American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

A Survey on Botnet Attacks

Jiala Mafo Jules[a*], Hongbing Cheng[b], Gloria Rumbidzai Regedzai[c]

[a,b,c]*College of Computer Science Zhejiang University of Technology Hangzhou-China*
[a]*Email: julemafo@outlook.com* , [b]*Email: chenghb@zjut.edu.cn*, [c]*Email: ruregedzai@icloud.com*

Abstract

Devices connected to the Internet are the target of numerous attacks to steal or exploit their resources. As these attacks become widespread (and sophisticated), the first step in protecting your organization is knowing exactly what you are facing. We currently have botnets that are the main source of network attacks such as spam, denial of service (DDoS), click fraud, data theft, Pass the Hash, and RDC attacks. With the evolution of technology, we have several solutions to protect against attacks that undermine businesses, governments, individuals, but security attack methods are increasing daily. This study seeks further investigate botnet attacks and also provide a comparison of these attacks, lastly, the survey will create awareness for forthcoming botnet research endeavors. Being rejected by search engines. Ensure that your abstract reads well and is grammatically correct.).

Keywords: botnets; DDOS; Data Theft; Security; Click fraud Introduction.

1. Introduction

A network attack is usually attributed to the botnet which is a collection of computers connected to the Internet infected by malicious software that allows these computers to be controlled remotely by an operator (hacker) via a Command-and-Control server to perform certain tasks such as embezzlement of information or launching attacks against other computers with that being said Botnet malware is designed to give its operators control over many computers at the same time. This allows botnet operators to use computing resources and bandwidth through various networks for malicious activities, which is a challenge in terms of repression. First and foremost it is important to note the importance of their impact on network security and the commission of offenses on the Internet. Then by the extremely international dimension of their diffusion and thus a certain difficulty to carry out investigations. Finally, a large number of actors may be involved (coders who write malicious software programs, political activists, mules responsible for eventually relaying the financial gains from illegal activities, sponsors, or service traders).

---

* Corresponding author.

Sometimes major organizations are set up to manage infrastructure for such botnets for the sole purpose of marketing its services (Binkley and Singh, 2006) [1] services. Too often a link exists between such and prohibited action by law. This study seeks to provide an outlook on current botnet attacks by exploring the intersection between the evolution of botnets, as well as the goals and perspectives of various types of networks. Secondly, an in-depth overview of botnet attack strategies will be provided in this research paper. Thirdly a description of innumerable categories of botnet attacks based on the company's experiences which have a significant impact on the effectiveness of any botnet detection mechanism will be outlined and lastly, a recommendation on relevant security policies for the users and network administrator to prevent attacks will be provided.

1.1 Botnets strategies overview

Botnets are usually defined as networks made up of malware-infected computers, which allow an offender, also known as a "botmaster", to simultaneously control thousands or even millions of machines at the same time. Botnets are very difficult to detect because they use only a small part of the computing power of the infected machine. This is what allows them to avoid disrupting the operation of the device and thus alerting the user. Some can even adapt their behavior to avoid being detected by the cybersecurity software. Over time, malware is becoming more and more advanced and therefore more difficult to detect [1] the construction of a botnet can be broken down into five main phases (Figure 1). In the first phase, the botmaster must develop malicious software with features that allow stealth with infected machines. Closely followed by the hacker injecting the malware into as many machines as possible. The third step is aimed at taking over infected machines and their integration into the pirate's command infrastructure [2] the fourth stage in the process is exploitation, where all the efforts of the pirates pay off and result in the extraction of financial gain or benefits in another form, such as the neutralization of an adversary. Lastly, the botmaster keeps a tight grip on the network of machines. It can be noted that besides Botnets which mostly use centralized commanding and control(figure2), there are Botnets that use Peer-to-Peer control, and in that case, there are no central controllers [3,4].

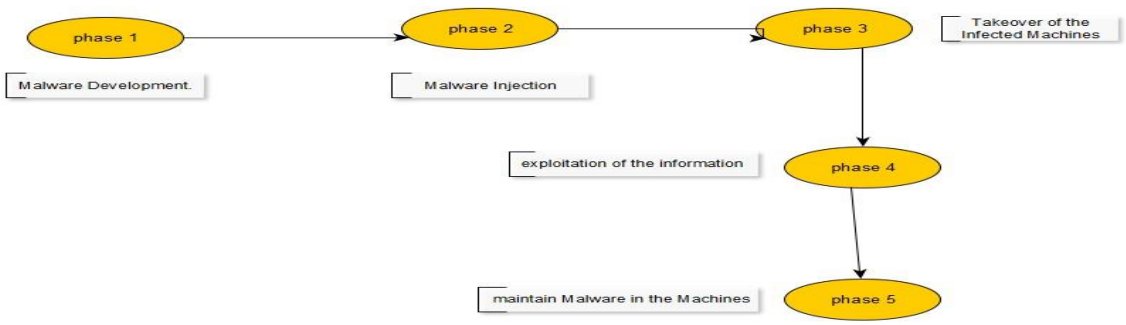

Figure 1: The five main phases of the botnets attacks.

A. phase 1: develop malicious software

Malicious Software is also commonly referred to as Malware. According to Schneir [5], "Malicious Software includes computer viruses, worms, and Trojan horses", other spyware, dishonest adware, crimeware, rootkits, and other unwanted software. At this stage, the communication has to be bidirectional to allow for the transmission of a "Virus" through various instructions, but also so that it can account in return for its state of functionality. This case integration into this is only possible through the ability of the software to extract the various information held by infected machines, be it documents, e-mails, or passwords used by owners to access bank accounts or other online services. If the botmaster does not have sufficient programming skills, obtaining already functional applications on hackers or hackers forums will be an option to consider, the price of which will vary according to the performance and technical support offered by its designers.

B. phase 2: malware injection

Most often, malware gets access to your device over the internet or by email [6,7]. However, users may access the site through pirated websites, game demos, music files, toolbars, software, free subscriptions, or any other item downloaded from the web to a device that is not protected by copyright. In this phase, the hacker must inject the malware into as many machines as possible. Several strategies are available to him: he can proceed to a more or less wide phishing campaign, sending millions of emails (Figure 2) inviting through recipients clicking on a link under pretenses and generally associated with a sense of urgency. A method of infiltration through outsourcing is responsible for the delivery or installation of computer equipment, the Botmaster may entrust specialized brokers with the mandate to install its application on machines already compromised, remunerating these intermediaries according to the volume of infections and the geographical distribution of a contaminated Computer[7,8].

C. phase 3: taking over infected machine

With the large size of botnets that often combine to attack tens of thousands of computers or a little more, with the establishment of specific communication protocols for coordination and distribution of tasks, Botmasters cannot allow individualized management victims. So Botmaster sends instructions to zombies via dedicated servers, called C & C servers (command and control), or via online chat channels to which robots connect at regular intervals [9]. At this point, the challenge for botmasters is to succeed in taking control without being detected by the victims or their Internet Service Providers (ISPs), which would lead to the implementation of corrective measures and the loss of control [10,11] believe that to maintain the stealthiest of communications with robots, the most technologically advanced bot masters implement encryption solutions

D. Phase 4: the exploitation of the information

The fourth phase is the exploitation of all information received after all efforts, put forward to make it a possibility. This information or crimes can be classified as tax fraud, banking, blackmail, and even destruction of property and private information. For that reason Companies having, for example, developing innovative Processes, working in certain sectors of activity even as subcontractors (military field, aeronautical, pharmaceutical, ...) or still responding to a major invitation to tender must, therefore, be particularly vigilant

[12]. Distributed Denial of Service (DDoS) attacks exploit the large size of botnets to saturate the servers of targeted request organizations and make them unavailable to legitimate users. These attacks can be sponsored for ideological reasons, but also to disrupt the commercial activities of competitors or blackmail against companies whose profitability is immediately eroded by this type of action, such as online shopping for example.

E. Phase 5: maintaining malware in the machine

Malware has evolved over the decades and is no longer used to destroy systems or to infect as many candidates' devices as possible for the sole purpose of enabling efficient communication. With that being said malware is becoming more discreet and its creators have only one fear which is losing discretion and getting exposed. Malware is usually hidden in software, in the operating system, in documents, and the Mails. This is to note that the only goal of botmaster today is to generate profits [13], by infecting the largest number of machines in the shortest possible time. And that's why technology such as rootkit systems, malware such as adware, or spyware have appeared because most are a catalyst to generating funds and maintenance of discreet in the computers through access to private information from the users.

1.2 Different categories of botnets

Botnets can be grouped into several broad categories that sometimes overlap since the features are sometimes common to different families and the intention behind the development has multiple underlying reasons. The following categories can be mentioned, among others [14]:

- Data theft: Bank details (credit card numbers, online bank account IDs, hijacking of a connection session to an online bank account, etc.); Spying on confidential or sensitive information.

- Spam or unsolicited e-mail, which is not limited to illegal commercial prospecting as defined by the law for trust in the digital economy but can relay various malicious messages or attempts at fraud, for example.

- Distributed denial of service (DDoS) attacks that aim to make an Internet connection or server inaccessible and are greatly facilitated by the use of a botnet that can gather several hundred thousand machines [15].

- Ransom software whose principle is to block the use of the victim's computer (or telephone) and demand the payment of a ransom, with the variant particularly becoming popular in the past couple of years which consists of posing as a legitimate message from police service and demanding payment of a fine.

- RAT (remote administration Trojans)[16] is particularity is to group in a single tool a whole bunch of features that could look like a remote help tool, but which allow many malicious actions to be

performed: activation of the video camera, recording screenshots, file copies, recording passwords, etc... They are used by spy companies as well as by young offenders in search of thrills - some publish video recordings of their exploits on the Internet as a form of cyberbullying their victims.

Manipulating online polls /games are getting more attention from online users. It is a technique, easy to manipulate with Botnets. Every bot with a distinct IP address, every vote will have the same credibility as a vote cast by a real person. Online games can be manipulated in a similar way to perform malicious activity.

1.3 Related work

In this Section, we present works that have been published in the area of botnets attacks, their detection and isolation, and the mitigation of large-scale Botnets attacks. Manoj, Divya, Kushinagar, and al [23], proposed an IoT defense algorithm to prevent Botnet attacks by making IoT devices in the same way intelligent as bots while preserving a lightweight and inexpensive solution. To understand the difference between a benign and a malicious request, a node analyzes the consistency of the packet content. Although results showed that this approach helps to prevent attacks, it depends on the limited resources of every bot [24,25]. Baldwin and Lodge [26,27] emphasize that to secure the botnet attack by using secure software, the approach uses an open protocol basic elements in the two models namely- centralize and decentralize, others approach is the Signature-based method analyzes network traffic based on packet-level and signatures of malicious payload through deep packet inspection (DPI). Therefore, it has higher accuracy for known attacks. However signature-based method could only analyze attacks or botnets already known [28]. In the articles [29,30] the researcher highlights the commercial and social benefits of safe and well-informed use of social networking websites. It emphasizes the most important threats of the users and illustrates the fundamental factors behind those threats. Moreover, it presents the policy and technical recommendations to improve privacy and security without compromising the benefits of information sharing through social networking websites. We noted that 90% of data theft or loss is due (in whole or part) to human error: incorrect configuration, use of overly simple login and password, loss or theft of laptops or smartphones, the opening of malicious attachments or URLs [31,32]. All these metrics are specific to crisis management following a cyber-attack and they condition the implementation. The aforementioned approaches focus on analyzing the incoming traffic or emulating a benign botnet to prevent Botnet attacks, while further protections by using secure software are still limited. Therefore, the avoid infections approach to detect and stop vulnerable devices proactively is still missing. Thus, we introduce some propositions to avoid the attack in Section V based on the users and administrators.

1.4 Propositions to avoid the attack

While there are plenty of potential malware vectors that the average organization needs to deal with regularly, there are also numerous different strategies that make keeping malware at bay far more manageable. The first of these is ensuring a viable communication flow at all times [33]. This means you will also need to ensure proper network segmentation at all times and also ensure that any control lists that are network-based are properly configured to ensure that they permit server-to-host and host-to-host connectivity via the minimum scope of ports and protocols and that directional flows for connectivity are represented appropriately. It is also important

to ensure that your flow paths for communications are not only well defined but authorized or documented as well. From there, you will want to strive to increase awareness of systems that can be utilized as a gateway to laterally pivot as needed or directly connect to relevant endpoints found anywhere throughout the enterprise[34]. Whatever you do, it is important to do what you can to ensure that these systems are maintained within these restrictive VLANs with appropriate network access control and segmentation as needed. When it comes to ensuring the right amount of control over who has access to what, it is important that enterprise systems that can interface with numerous endpoints directly all require dual-factor authentication for any interactive logins [35]. Further, it is important to make sure that authorized users are limited to a specific subset of the organization's personnel. Whatever you do, the default user group mustn't have the ability to authenticate or access these systems directly. We will also need to ensure that unique domain accounts are documented and utilized for every service that involves an enterprise application. The context in which these permissions are assigned to various accounts should always be fully documented and also configured in such a way that the greatest number of users have the fewest number of privileges possible [36]. Doing so provides the enterprise with the ability to track and monitor actions that are taken based on assigned service accounts. This is why it is important to avoid providing a service account with either interactive or local login permissions. Service accounts should be expressly denied these types of permissions, especially if access to critical data locations or important network shares [37]. Additionally, accounts that are used to authenticate centralized servers should not contain-downstream systems that have elevated permissions as this could allow a system that is far easier to compromise to infect a system that is typically far better protected. A good example would be a hacker who has just created a key logger to recover personal passwords and credit card numbers and has associated it with a rootkit to divert attention from antivirus software. This hacker infects 15 computers via malware. On these 15 computers, retrieval of 100 credit card numbers, and 150 remote mailbox passwords of all kinds (Hotmail, Yahoo, SFR, outlook,) is a possibility. The hacker retrieves all this and goes to a hacker block which will send a notification to all other users of the block based on the fact that there are numerous credit card numbers and passwords. This information can be used for identity theft purposes in the hopes to gain profits from the sale of such confidential details which can be easily sold for almost $12. Now the question is "why do people buy credit card numbers and mailbox passwords?" Identity theft on credit cards is solely to make online purchases [38], however, for passwords, this allows for access to spam the user's contacts on email addresses. Spam will most often be sent to sites that will increase their number of visits, and therefore their earnings. In this very complex environment, each actor needs the other, and this system is based on money. We can also note that many pirates never create malware utilized personally, but purchase from other pirates who develop and sell it [39]. Although botnets pose a threat to Internet users and are difficult to eliminate, this is the problem that can be solved by acting swiftly and taking necessary measures to eliminate possible risks and minimize the impact [40]. This section of the study stipulates several types of security tools that can mitigate botnet attacks.

2. antivirus

In [41,42] are of the notion that antivirus software uses several techniques to detect attacks, including malware signatures. The more signatures one has the more likely it is to detect attacks, hence its effectiveness. Therefore emphasizing the importance of regularly updating antivirus software. The same goes for firewalls, if one uses another security software application of the same policy is advisable. However, no matter how up-to-date

software is it surely doesn't guarantee 100% effectiveness... It is preferable to download the security software (and indeed all software) on the publisher's site or reliable sites. And above all, do not download software offered by advertisements. Accordingly, antivirus software should be configured to attempt to disinfect infected files and to either quarantine or delete files that cannot be disinfected. For having easier updating and maintenance, some integral software solutions such as Internet Security software (Kaspersky Internet Security or Norton Internet Security) can be installed.

3. Updates

Maintaining the operating system updates allows for closed security gaps detected by the operating system vendor. These vulnerabilities are, so to speak, kinds of "holes" in the operating system through which malware can penetrate. It is system vulnerabilities that put it at risk, even if it has an updated antivirus, hence the antivirus software offering installation of operating system updates and detection of critical computer failures. The more up-to-date the operating system is, the less free access, and lower the potential risk of being infected, so updates should be made as soon as availability allows. But, the updates should be framed according to the working environment, as updates may cause other issues such as software malfunctions compatible [43]…

4. Vigilance

Concerning vigilance, users are the main actors who lead to good data security. In the case of botnets, an infected computer has the purpose of attacking all the other computers of the network, so every user bears the responsibility to avoid such instances, therefore, every organization has to hire an engineer to assist in increasing user knowledge through training of employees from falling victim to obvious traps on the net, such as P2P, cracks, suspicious sites, pornographic sites... Indeed, these four things are the main vectors of infection on the web [44]. It is also very important to understand that antivirus, firewalls, and other security software alone do not ensure the security of network infrastructure, and it is solely up to users to stay vigilant against such traps. Contrary to what the vast majority of people think, security software (Antivirus) is not powerful enough to prevent all infections and fight against attacks, infections evolve daily until recognized and included in viral databases, daily operations exist without barriers.

5. Firewall

Firewalls and load balancers can help absorb some botnets attacks, for example, those generating relatively low traffic. Firewalls can be used to filter traffic based on the transport protocol and source or destination ports or limit the number of requests per address Source IP to a server [45]. Why a firewall?

- ➢ Control: Manage outgoing connections from the local network.
- ➢ Security: Protect the internal network from intrusions from outside.
- ➢ Vigilance. Monitor/trace traffic between the local network and the internet.

On the other hand, we have several types of firewall, we can quote:

- Network-level firewall: more specific to TCP / IP protocol management, Based on packet filtering with the ability to filter (if available mechanism) packets depending on the state of the connection and with for main Interest, transparency for the user's network.

- Application-level firewall: Generally based on the proxy mechanism with the principal Interest:

Possibility of interpreting the content of the traffic.

- Application Firewall

The applicative firewall is essential in the Verification completion of the conformities of the packet as an expected protocol. Allows for more complete protection (deletion of active content in web pages, deletion of macros in documents ...) requires more resources, impact on performance.

6. Secret key policies

The passwords are chosen by users mean the difference between a cracker PC and a protected PC. Hence choosing a password link to the personal information of the user could prove fatal. Therefore it is advisable to use a variation of letters, numbers, and characters hence maintaining user discretion as much as possible while making it easy for the user to memorize the information for future use [45,46]. It is also important to highlight to users to never at any point share this confidential information. Most people create passwords based on company names and family references. This is to say that users always have a point of reference to which they memorize such confidential information.

7. User Training

Watch Guard Technologies in 2008 wrote an article on defeating the botnets of the future where they reiterated that user knowledge and awareness are crucial as a defense strategy against Botnets because irrespective of all system measures and precautions put in place for defense purposes is all in vain if the user isn't well versed on how to manipulate the tools, therefore, constant training of users is essential. Organizations could use basic techniques and information to improve employee user knowledge through the emphasis on the following information [47]:

-Accessing questionable Emails is prohibited (transfer it to your administrator).

-Saving important passwords on the workstation browser must be avoided at all costs.

-Always ensure to check the padlock on the address bar of the internet browser when making online payments…

Organizations must determine which methods most effectively teach users to recognize cyber threats, operate applications safely, and comply with policies. Common methods include mandatory training, instructional e-mail from IT, department training, and self-phishing. Self-phishing occurs when IT distributes to employees decoy computer-mediated messages embedded with cues and lures that they are expected to catch. Mock cyber-attack exercises safely simulate deception, expose vulnerabilities, highlight learning needs, and provide feedback on training effectiveness.

7.1 Crisis Management Phases

In the case of a crisis, organizations that lack protection against attacks on electronic systems are bound to collapse [48]. Based on the cybersecurity incident response plan, it will be able to define several standard operating procedures for frequent incidents with a proven probability in the organization. These procedures should explain step-by-step how a specific problem can be addressed. These rapid response guides for likely scenarios should be easily accessible. However, analyses by researchers revealed that most organizations' botnet protection systems utilized the following services to manage system attacks:

- Packet size test
- Source and destination address testing (as well as loopback, unicast, multicast...)
- Fragmentation test
- Use of virtual IP addresses for session validation and ACK (TCP counter-attacks)

- Testing of the number of SYNs (TCP counter-attacks)
- NAT of local to virtual IP addresses based on global IP
- Flow control
- Content controls (port, tag, URL, file extensions) -other firewall functions, all based on load balancing and redundancy.

Beyond a strategic choice of technical protection, it is important to develop several good practices for optimal crisis management in the event of a crisis of attack. These organizational measures can be sequenced chronologically, according to the stage of the attack to which they relate. As a precautionary measure, an analysis of the criticality of the targeted services, the threat, and overall security needs will allow for a shift towards one of the four previous technical choices. This will also help to build the future management process, particularly in the event of a crisis [48]. Once an attack is declared, it is essential to be able to effectively identify its behavior, determine its extent, and identify the first services impacted[49]. The crisis management processes initially determined will also allow to frame and mitigate edge effects. Finally, once the attack is under control, the services are restored and their proper functioning tested and validated, it will also be recommended to document the details of the incident, to draw up feedback, and thus adjust protection and action plans by consequently, in the interest of continuous improvement.

- ***Phase 1: Before the attack***

-Analyze the threat

-Analyze security needs

-Choose some of the basic rules listed above.

-Build crisis management processes

- ***Phase 3: during the attack***

-Identify its behavior

-Determine it's the magnitude

-Identify impacted services

-Apply crisis management processes

- ***Phase 3: after the attack***

-Repair and test impact services

-Bring back experience

-Adjusting protection plans and crisis management processes.

In the case of a botnet attack, the management of

The crisis caused by the attack could, therefore, correspond to the sequence as shown in Figure 3

Figure 1

In most cases, two issues arise in the event of an attack: cutting off-network access or finding the hacker. Both scenarios are feasible if and only if the response policies have been properly implemented on the user side and network administrators. In addition to all these measures and techniques, it is also necessary to consider setting up a detection system that sends warning thresholds to trigger preventive actions, therefore defending as soon as possible.

8. Conclusion

In conclusion, this study pinpointed existing Botnets attacks and Botnets' strategies coupled with various phases and basic rules to avoid infections. Botnet attacks exploit flaws in protocols and systems to deny access to target services. Attackers also control a large number of compromised hosts to launch the attacks. Simply securing servers is no longer sufficient enough to sustain systems under siege, because Botnet attack techniques are more complicated and many unwitting hosts are involved in a botnet in such scenarios. For defenders, it is difficult to decide whether a packet is spoofed, to prevent a host from being compromised and controlled, to ask upstream routers to filter unwanted traffic, and to keep defenders themselves from botnets attacks, therefore, making them complex. However numerous approaches have been proposed to counter them such as applying strategies that defend against such attacks. Besides, knowledge of the financial impact of a botnet attack should also encourage awareness of botnets when formulating security policy, as well as implementing procedures, and controls. Although bots and botnets have been present for the last five years at least, they are still a little-understood threat, which needs to be serious to be considered.

References

[1]. 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, pp. 7–7, Berkeley, CA, USA, 2006

[2]. Top Ten Cyber Security Menaces for 2008, SANS Institute, 2009.

[3]. Ramneek Pur, Bots &; Botnet: An Overview, SANS Institute Information Security Reading Room, GSEC Practical Assignment Version 1.4b, August 08, 2003

[4]. Muhammad Mahmoud, Manjinder Nir, and Ashraf Matrawy, International Journal of Network Security, Vol.17, No.3, PP.272-289, May 2015

[5]. Schneier, B. (2004). *Secrets and Lies*. Indianapolis, Indiana: Wiley Publishing, Inc.

[6]. Narendra Kumar Tyagi(Asst, Professor) DCE.Khentawas, Gurgaon, AbhilashaVyas(Asst. Professor)DCE.Khentawas, Gurgaon, Data security from malicious attack: Computer Virus.

[7]. Sharp, Robin, An Introduction to Malware, pp. 18, 2017

[8]. Matija Stevanovic and Jens Myrup Pedersen Networking and Security Section, Department of Electronic Systems Aalborg University, DK-9220 Aalborg East, Denmark Machine learning for identifying botnet network traffic, pp.5-6, 2013

[9]. Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna University of California, Santa Barbara, CCS'09, November 9–13, 2009, Chicago, Illinois, USA.

[10]. Paul Barford Vinod Yegneswaran, an inside Look at Botnets, computer sciences department university of Wisconsin, Madison, pp.15-16, 2017.

[11]. Trend Micro, Taxonomy of Botnet Threats, A Trend Micro White Paper / November 2006.

[12]. USENIX Association Understanding the Mirai Botnet, 26th USENIX Security Symposium 1093.

[13]. Massimiliano Romano, Simone Rosignoli, Ennio Giannini, Robot Wars – How Botnets Work, Window Security, 2009.

[14]. S. K. Pandey, Security Vigilance system through Level Driven Security Maturity Model, International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.2, April 2012.

[15]. Defeating the Botnets of the Future, WatchGuard Technologies, 2008.

[16]. K. Veeramachaneni, I. Arnaldo, V. Korrapati, C. Bassias, and K. Li, "Aiˆ 2: training a big data machine to defend," in Big Data Security on Cloud, IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on. IEEE, 2016, pp. 49–54.

[17]. N. Blenn, V. Ghiette, and C. Doerr, "Quantifying the Spectrum ¨ of Denial-of-Service Attacks through Internet Backscatter," in Proceedings of the 12th International Conference on Availability, Reliability, and Security - ARES '17. ACM Press, 2017, pp. 1–10.

[18]. Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," Journal of Information Processing, vol. 24, no. 3, pp. 522–533, 2016.

[19]. A. Tuor, S. Kaplan, B. Hutchinson, N. Nichols, and S. Robinson, "Deep learning for unsupervised insider threat detection in structured cybersecurity data streams," in Artificial Intelligence for Cybersecurity Workshop at AAAI, 2017.

[20]. Symantec, 2018. APT28: New Espionage Operations Target Military and Government Organizations, 18 Feb 2019.

[21]. Mirea, M., V. Wang, and J. Jung. 2019. The not so dark side of the darknet: A qualitative study. *Security Journal* 32: 102–118.

[22]. Chen, W., et al. 2017. CloudBot: Advanced mobile Botnets using ubiquitous cloud technologies. *Pervasive and Mobile Computing* 41: 270–285.

[23]. Manoj Rameshchandra Thakur, Divye Raj Khilnani, Kushagra Gupta, Sandeep Jain, and Vineet Agarwal, Detection and Prevention of Botnets and malware in an enterprise network, International Journal of Wireless and Mobile Computing · May 2012.

[24]. An Approach to Secure Software Defined Network against Botnet Attack November 2019 Journal of Physics Conference Series 1362:01212.

[25]. Botnet detection using software-defined networking, 22nd International Conference on Telecommunications, June 2015.

[26]. Shang-Chiuan Su,[1] Yi-Ren Chen,[1] Shi-Chun Tsai,[1] and Yi-Bing Lin Detecting P2P Botnet in Software Defined Networks, Security and Communication Networks, Volume 2018

[27]. Baldwin, R., Cave, M., & Lodge, M. (2010). Introduction: Regulation–The field and developing agenda. Dans R. Baldwin, M. Cave & M. Lodge (Éds.), *The Oxford handbook of the regulation* (pp. 3-16). Oxford: Oxford University Press.

[28]. Abdelrahman, O.H., E. Gelenbe, G. Görbil, and B. Oaklander, "Mobile Network Anomaly Detection and Mitigation: The NEMESYS Approach," Information Sciences and Systems 2013 Lecture Notes in Electrical Engineering, vol. 264, pp.429-438, 2013.

[29]. Abdullah Al Hasib, "Threats of Online Social Networks", IJCSNS, Vol. 9, No 11, November 2009

[30]. THREATS STATISTICS, Malware, Incidents Web and Network Threats, McAfee Labs Threats Report, March 2018.

[31]. IBM Security, releases the IBM X-Force Threat Intelligence Index, 2019.

[32]. IBM Security, releases the IBM X-Force Threat Intelligence Index, 2020

[33]. Mahmoud, M., Nir, M., & Matrawy, A. (2015). A Survey on Botnet Architectures, Detection, and Defences. IJ Network Security, 17(3), 264-281.

[34]. PENG, T., LECKIE, C., AND RAMAMOHANARAO, K. Survey of network-based defense mechanisms countering the dos and DDoS problems. ACM Comput. Surv. 39, 1 (Apr. 2007).

[35]. ROBINSON, M., MIRKOVIC, J., MICHEL, S., SCHNAIDER, M., AND REIHER, P. Defcom: defensive cooperative overlay mesh. In Proceedings DARPA Information Survivability Conference and Exposition (April 2003), vol. 2, pp. 101–102 vol.2.

[36]. SAHAY, R., BLANC, G., ZHANG, Z., AND DEBAR, H. Towards autonomic DDoS mitigation using software-defined networking. In SENT 2015: NDSS Workshop on Security of Emerging Networking Technologies (2015), Internet society.

[37]. SATYANARAYANAN, M. A brief history of cloud offload: A personal journey from the odyssey

through cyber foraging to cloudlets. GetMobile: Mobile Comp. and Comm. 18, 4 (Jan. 2015), 19–23.

[38]. SEKAR, V., DUFFIELD, N. G., SPATSCHECK, O., VAN DER MERWE, J. E., AND ZHANG, H. Lads: Large-scale automated DDoS detection system. In USENIX Annual Technical Conference, General Track (2006), pp. 171–184.

[39]. SITARAMAN, R. K., KASBEKAR, M., LICHTENSTEIN, W., AND JAIN, M. Overlay networks: An akamai perspective. Advanced Content Delivery, Streaming, and Cloud Services 51, 4 (2014), 305–328.

[40]. WANG, Y.-P. E., LIN, X., ADHIKARY, A., GROÌ´LVLEN, A., SUI, Y., BLANKENSHIP, Y., BERGMAN, J., AND RAZAGHI, H. S. A Primer on 3GPP Narrowband Internet of Things (NBIoT). In arxiv.org (2016).

[41]. Da-Wen Huang, 1 Lu-Xing Yang, 2 Xiaofan Yang, 1 Xiang Zhong, 1 and Yuan Yan Tang 3 Evaluating the Performance of a Static Patching Strategy against Computer Viruses, Hindawi, Volume 2020 |Article ID 9408942

[42]. ZARGAR, S. T., JOSHI, J., AND TIPPER, D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Communications Surveys Tutorials 15, 4 (Fourth 2013), 2046–2069.

[43]. G. Nikolic, T. Nikolic, M. Stojcev, B. Petrovic, and G. Jovanovic, "Battery capacity estimation of the wireless sensor node," in *Proceedings of the IEEE 30th International Conference on Microelectronics (MIEL)*, pp. 279–282, IEEE, 2017.

[44]. Farrell, G., Tseloni, A., Mailley, J., & Tilley, N. (2011). The crime drop and the security hypothesis. *Journal of Research on Crime and Delinquency*, *48*(2), 147-175.

[45]. Akamai, "Spike DDoS toolkit," Tech. Rep. 1078, Akamai, Cambridge, Mass, USA, 2014.

[46]. M. J. Bohio, "Analyzing a backdoor/bot for the MIPS platform," Tech. Rep., SANS Institute, 2015.

[47]. Symantec Security Response, ShellShock: All you need to know about the Bash Bug vulnerability, Symantec Blog, 2014.

[48]. Akamai, "Case study: FastDNS infrastructure battles Xor botnet," Tech. Rep., Akamai Technologies, Cambridge, Mass, USA,2015.

[49]. NSFOCUS DDoS Defense Research Lab and Treat Response Center (TRC), "2016 q3 report on DDoS situation and trends," Tech. Rep., NSFOCUS, Inc., 2016.