Botnet: Assessment of Threat Vectors and Mitigation

Dr. Shruti Mantri
Dept of Information Technology
Kirti M. Doongursee College, Mumbai

Abstract- *Botnets become widespread in wired and wireless networks, whereas the relevant research is still in the initial stage. In the recent years IOT as well as intelligent devices are infected and attacked by botnets. In this paper, the researcher analyses, classifies the bots and provides counter measures to control botnets. The researcher first discusses fundamental concepts of botnets, including formation and exploitation, lifecycle, and major kinds of topologies. Several related attacks, detection, tracing, and countermeasures, are then introduced, followed by possible future challenges.*

Keywords- Botnets, threat vectors, malware, DDOS, botnet detection, cyber security

I. INTRODUCTION

Successful attack on IOT device, with an installed base of hundreds of millions could causehavoc than one device at a key point in a critical infrastructure control system(Macfree Labs 2016 ,Zhao *et al.*, 2012)(Bu *et al.*, 2010). The device could be a desktop computer, laptop, webcam, modem, or a Wi-Fi router etc.(Bu *et al.*, 2010).Attackers these days make use of untraceable feature of coordinated attacks to compromise a system or network. Group of hostssystems at different locations around the world are governed by a malicious code to initiate attack; it is very difficult to trace back the origin of the attack due to the complexity of the internet. Due to this,events of information leakage, click fraud, denial of service, ransom-ware, mobile device hacking, email spam etc. are serious problems these days. This paper discusses about bots, its evolution, life-cycle, command and control models; different types of bots, botnet attacks, botnet detection techniques and mitigation mechanism.

1.1 Botnet and Life-Cycle of Botnet

The internet bots are programs, designed to be self-propagating malicious programs that spread to form a network of bots called as botnet. Under a command and control infrastructure bots are able to form self-propagating, self-organizing, and autonomous framework named botnets. The botnet master then remotely controls the bots to execute attack. Botnet gains control of the system through a malicious code. Once they get access they turn the computers into zombies to execute denial of service attack against ecommerce sites, spread worm, virus, Trojan horse, generate spam, phishing email, distribute pirated media, and other types of online frauds.The controlled systems are called as zombies or bots derived from the word robot.

To understand the life cycle of bot let's consider the example of spamming botnet:(i) The attacker sends outs malicious codes to infect victim's machines whose payloads are bots (ii) the bots on the infected hosts log onto an IRS server or other communications medium forming a botnet architecture (iii) spammer makes a payment to the owner of the botnet to gain access right (iv) the spammer then sends commands to the botnet master to order bots to sends out spams (v) the infected hosts sends spam messages to various mail servers in the cyber space to execute attack(Xiao *et al.*, 2009).

Once the system is infected with zombie, it downloads the rest of bot code from the server and installs it dynamically. The malicious code (bot program) searches for the internet relay chat(IRS) servers(Ajmera and Gautam, 2014). The IRC servers is also called command and control (C&C) server. Once the C&C server's address is known, the bot then logs into it as authenticated user. Bot also updates its code if an update is available(Ajmera and Gautam, 2014).

1.2 Classification of Botnets

In the current study, Botnet are differentiated based on the architecture and protocol(Ajmera and Gautam, 2014). Based on the architecture botnet can be classified into four types: (i) Centralized botnets; (ii) Decentralized botnets; (iii) Hybrid model C & C; (iv) Random modelC &C.

(i) Centralized botnets

In a centralized botnet, all devicesand systems are connected only to C&C. The center is on lookout for the new botnets to connect. Once the new bot connects to the server, their information is stored in database, to monitorthem and send commands for execution. The zombie computers in the network are visible to the control center. The zombie owner accesses the C&C to manage the centralized botnet(Ajmera and Gautam, 2014).

(ii) Decentralized botnets

In this types, bots connect to several infected machines in the network and not to a C&C. Bots receive commands from neighboring bots in network to be executed. In a decentralized architecture, the attackers needs to get access to one system infected by zombie to activate it. The activated system in turn activates its neighbors and the chain continues. The decentralized bots are based on P2P protocol and work as overlay network: (i) unstructured P2P overlay (ii) structured P2P overlay and (iii) superpeer overlays

(iii) Hybrid model C & C

According to (Silva *et al.*, 2013), hybrid bots is a combination of centralized and decentralized bots. They are categorized into two parts: (i) servants bots and (ii) client bots. Servant bots act as both clients and servers, configured with static and routable IP. Client bots are configured with dynamically non-routable IP. As per (Silva *et al.*, 2013), servant bots have their IP address on peer lists and keep listening to incoming connection.They also use a symmetric key for communication(Silva *et al.*, 2013).

(iv) Random model C & C

According to (Silva *et al.*, 2013), this mode was developed by (*Cooke et al.*, 2005) and bot does not contact the botmaster or other bots, but waits for connection request from botmaster. To execute an attack, the master scans the network to locate zombies, and once found it commands the zombie.
Botnets can also be classified based on network protocols into three categories:(i) internet relay chat (IRC) bot; (ii) instant messaging bot (iii) web-oriented bot(Xiao *et al.*, 2009). IRC servers are interconnected and pass message from one to another. Thus is it possible to connect 100 of clients via multiple servers. The attacker uses control channel of IRC to infect multiple systems with bots. The attacker also attempts to secure the control channel for bots business. Instant Messaging (IM) bots use communication channel provided by IM services.Web-oriented botsconnects to a predefined web server, receives commands from it and transfers data as response.

1.2.1 Evolution and types of Bots

Bots originated from IRC; First bot was developed in 1988 by Jarkko Oikarinen. Eggdropcreated by Jeff fisher was first published in 1983 and developed further thereafter(Tyagi and Aghila, 2011). The later malicious botdeveloped were used for the attacking IRC users or servers. Denial of service (DOS) and then distributed denial of service (DDOS) attacks were designed and developed using bots.Different types of bots have been developed that involves complex mechanisms for communication with the bot master and exploitprotocols. The different types of bots are:

(i) **Ago-bot:** This bot was coded using C++ programing language. It uses control protocol in IRC channel and has special IRC commands for gathering sensitive information. It has(Hua and Sakurai, 2013)(Xiao *et al.*, 2009): (i) IRC-based C2 framework (ii) it launches DOS and DDOS attacks (iii) attack a large number of targets (iv) limits polymorphic obfuscations (v) capture sensitive information via traffic sniffing (vi) capture key logging (vii) can avoid detected by antivirus software and (viii) can detect debuggers and virtual machines; features(Xiao *et al.*, 2009)

(ii) **SDBot:**It has no propagation capability and hasbasic functions of host control**.** It has its own IRC functions(Xiao *et al.*, 2009). To contact the server, SDBot identities itself with the server, once itis identified and authenticated it receives message from the server, the bot acknowledges the response with a connection. Once connected it can be controlled by the master to execute an action. Using NetBIOS scanner, SDBot scans for target for spreading. It is commonly used for flooding and DDOS attacks.(Xiao *et al.*, 2009)

(iii) **SpyBot:** SpyBot is an enhanced version of SDBot and consists of both command language implementation, scanning capability and host control. It is also commonly used for flooding and DDOS attack.

(iv) **GTBot:** GT (Global Threat) bot, is also known as Aristotles and hasdifferent variants. It is widely used for windows operating systems and is build up with IRC host control, DOS attacks, port scanning, and NetBIOS/RPC exploiting capabilities. It also records the responses to commands received from remote hosts(Xiao *et al.*, 2009).

II. BOTNET ATTACKS

According to (Wilson, 2008) botnet designers make large sums of money by marketing or selling their bots. According to CRS report for congress, 2008 (Wilson, 2008), Jeanson Ancheta, a 21 year old hacker made more than $100000 from different internet advertising companies. These companies paid him to get access to bot code on more than

400000 thousands vulnerable host. He also made money by renting his botnet network. In 2007, government computer systems in Estonia were attacked by DDOSattack to mark protest against officials in Estonia against moving Soviet era war memorial memorializing an unknown Russian who died fighting the Nazis(Wilson, 2008). According to Shadowserver Foundation, from November 2006 to May 2007, approximately 1,400 command and control servers were found to be active on the internet.According to Symantec, since 2006 to 2017, there have been many sophisticated complex attacks being carried out that have rocked the internet. During the period 2007-2008, Storm (2007); Mariposa (2008); Kraken(2008); Conficker(2008-2009); Cutwail(2007-2010); Grum(2008) botnets were released. Storm was first detected in the network in January 2007 and possessed strong email subject (social-engineering).The code was designed to targetMicrosoft Windows operating system. Once activated the bot gathered data, attacked web sites, fabricated as genuine user and sent emails. Approximately 6,000 systems in the network wereused to spread the bot code;Storm sent a record breaking 57 million messages.The server systems that controlled the botnet re-encoded their infection software twice an hour to identify new hosts in the network. Hence it was difficult for anti-virus to detect the botnet. The location of the remote servers was kept concealedby changing DNS technique called 'fast flux'. This made identification of virus hosting sites difficult to counter or block them. In short, the name and location of such machines are frequently changed and rotated, often on a minute by minute basis. Mariposa released in 2008; was involved in cyber-scamming and denial of service attacks. The Kraken botnet was one of the largest botnet of April 2008. It targeted machines of fortune companies.The Grum botnet released in 2008-2012, was involved in sending pharmaceutical spam e-mails. The zero access botnet released in 2011, spread upto 9 million systems. Once the system got infected with botnet toolkit, it would start with (i) bitcoin mining and (ii) click fraud. The machines involved in bitcoin produced money worth 2.7 million US dollars as in September 2012. As per (Bilodeau *et al.*, 2014)Windigo botnet was released in 2011 and infected systems majorly in US, UK, and Europe. It compromised Linux operating systems. The main components of the Windigo operation were: (i) OpenSSH backdoor (ii) web redirection module and (iii) spam-sending program(Bilodeau *et al.*, 2014).

Banking botnets were released in 2013 targeted financial institutes; banking websites; business finances and payroll services, stock market websites, social networking, job portals, entertainmentand dating portals etc. It targeted financial organizationsin United States. Mirai botnet, released in 2016 carried out DDOS attack that disrupted internet and server of DYN; brought down websites of Twitter, Guardian, Netflix, Reddit, CNN etc. in Europe and US.Mobile based botnet attacks are also increasing day to day and smartphones users are unaware about the devices being affected by botnets(Tidke and Karde, 2015). The world first mobile worm "Cabir" appeared in 2004. Cabir infected Nokia Series 60 mobile devices. Fortinet was discovered in 2009. Plankton discovered in 2011, is anAndroid malware. 'Android.hehe' released in 2014 has the ability to steal text messages and intercept phone calls. According to Jacob Aron and Munish Sharma, "Attack as Service" is used by attackers to run a denial of service, spam, phishing etc. attacks using a cloud platform. In this type, the Bot master uses cloud services to build botnets.

III. BOTNET DETECTION AND CONTROL

Botnet detection and countering them is also important to improve the cyber-security. Defence techniques against bots needs to involves three things: propagation control and communication to be disabled between bots and C&C server. Botnet detection techniques were originally categorized into two types: (i) honey nets (ii) intrusion detection. Honey nets and honeypots gather critical information about the cyber-attacks. Honey net monitors, collects, modifies and controls communication over the honeypot. Intrusion detection can be signature based or anomaly based. In a signature based technique the malware is monitored as sequences of packet. Anomaly based detection detects malicious threats by searching abnormal behavior in network(Tyagi and Aghila, 2011). Data-mining techniques can also be used to extract data for analysis from network log file(Sivakumar and Srilatha, 2016). Flow correlation algorithm can be used to compare flow of objects based on certain characteristics. (Guntuku, Narang and Hota, 2013) proposed a hybrid framework by integrating neural networks with Bayesian regularization pre-processing module. This framework is suitable for detection of newer and unseen botnets in live traffic of a network. Neural network and deep learning is more suitable for traffic identification, feature learning, protocol identification and anomalous protocol detection(Wang, 2015). To detect peer-to-peer bots is difficult due to its decentralized nature(Narang *et al.*, 2014). (Narang *et al.*, 2014) has proposed a framework PeerShark;that detect P2P botnet traffic and distinguish it from other traffic in the network. (Narang *et al.*, 2014) uses 2-tuple conversation based approach to detect botnet. Fast Flux Botnet detection technique and domain flux botnet detection can be used to detect and trace more sophisticated botnet.

IV. CONCLUSION

According to network attack statistics, botnet based attacks account for majority of network attacks and application targeted DDOS attacks are also increasing. The increase in the use of smart terminals and mobile applications to have resulted in increase in botnet attacks. Botnets in China and USA account for 30.3 % and 26.2 % of the global botnets according to Huawei Cloud Security Center Survey. Among the botnet controllers, 42.2% are in USA, 3.8% in China, 9.1 % in Germany, 7% in France and 5.8% in UK. In the coming years, there will be increase in mobile botnets, larger point-to-point botnets and use of evasion techniques like Fast-Flux. The proliferation of internet services and cloud computing in the last couple of years has resulted in increase in DDOS attacks on cloud IDCs. The attackers these days prefer to target light traffic applications and other low-speed attacks to reduce the attack cost, conceal attack sources and evade security devices without reducing attack severity. Multi-core network security devices too unevenly distribute traffic to their multiple cores. This vulnerability can also be exploited by attacker to execute new type of DDOS attacks. Network governance needs to emphasize on network security devices to be capable of DDOS attack tracking and detecting malicious fast-flux DNS request, botnet communication packet monitoring and behavior identification. Network governance also needs to focus on cloud-based botnet monitoring and analysis. There is also a need to design and develop more unsupervised machine learning and deep learning algorithms for detection of new entrants of botnets and detect and counter them at first instance. Also there is need of work to be done to detect and filter fast-flux DNS requests, as DNS servers function are the first point for internet connection and fast-flux DNS request detection. Botnet governance is global responsibility and requires cooperation among network security-related organizations to track botnet sources, shut-down botnet source servers or C & C servers and also investigate botnet writers from law-enforcement aspects. Timely updates of security patches is also responsibility of every individual user of intelligent device. The owners of web-resources need to focus on effective protection from botnet attacks originating from servers botnets.

REFERENCES

[1] Ajmera, D. R. and Gautam, R. (2014) 'International Journal of Advanced Research in Computer Science and Software Engineering', 4(1), pp. 584–587. Available at: http://www.ijarcsse.com/docs/papers/Volume_4/2_February2014/V3I12-0320.pdf.

[2] Bilodeau, O. *et al.* (2014) 'Operation Windigo - The vivisection of a large Linux server-side credential stealing malware campaign'.

[3] Bu, Z. *et al.* (2010) 'The New Era of Botnets', *White paper from McAfee.* Available at: https://www.botnets.fr/images/b/b5/Wp-new-era-of-botnets.pdf.

[4] Guntuku, S., Narang, P. and Hota, C. (2013) 'Real-time Peer-to-Peer Botnet Detection Framework based on Bayesian Regularized Neural Network', *arXiv preprint arXiv:1307.7464*. Available at: http://arxiv.org/abs/1307.7464.

[5] Hua, J. and Sakurai, K. (2013) 'Botnet command and control based on Short Message Service and human mobility', *Computer Networks*, 57(2), pp. 579–597. doi: 10.1016/j.comnet.2012.06.007.

[6] Narang, P. *et al.* (2014) 'PeerShark: Detecting peer-to-peer botnets by tracking conversations', *Proceedings - IEEE Symposium on Security and Privacy*, 2014–Janua, pp. 108–115. doi: 10.1109/SPW.2014.25.

[7] Silva, S. S. C. *et al.* (2013) 'Botnets: A survey', *Computer Networks*, 57(2), pp. 378–403. doi: 10.1016/j.comnet.2012.07.021.

[8] Sivakumar, B. and Srilatha, K. (2016) 'A novel method to segment blood vessels and optic disc in the fundus retinal images', *Research Journal of Pharmaceutical, Biological and Chemical Sciences*, 7(3), pp. 365–373. doi: 10.15680/IJIRCCE.2016.

[9] Tidke, S. and Karde, P. (2015) 'Botnet Attack: Is it a risk for Smart Phones?', *IOSR Journal of Computer Engineering Ver. II*, 17(3), pp. 2278–661. doi: 10.9790/0661-17326972.

[10] Tyagi, A. K. and Aghila, G. (2011) 'A Wide Scale Survey on Botnet', *International Journal of Computer Applications*, 34(9), pp. 975–8887.

[11] Wang, Z. (2015) 'The Applications of Deep Learning on Traffic Identification', *Black Hat USA*.

[12] Wilson, C. (2008) 'Botnets , Cybercrime , and Cyberterrorism', *October*, pp. 1–40. Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA474929.

[13] Xiao, Y. *et al.* (2009) 'Botnet: Classification, attacks, detection, tracing, and preventive measures', *Eurasip Journal on Wireless Communications and Networking*, 2009. doi: 10.1155/2009/692654.

[14] Zhao, D. *et al.* (2012) 'Peer to peer botnet detection based on flow intervals', *IFIP Advances in Information and Communication Technology*, 376 AICT(1), pp. 87–102. doi: 10.1007/978-3-642-30436-1_8.

[15] Thomas, K (2015) 'Nine bad botnets and the damage they did' Available

at:https://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/ (Accessed: 5th September 2017)

[16] Kerbs on security (2016) 'Source code for IOT Botnet 'Mirai' Released', Available at: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/ (Accessed: 10th September 2017)

[17] Morrison T (2014) 'Spamhaus Botnet Summary 2014', Available at: https://www.spamhaus.org/news/article/720/spamhaus-botnet-summary-2014 (Accessed: 10th September 2017)

[18] Dell SecureWorks Counter Threat Unit(TM) Threat Intelligence (2014) 'Top Banking Botnets of 2013' Available at: https://www.secureworks.com/research/top-banking-botnets-of-2013 (Accessed: 10th September 2017)

[19] Wilson C. (2008), 'Botnets, Cybercrime and Cyber-terrorism: Vulnerabilities and Policy Issues for Congress' CRS Report for Congress

[20] Available at: https://en.wikipedia.org/wiki/ZeroAccess_botnet (Accessed: 11th September 2017)

[21] Available at: https://en.wikipedia.org/wiki/Storm_botnet (Accessed: 11th September 2017)

[22] Available at: https://en.wikipedia.org/wiki/Mariposa_botnet (Accessed: 11th September 2017)

[23] Available at: https://en.wikipedia.org/wiki/Conficker (Accessed: 12th September 2017)