channel is called as "party line". This is mainly used for chatting and files sharing.

GT bot: This is mIRCS based bots. mIRC is a popular IRC client for windows. GT means Global Threat. This bots launch mIRC chat-client, set of scripts and binaries. One of the binary HideWindow make the mIRC instance unseen by the user. Other binaries are containing Dynamic Link Libraries (DLLs) will be linked to mIRC. This is Trojan horse type of Bot once installed stealth mIRC, joins IRC network and awaits commands of the bot master. These bots used to launch DDoS attack.

SDBOT: SDBOT uses Internet Relay Chat (IRS), the first occurrence was found in 2004. After that different variants of this botnet is still appearing. Currently most of the IRC botnets are disappearing but SDBOT still exists. This is low profile botnet, it is very difficult to find this botnet. Unlike other botnet this will not interrupt on going activities on user system. Cyber criminals are attracted by download ability of SDBOT. Cyber criminals to install malware will pay to SDBOT group and will pass their malware to thousands of SDBOT installed system.

Agobot: This bot belongs to group of computer worms. This bot was popularly known as Gaobot. This was written using C^{++} and assembly. The bot was developed in modular way it is easy to add new commands to it. Different possible attacks can be performed by this bot are sending large number of un solicited emails using its own SMTP engine. It can open back door for different random TCP port through IRC channel and can terminate different security and monitoring tools and it can perform DDoS attacks.

Spybot: This belongs to computer worm's family. Once, Spybot infected the system joins to IRC server port using preconfigured channel. IRC server will issue commands issued by the remote attacker. The main attack performed by this is scan the host in the network to identify machines to propagate bots. Another action performed by this bot was start and stop of the key logger. It effects mainly Microsoft Windows machines. Spybot search and destroy is famous Microsoft program used to identify and remove the malware from the system.

Sinit: This belongs to P2P botnet family. Sinit bot probes and finds other Sinit bots. As part of it Sinit infected devise will send discovery packets once response received both hosts exchange their list of Sinit devises and they will spread the Trojan through network.

Bagle: Bagle is computer worm type of botnet, it mainly effects Microsoft Windows second variant Bagle B spread faster than Bagle A. Bagle uses its own SMTP engine and sends attachment to recipients gathered from the system. It copies to windows system directory opens backdoor to vulnerable port around 230,000 instances of this bot present in the cyber net.

Marina botnet: it can damage Microsoft computer operating system level programs and files. This will enter to system through infected e-mails. Using this, bot master can control system. It can theft the personal information and can damage the system. This bot will spread to other systems through network devises. In the cyber net around 6,215,000 instances are present.

Sality: Sality is P2P botnet, it effects Microsoft Windows system. This was used to delete certain files, steal personal information. Can generate replay spam through HTTP proxy, password cracking. 1,000,000 variants of this bot are present in the network.

Mariposa botnet: This is one of the largest bots available in the network. It was intended to DDoS attacks and cyber scamming (Anonymous, 2013). As it was grown in bigger size it is very difficult to calculate the effects caused by this bot. As part of this t personal information was theft and was sold.

Conficker: Conficker is warm effecting Microsoft Windows. This Bot spread in large span it was having 12,000,000 instances in the cyber world. It used operating system flaws and done dictionary attack. Around 190 countries are affected by this bot (Zhu *et al*., 2008). This botnet executed different vulnerable things like disable functionality of Microsoft Windows, resetting account locking policies, locking user accounts, making antivirus and security servers as inaccessible.

Bredolab: It is also called as Oficla, it was Trojan horse mainly focused on e-mail spam. It was spread in millions of devises (Feily *et al*., 2009). Bredolab will send mail with malware attachment when the attachment opened in a system it will affect other system and the new system will become part of botnet. This botnet has capability of sending 3.6 billion viral mails each day. These bot owners leased the affected system to others and from that they earned money.

Zeus: It is also known as boot it is Trojan horse will effect windows machines. This is mainly used to steal the information by using keystroke. It can also have downloaded crypto locker to do ransomware (Ullah *et al*., 2013). It effected big institutes like Bank of America Amazon, Cisco. This bot is very sophisticated up to date antivirus also not able to detect this. It was spread in large scale 3,600,000 systems are affected by this.

Mirai: Mirai is malware effects Linux running machine. Bot master can control the malware system. This was targeted IoT devises. This was targeted on network devises home (IP camera) routes and can do DDoS attacks on network. In 2016 Dyn attack was performed by this. Attackers published the source code of the bot that opened gates for cyber criminals to enhance their attacks.

Botnet based on protocol: Botnets up to now mainly using protocols IRC, P2P, HTTP, DNS. Centralized botnets generally uses IRC. Lot of bots got in activated after shutting down the bot master recent times attackers turned towards P2P (Peer to Peer) architecture. Botnet initially started with IRC protocol (Ramachandran *et al*., 2006). In 2003 onwards botnet took new turn using P2P. The P2P architecture has removed the need of centralized C&C server. The year 2006 onwards bot started using

Table 1: Botnet across the protocols

Botnet/Years	Protocol
Eggdrop (1993)	IRC
Gtbot (1998)	IRC
Sdbot (2002)	IRC
Spybot	IRC
Sinit (2003)	P2P
Phatbot (2004)	P2P
Spamthru (2006)	P2P
RxBot	IRC
Rustock	HTTP
Peacomm (2007)	P2P
Zbot	HTTP
Asprox (2008)	HTTP
Bobax	UDP
Donbot (2009)	TCP
Festo (2010)	HTTP
TDL-4 (2011)	P2P
Chameleon botnet (2012)	Hybrid (mimicking human behavior)
Mirai (2016)	Hybrid (IOT)

most widely used HTTP protocols, after using HTTP the size of the bots increased drastically. Attackers started using network protocols TCP/UDP spams were spread in the network rapidly currently attacker coming with Bots like Mirai which can operate on IOT devises (Table 1).

Life cycle of botnet: As part of first phase bot master develops client and server application. Bot master propagate the developed client application, potential bot through different means. Bot master propagate them through famous attractive advertisements which will cause download of the malware, propagates through mail attachments, spreading through infected plug in devises like disks. In second stage installed program in the malicious devise will intimate to the bot master about its presence. Then bot master will give binaries to be executed, so that, it will become bot. In this phase, bot master relay on protocols like FTP, HTTP, P2P to download binaries (Liao and Chang, 2010). Once, Bot is installed it will start communicating With bot master and will execute the commands received. Based on the commands from Bot master Bot can change the attacking pattern. When attacking pattern was identified botmaster will change the pattern, so that, it can escape from detection systems. If bot master want to signoff from the activity, it can send removal command, so that, bot will destroy its binaries from the malicious devises (Fig. 4).

Botnet architecture: Botnet architecture can be in four types:

- Centralized botnet architecture
- Peer to Peer botnet architecture (P2P)
- Hybrid botnet architecture
- HTTP and P2P botnet architecture

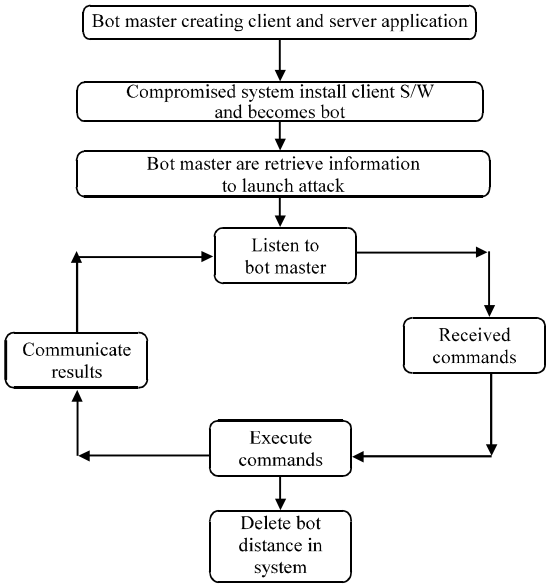

Fig. 4: Life cycle of botnet

Centralized botnet architecture: This is the first botnet architecture. Bot master will control all the bot through centralized server C&C (Command and Control) server. C&C uses IRC (or) HTTP all the bots came in initial days Eggbot, SDBot, GTBot, SpyBot used this architecture. Initial days C&C server was single later multiple C&C servers used to propagate the bot. The main advantages of this are easy monitoring. It is quick and easy to change botnet pattern across the bots. Bot master can select group and launch an attack can be traced The main disadvantage is if C&C server made down entire bot will be in active. By tracking the commands send by C&C server botnet activities can be identified. By using Honey pot bot master can be traced and bring down the attack.

Peer to Peer botnet architecture (P2P): Defense system is able to crack the attacks coming from centralized bot architecture quite easily. Attackers moved to P2P architecture. In this approach, single point of focus (or) failure removed. After P2P it becomes hard to monitor and detect the botnet. In P2P architecture bot master injects bot in to devise this devise (first bot) transfer to peer systems. In this architecture, each node acts as server and client. This architecture works in two phases first identifying bot second spreading bot in to that devises. Sinit, Phatbot, Spamthru are the initial bots developed using P2P. With this architecture even few bot devises were identified it is difficult to remove the complete botnet from the network. In P2P architecture, attackers started using encryption to fly out of intrusion system. P2P

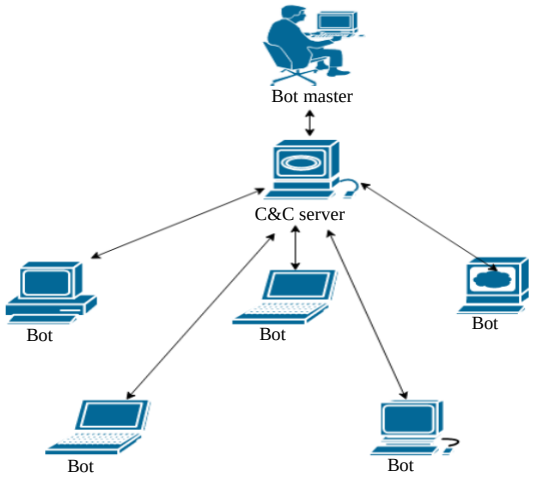

Fig. 5: C&C architecture

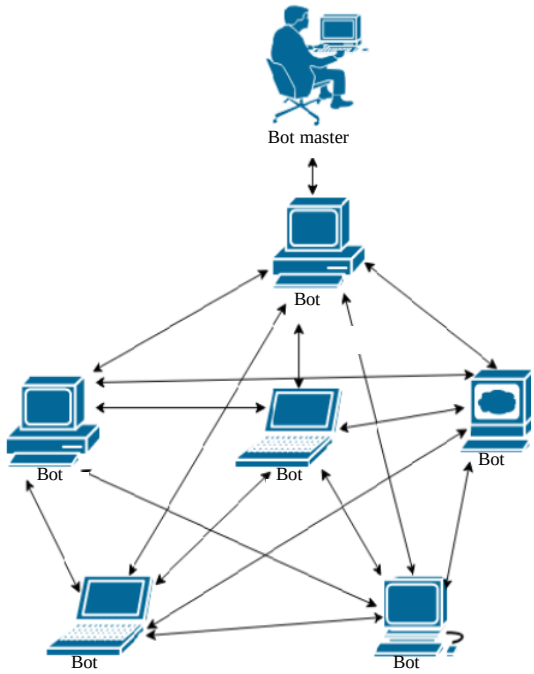

Fig. 6: P2P architecture

botnet also has its own set of weakness. This architecture involves lot of probing and generates lot of traffic. Defenders can detect bot by using network flow. Data mining techniques and algorithms are giving better results (Williams, 2009) (Fig. 5 and 6).

Hybrid botnet architecture: This is mixture of C&C and P2P architecture. Bots are divided in to two groups servant bots, client bots. Servant bots can act as server and client. Servant bots maintain their own peer list and will not share this list to other elements. Generally, server

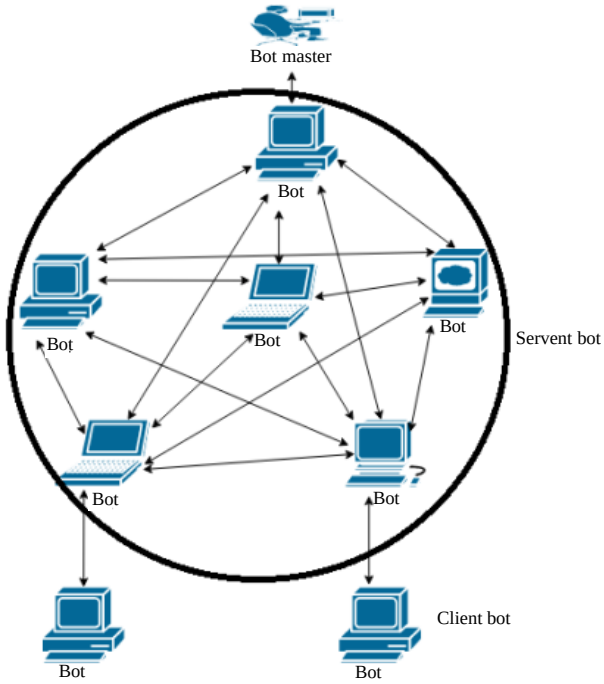

Fig. 7: Hybrid architecture

bot will have global ip and client bot will have private ip address. Periodically servant bot and client bot will communicate with each other based on peer list to retrieve commands issues by bot master. The new commands will be shared to servant bots in its peer list. Hybrid P2P is extension of development of C&C botnet architecture. The bots in servant bot acts as servers as they are large in numbers and periodically connecting with each other and updating it is very difficult to completely shut down (Fig. 7).

Hypertext Transfer Protocol Peer to Peer (HTTP2P): This architecture was mainly developed to divert firewall and intrusion detection systems. To overcome centralized approach P2P approach was developed but P2P network has threat of Sybil attacks (Labovitz, 2010). To overcome that drawback of P2P network attackers working on this approach. In this architecture, they combined HTTP and P2P protocols. Bot master search for client bot and that message will be ciphered. Once, bot was found commands will be issued.

Botnet topology: Based on existing architecture botnet can have four type of topology: start topology, multiple server topology, hierarchical topology, random topology (Anonymous, 2010a-d).

Star topology: One centralized C&C server sends commands to all the bots. C&C will issue command to

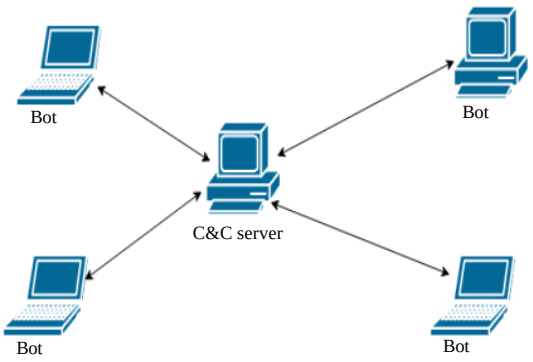

Fig. 8: Star topology

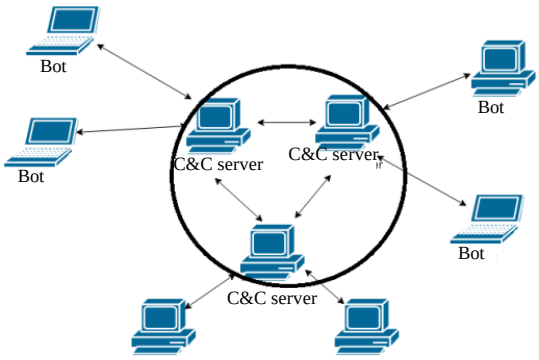

Fig. 9: Multiple server topology

each bot directly. Disadvantage is single point of failure if C&C server was identified bot can be shut down. Advantage is C&C can issue commands directly propagation will be very fast. On demand the attacking pattern can be changed very quickly (Fig. 8).

Multiple server topologies: This is extension of star topology. Here, C&C server load is shared by multiple servers. Multiple servers will communicate with each other on the commands need to be given to the bot. Even one C&C server was brought down also still bot can be operated. Using this topology botnet can be spread across different geo graphical location. Multiple C&C servers are maintained for load balance and redundancy. It overcomes the single point failure of start topology by using this botnet can be spread across large area. The disadvantage is it needs lot of additional effort to create and maintain (Fig. 9).

Hierarchical topology: Botnet maintains proxy C&C servers. It can be spread geographically. Bot master will issue the command to the proxy servers. Proxy servers will issue commands to the bots. In hierarchical topology multiple C&C servers are maintained as multiple groups. They will be assigned with different tasks. This can be

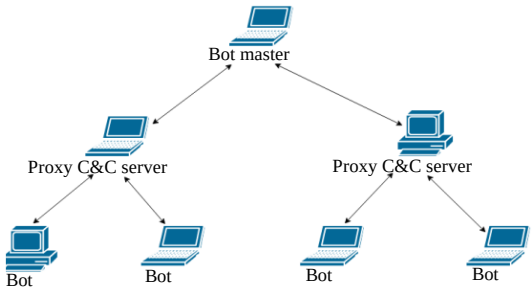

Fig. 10: Hierarchical topology

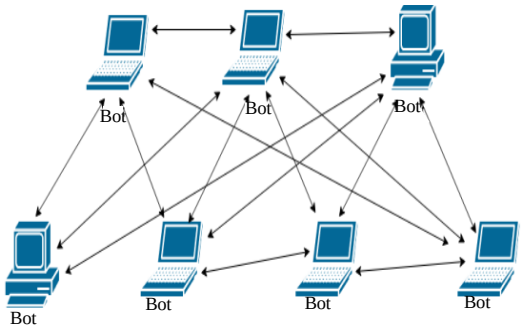

Fig. 11: Random topology

used in complex bot attacks. This topology provides more reliability. The disadvantage is C&C server is not communicating directly with bots there will be latency in the commands propagation.

Random topology: In this topology, there won't be any C&C server. Bot master can inject commands through any bot agent. This architecture is highly resilient, it is very difficult shutdown this kind of botnet. Bots will communicate with peers and can use encryption also in their communication. Defenders by using honey pot can retrieve the attacking pattern. In this topology, latency will be observed in the bot commands propagation (Fig. 10 and 11).

RESULTS AND DISCUSSION

Botnet impact on cyber net

Political motivated: Mark Russinovich wrote novel, theme of the novel is by using cyber-attacks criminals will bring down the national infrastructure. It is becoming reality now, cyber-attack are used to attack countries for political gain. These are incident recorded in recent past.

In 2007, attacks on Estonian: Cyber-attacks targeted lot of government websites Estonian websites including their Parliament, Minsters websites, newspapers and broadcaster's websites. After this attacks NATO

enhanced their cyber defense system. It established center in Tallinn. After this, only European Union called cyber-attacks as criminal offense.

In 2008, attack on Georgia: Georgia country was severally affected by botnet attacks. Georgian President website was hacked and made down for 24 h. DDoS attack started on Augon news agencies, radio stations. Most of the internet traffic generated from Georgia was blocked (or) diverted.

In 2009, attack on South Korea: By using botnet large number of computers in South Korea were undertaken and they performed DDoS attack as per Korean government 20,000 computers were hijacked to do this activity (Williams, 2009). This attack was targeted official government, media and financial sites in South Korea and America. During July time frame the servers were attacked with huge influx traffic and services were brought down. They targeted in three phases. First attack happened on July 4th 2009 South Korean and United States websites that includes white house and the Pentagon sites were attacked. Second attack happened on July 7th 2009, South Korean highly secured web sites like National Assembly, Ministry of Defense and National Intelligence were attacked on July 9th third attack happened on South Korean banking and National intelligence service.

In 2010 attack on Myanmar: DDOS attack happened on 2010 ahead of Myanmar elections. Attacks happened on larger scale. Attackers taken can control of large number of devises in the country from October-November almost every day they attacked, the attack also happened more time every day around 8 h. The size of attack grown up to 15 Gbps. It brought down the internet service in the country (Labovitz, 2010).

In 2011 attack on Malaysia: Large number of Malaysian websites were attacked around 51 sites were hacked and 41 website services were disrupted. Mainly, Malaysian government sites were attacked.

Financial motivated: Zesus, SpyEye are examples of financially motivated botnets. By using these botsattacker's steals banking information. Attackers uses keylogging, screen scraping, browser protected storage. According to Trusteer, (security company) 44% of banking malware were created by Zesus. In many banking accounts amount were transferred without their knowledge. Little and King LLC lost $164,000 by Zeus infected computer.

Table 2: Zeus infected machines across countries

Country name	Machines infected (%)
Egypt	19
Mexican	15
Saudi Arabia	13
Turkey	12
United States	11

By using Zeus attackers in Ukrine stolen $415,000. As per reports $100 million us dollars were lost because of Zesus the US-based corporate security company NetWitness reported the detection of Zeus-infected computers in 2,500 organizations in 196 countries worldwide. A total of 76,000 infected computers were detected. NetWitness reported Zeus-infected in 76,000 computers, around 2,500 organizations worldwide. It impacted 196 countries (Anonymous, 2010a-d) (Table 2).

South Korean gambling site attack: DDOS attack was done on Gambling sites rapidly in 2011. By using botnet attack competitors gambling sites were made down. The genuine login users were refused to access the site and were diverted to other gambling sites. The targeted websites lost lot of money, their revenue was affected. DdoS attack happened on famous financial sites like Pay Pal, MasterCard Amazon, Visa and Swiss Bank.

Personally motivated: Botnets are used to theft personal information. Cyber criminals will send phishing mail (or) fraud link. Users information like phone number, email address, password, credit card details. Different botnet attackers started sharing the information they are able to form more complete digital profile information. After getting the digital identity they can perform all illegal activities without any difficulty. Bots like Waledac and Core flood used to steal the personal information.

CONCLUSION

As part of the survey we tried to bring all bot related information bot net architecture, topology, different type of bots and their impact on the cyber world. Coming days, we are planning to bring up study on different prevention and detection methods.

ACKNOWLEDGEMENT

Botnet impact on Cyber net submitted by research student Rama Krishna V was the work done by him under my guidance in Satyabhama Institute of Science and Technology.

REFERENCES

Anonymous, 2010a. Mariposa botnet-12.7 million bots strong-knocked offline. TechHerald.in, Mumbai, India.

Anonymous, 2010b. War in the fifth domain: Are the mouse and keyboard the new weapons of conflict. The Economist, Westminster, London, UK. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

Anonymous, 2010c. War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?. The Economist, Westminster, London, UK.

Anonymous, 2010d. Zeus malware: Threat banking industry Unisys Stealth Solution Team. Unisys, Blue Bell, Pennsylvania, USA. https://botnetlegalnotice.com/citadel/files/Guerrino_Decl_Ex1.pdf

Anonymous, 2013. CryptoLocker ransomware information guide and FAQ. Bleeping Computer® LLC, Melville, New York. https://www.bleepingcomputer.com/virus-removal/cryptolocker-ransomware-information

Bacher, P., T. Holz, M. Kotter and G. Wicherski, 2008. Know your enemy: Tracking botnets. Master Thesis, Honeynet Project, Menlo Park, California.

Choi, H., H. Lee and H. Kim, 2009. BotGAD: Detecting botnets by capturing group activities in network traffic. Proceedings of the 4th International ICST Conference on COMmunication System SoftWAre and MiddlewaRE (COMSWARE '09), June 16-19, 2009, ACM, Dublin, Ireland, ISBN:978-1-60558-353-2, pp: 21-28.

Feily, M., A. Shahrestani and S. Ramadass, 2009. A survey of botnet and botnet detection. Proceedings of the 3rd International Conference on Emerging Security Information, Systems and Technologies, June 18-23, 2009, Glyfada, Athens, Greece, pp:268-273.

Fossi, M., G. Egan, K. Haley, E. Johnson and T. Mack *et al*., 2011. Symantec internet security threat report trends for 2010. Symantec Internet Secur. Threat Rep., 16: 1-20.

Ianelli, N. and A. Hackworth, 2005. Botnets as a vehicle for online Crime. Master Thesis, CERT Coordination Center, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA.

Labovitz, C., 2010. Attack severs Burma internet. Arbor Networks, Westford, Massachusetts, USA. https://asert.arbornetworks.com/attac-severs-myanmar-internet/

Liao, W.H. and C.C. Chang, 2010. Peer to peer botnet detection using data mining scheme. Proceedings of the International Conference on Internet Technology and Applications, August 20-22, 2010, Wuhan, China, pp: 1-4.

Markoff, J., 2009. Worm infects millions of computers worldwide. The New York Times, New York, USA. https://www.nytimes.com/2009/01/23/technology/internet/23worm.html

Paxton, N., G.J. Ahn and B. Chu, 2007. Towards practical framework for collecting and analyzing network-centric attacks. Proceedings of the 2007 IEEE International Conference on Information Reuse and Integration, August 13-15, 2007, IEEE, Las Vegas, Illinois, pp: 73-78.

Ramachandran, A., N. Feamster and D. Dagon, 2006. Revealing botnet membership using DNSBL counter-intelligence. Proceedings of the 2nd Conference on Steps to Reducing Unwanted Traffic on the Internet, July 7, 2006, San Jose, CA., USA., pp: 1-6.

Ullah, I., N. Khan and H.A. Aboalsamh, 2013. Survey on botnet: Its architecture, detection, prevention and mitigation. Proceedings of the 2013 IEEE 10th International Conference on Networking, Sensing and Control (ICNSC), April 10-12, 2013, IEEE, Evry, France, ISBN:978-1-4673-5198-0, pp: 660-665.

Williams, M., 2009. UK, not North Korea, source of DDOS attacks, researcher says. IDG Communications, Framingham, Massachusetts. https://www.pcworld.com/article/168353/article.html

Zhu, Z., G. Lu, Y. Chen, Z.J. Fu, P. Roberts and K. Han, 2008. Botnet research survey. Proceedings of the 32nd Annual IEEE International on Computer Software and Applications, 28 July-August 1, 2008, Turku, pp: 967-972.