Features of the Global Nature of Botnets

Posted on January 5, 2024

Botnet Evaluation

Internet-related criminal attempts are made through botnets which are a network of computers infected with malware opted for cyber intrusions globally. Botnet complaints are received and processed further by the partnership of the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI) through centers such as Internet Crime Complaint Center (IC3) to investigate the suspected internet-facilitated activities concerning criminal or civil violations on the Internet. The center of IC3 cites that identity theft and merchandise are most of the internet-facilitated complaints reported on the part of internet users. This essay evaluates botnet intrusions into the major power systems of the United States over the past 10 years despite strict cybersecurity policies.

One of the key features of Botnet that highly impact the core power systems is that Botnets turn a computer into a “zombie” or a “robot” that operates according to the instructions given by the attackers or is simply jammed due to the restricted access. For an attacker, that computer would be a “robot” that can be operated remotely, but for an organization, the computer would be a “victim” that causes billions of dollars worth of damage. However, the prevalence of botnets is mostly a mystery because of the zero regulations in the cyber world (Choo, 2007). For instance, online gambling is one of the daunting international Botnet concerns around the world, especially in countries which have had fewer or zero gambling regulations for internet users over the last 10 years because of the massive use of technology. It is a popular industry, particularly in developing countries where criminals locate servers of law enforcement agencies and evade their regulations. In Russia, a criminal organization named Russian Business Network rents server resources to criminals in and out of the country to criminal organizations. These organizations deal in child exploitation, spam, and malware which links criminal organizations further to the multiple DoS events.

DrStrangeLove is a worm which has the ability to replicate itself, disabled and infected core power delivery systems of nearly 34 cities in the United States for the few past years. It has infected, disabled, and shut down the Supervisory Control and Data Acquisition Systems (SCADAs) and prevented administrators from logging on their servers by shutting their power delivery systems in around 49 cities. Attackers have made their way to the DoS systems and slowed down internet speed on the large scale across the country. A hundred thousand Botnets were spread around the globe which restricted analysts and programmers from understanding the real cause and source behind the attack. A massive disturbance was created in the country as mobile phone communications were also attacked due to the jammers in the form of a Botnet that impacted phone lines of the US government. The economy of the United States highly suffered damage of billions of dollars due to the massive Botnet attack. Cyber Command of the United States, for example, recently planted a self-replicating

worm that was capable of disturbing, shutting down, and blocking the telecommunication system of Azhirabad to change missile warheads over the internet. The worm after distorting the electrical power grid system of Azhirabad destroyed itself so that it could not be detected. Therefore, it is important for global cybersecurity systems to develop a robust mechanism for the identification, analysis, and removal of botnets (Karim et al., 2014).

Moreover, a Zeus-based Botnet attacked a large regional bank, Westwood Mutual's IT system has compromised more than $1.5 million and nearly 5000 online banking accounts countrywide. The intruders have stolen confidential information through the malicious code that has remotely controlled Westwood Mutual's system by remotely controlling it via the internet. Thousands of online banking accounts were disabled or blocked to harvest confidential information of the users by distributing spam. The kind of Botnet used to attack Westwood Mutual operates through an Internet Relay Chat (IRC) for remote hacking, spamming, and attacking the systems through malicious codes via the internet. Internet abusers exploit applications over the network by committing different crimes such as phishing, scamming, malware distribution, etc. (Binsalleeh et al., 2010). This channel is a means of peer-to-peer networking communication or real-time communication with the use of a server over a network, or internet for the stealth. The server named Command and Control (C & C) Server is used for the protection against detection and identification of intrusion of the Botnet into the systems.

A botnet is a network of "bots" that evade the security of other systems or networks with embedded malware in their malicious coding so that the attackers can operate the infected or victim computer, network, or system according to their own interests. Bots allow the systems to be controlled as part of an embedded network while acting as a "zombie" to the security organizations to launch Distributed Denial-of-Service (DDOS) attacks. They generally leverage the operations of the computer systems over the network without permission or get detected by the owner of the system. Cybercriminals harness botnets that opportunistically exploit the privacy and security of internet users over the network by exploiting the flaws in the devices to perpetrate their illegal operations. This paper delves into the 6 important features such as nature, purpose, size, attack method, and attribution of the botnets that have emerged, changed or evolved over the past 10 years.

1. Nature of Botnet: Botnets are the collective network of security-compromised malicious computers or systems that disturb, infect, or block other systems without owners' permission. Bots have a flexible and dynamic nature as they get updated from day to day by their botmasters as per their nefarious designs. They are controlled by a third party as per its own nefarious designs to steal something or to pose some serious threats to the computer systems through Internet Relay Chat (IRC).
2. Purpose of Botnet: The purpose of a botnet is the installation of malware for sending out spam messages that often include malware hidden in malicious codes they sent to the owner of the system which compromises the security of that system.
3. Size of the Botnet: Bots usually get towered numbers from each malicious code sent to the computer systems over the network. For instance, Cutwail Botnet is a popular botnet of the contemporary decade that replicates itself to recruit more computers to the botnet by sending

automated directions to other computers via a covert channel to make more computer "zombies" for thieving and mining information through the illegal channel.

4. Attack Method of the Botnet: Hackers usually instruct the compromised computers through a command-and-control server for building online threats such as data theft, spam, online fraud, security risks, etc.
5. Attribution of the Botnet: Botnets are attributed as the trick used to lure the user over an instant message attachment, an email, or downloaded content from the web by self-replication of the malware. Self-replication is the attribution of the botnet which attackers use to affect a large number of computer systems over the network such as Slammer and Blaster which replicate themselves to enable covert communications of rogue "zombies" or actors.
6. Lifecycle of a Botnet: Botnets vary in their sizes, structures, and purposes, but they all share the same phases in their lifecycle. Bots go through the stages of propagation of infection, rallying, commands, reports, abandonment, and defense. First of all, botmasters use the infection processes to compromise another computer system, then it moves to the next stage of rallying through self-replicating, the stage of commands and reports occurring when bots are spread with day-to-day updates of stealing information. Bots after executing the desired process in the hands of botmasters are abandoned by the attackers as a defense so that the source of the botnet could not be detected (Eslahi et al., 2012).

Factor to Mitigate Botnets' Impacts Over the Next 10 Years

Cross-border collaboration and enforcement of the global cybersecurity laws and regulations is one of the significant factors the channel of botnets can be controlled, and their threatening impacts can be mitigated. These collaborative actions facilitated by cybersecurity laws should be implemented across the globe to make botnet attacks illegal. In order to mitigate the unsolicited spam or fraudulent attacks, the cyber world must permit information mining and collection appropriate to dismantle the impacts botnets potentially have caused to vulnerable devices (Yaacoub et al., 2020).

References

Eslahi, M., Salleh, R., & Anuar, N. B. (2012). Bots and botnets: An overview of characteristics, detection and challenges. *2012 IEEE International Conference on Control System, Computing and Engineering*, 349–354.

Yaacoub, J.-P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and Microsystems*, *77*, 103201.

Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., & Wang, L. (2010). On

the analysis of the Zeus botnet crimeware toolkit. *2010 Eighth International Conference on Privacy, Security and Trust*, 31–38.

Choo, K.-K. R. (2007). Zombies and botnets. *Trends & Issues in Crime & Criminal Justice*, *333*.

Karim, A., Salleh, R. B., Shiraz, M., Shah, S. A. A., Awan, I., & Anuar, N. B. (2014). Botnet detection techniques: Review, future trends, and issues. *Journal of Zhejiang University SCIENCE C*, *15*(11), 943–983.