2nd National Conference on Recent Innovation in Engineering, Science, Humanities and Management
REVA University, Yelahanka, Bangalore, (India)
29th-30th March 2019 www.conferenceworld.in ISBN : 978-93-87793-79-8

AN EMPIRICAL STUDY ON CYBER SECURITY THREATS AND ATTACKS

R. Sri Devi [1]

(Computer Science, Karpagam Academy of Higher Education, Coimbatore, India)

Dr. M. Mohankumar [2]

(Assistant Professor, Department of CS,CI &IT, Karpagam Academy of Higher Education, Coimbatore, India)

ABSTRACT

Nowadays cyberspace is facing various types of cyber threats and attacks. Cyber security is concerned with making cyberspace safe from cyber threats. Recently, everything has been computerized, with cybernetics using various technologies such as cloud computing, smart phones, Internet of Things techniques, etc. Concerns about privacy, security and economic reimbursement are increasing due to cyber-attacks. The main aim of the hacker is to gain unlawful access to users' computer information, software, intellectual property or basic network. Cyber threats pose a lot of socio-economic, environmental, ethical, national and international problems. This paper provides information about various recent trends in cyber-attacks and the vulnerability of infrastructure based on various research articles.

Keywords: Cyber Espionage, Cyber Security, Key Loggers, Persistent Threat, Ransomware

1. Introduction

Cybercrime is not a new phenomenon. Lack of information security gives rise to cybercrimes.

India is the fourth highest Internet user in the world [29]. Due to the development of new technologies in cyberspace, the users depend more on internet for their daily activities and become more vulnerable too to all kinds of cyber-attacks [22]. In April 2017, G7 Ministerial Conference requested all countries to observe laws and show mutual respect for other countries using ICT devices, declaring cyber security the national responsibility of every country.

Cyber security means protection of information, computer devices, computer resources, hardware, software, network and communication devices from any unofficial access as well as from destruction. [28]. The cyber threats evolved as viruses in the year 1990, grew as worms in a decade, metamorphosed into threats such as botnets, Advanced Persistent Threat, Insider attack and so on.

Now there are entirely new types of problems because of the progress brought about by modern technology. Cyber extortion is a threat by attackers who hijack some confidential documents that they use to blackmail someone demanding money. For example, Panama Papers hack, managed to leak11.5 million secret documents

ISBN : 978-93-87793-79-8

that had monetary and attorney client information for more than 214,488 offshore organizations. Also, Car Hacking remains a real threat. [31] The attackers could take over the control of a full system and hack applications by identifying weaknesses in the application security like, for example, SQL Injections, brute force attack, etc. To secure a computer system from the attackers, it is very much essential to understand thoroughly various threats and attacks.

This paper discusses major cyber security problems such as Malware attacks, Dos /DDos attacks, Data theft, Cyber Espionage, Botnets and insider threat attack are the new scenario manifest in the cyber world. [22]

The remaining of this paper is arranged as follows: Section 2 focuses on recent trends in cyber-attacks, Section 3 the vulnerability of critical infrastructure and Section 4 presents conclusions.

2. Recent Trends in Cyber attacks

The advent of new technologies also brings with it many dangerous forms of cyber-attacks [21]. This paper deals with recent threats such as Ransomware, Advanced Persistent Threat, Insider Threat, Malware and Botnets.

2.1 Malware

Malware is one of the major security threats and the most terrible one being faced bythe Internet users today. Malware is a software designed to cause damage to client, server, computer system or network,without the owner's knowledge or consent. Malware can be arranged as computer viruses, Trojan Horses, Rootkits, Botnets, Key loggers, Backdoors and Spyware. [28]

- Wanping *et al*.[23] have elaborated on the effect of malicious code on network topology and developed a novel high dimensional compartment-based model by a node-based approach without assuming homogenous connectivity network, and concluded that malware couldbe controlled by a proper adjustment of the network.

2.2 Ransomware

Ransomware, as a service, is a new trend nowadays. Ransomware is a malicious software that was first identified in 1989[32]. There were 500,000 malicious applications in the year 2013, increasing to 2.5 million in 2015,3.5 million in 2017 and 77 percent of the applications now [31].The attacker demands from the organizations a ransom for his refurbishment to get access to computer system or recovery of information. The recent rise of ransomware is mainly due to digital coins [21].

- Nikki Spence *et al*.[1] from a literature review study contend that ransomware incidents have been increasing in healthcare as well as industry, and concluded that it is necessary to develop a proper disaster recovery plan.
- SmrutiSaxena [18] talks of ransomware analysis and crypto-locker. The prevention and ransomware removal techniques are explained at the end of the paper, which concludes that ransomware being a big malware, preventive measure and effective techniques must be developed against it.

ISBN : 978-93-87793-79-8

2.3 Cyber Espionage

Cyber espionage is an international problem in today's world. Cyber espionage is stealing confidential information from individuals and military or government organisations without their knowledge through techniques such as cracking techniques, use of proxy servers and malicious software.

- Taein Kang *et al*. [16] have used a DMOS (Deep Mobile OS Security) technique to enhance operating system security for secure computing on the android platform mobile devices. This ability is applied to systems and devices operated on the Android OS, and this method is more helpful to check security risks.

2.4 Advanced Persistent Threat

An advanced persistent threat (APT) is a furtive network attack, and organised hackers use Advanced persistent Threat (APT) attacks to steal confidential data of offices, national defence forces and businesses. The aim of APT is to maintain a long term foothold on the network [33].

- Yuan Yan Tanget *et al*. [27] have proposed a dynamic Generic Secure Compromised Secure (GSCS) model and suggested equilibrium security for security purpose. The limitation in equilibrium affects the network topology, the prevention resources and the quantity of the defence mechanism.
- Micro Marchetti *et al*. [34] have focussed on an innovative approach to analyze systematized high volumes of network traffic on data exfiltrations, other suspected APT activities and applied their analyses on a small set of hosts.

2.5 Insider Threat

The insider threat is a malicious threat that happens inside the organisation from the insider, and misuses the systems with authorized access.

- Sara Khanchi *et al*.[15] have employed for the detection of insider threats' applications of Linear genetic programming(LGP) and stream-active learning. Decision tree and Bayesian based algorithm is used for the study.

2.6 Botnet

Botnet is a group of computers that takes control of each internet-connected devices to carry out distributed denial of service (DDOS) attack, send spam and hackers to sabotage the connection and devices.

- Andrea Oliveri *et al*. [25] have proposed a modular structure architecture and used sagishi in the active honeypot concept, which can be helpful to identify malware.
- Bock *et al*.[24] use a Trust-based Botnet Monitoring Countermeasure (Trust Bot MC) mechanism to observe activity, and a computational trust model is used for tracking technique.

3. Vulnerabilities in Critical Infrastructure

Cybercrime involves massive and coordinated attacks against the information infrastructure of a country. The information and communication technologies perform an essential role in the Next Generation Networks (NGN) and are more vulnerable to cyber-attacks [20]. Attackers would look to exploit the vulnerability in the networks

ISBN : 978-93-87793-79-8

most often because the networks are not adequately protected in processing large data and havevarious issues in the network.

- Kai Yang *et al.* [12] have recommended a suitable approach to generate finger prints of IoT devices, used neural network to generate finger prints and explored the implementation of three different protocols such as transport layer, application layer and network layer.
- Gupta *et al*.[14] have studied the vulnerability in the existing ICT infrastructure.
- Margus Valja [17] has studied the weakness and vulnerability of software, security, cryptographic problems and programming errors running on industrial embedded power system.
- Schneidewind [3]has adopted a technical approach to find system vulnerability in the internet by cyber-attack in US critical infrastructure, used code-scanning tools to prevent unauthorized access, and user authentication to prevent critical infrastructure cryptography.
- Ling Li *et al*. [4] have suggested a method for protecting organization information security using Protection Motivation Theory (PMT) framework, which is related to self-reported cyber security protection action on the part of the employee.
- White G.B [5] has used three tools and developed Community Cyber Security Maturity Model (CCSMM) to address national cyber security issues.
- Martino Trevisan *et al*. [13] have developed 'Coupling Privacy with Safety (CPS) and maintained Quality of Service of Vehicular Ad-hoc Networks (VANETs), which also provide protection and safety against three types of attacks. Its limitation is that in an emergency situation CPS has no signature verification.
- Anan Sajid *et al* [19] have analysed some important information about SCADA systems with vulnerability, threats and management in IOT and cloud computing. The problem here is that the data stored on servers for sharing and backing up are managed by a third party.
- Armstrong Nhlabatsi *et al*.[10] recommend STRIDE threat model and threat identification model and also mapped the attacks to the cloud components and their associated vulnerability, using tracing method for identifying the malware in the cloud. Mapping approach is used in open Web Application Security Project (OWASP) attack.
- Enrico Cambiaso*et al.* [11] have proposed a slow DoS threat attack in application servers which is a malware attack both in wireless and wired connections from Microsoft IIS. They conducted wired network test in WAN network, Internet Network and Lan Network and wireless network test in WIFI network, 4G/LTE network and 3G/HSPA network.

4.Conclusion

In this paper various forms of cyber security menace and vulnerability in critical infrastructure are discussed. The number of cyber-attacks and threats has increased substantially in recent years, and hackers go after individuals, groups, businesses and government to steal critical IP and national secrets. The threats are getting bigger and affecting people, hardware, software, applications and networks. Cybercrime can affect the stability

ISBN : 978-93-87793-79-8

of a nation. It is important to understand that most situations need balancing the various security methods used, goals, their efficiency and their effectiveness in the detection, prevention, or reaction to, their possible side effects. Security policy, network monitoring and mechanisms for mitigating threats are important in protecting the world from cyber-attack. Cyber-security is an important tool in preventing, and protecting from, unauthorized surveillance.The purpose of the paper is to provide a substantial basis for further research in this area.

References

[1] Spence, N., Bhardwaj, N., Paul III, D. P., &Coustasse, A. (2018). Ransomware in Healthcare Facilities: A Harbinger of the Future?. *Perspectives in Health Information Management*.

[2] Yang, L. X., Li, P., Yang, X., Wen, L., Wu, Y., & Tang, Y. Y. (2017). Security evaluation of cyber networks under advanced persistent threats. *arXiv preprint arXiv:1707.03611*.

[3] Schneidewind, N. (2010). Metrics for mitigating cybersecurity threats to networks. *IEEE Internet Computing*, *14*(1).

[4] Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13-24.

[5] White, G. B. (2011, November). The community cyber security maturity model.In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on* (pp. 173-178).IEEE.

[6] Span, M. T., Mailloux, L. O., Grimaila, M. R., & Young, W. B. (2018, June). A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE.

[7] Smith, M. D., &Paté-Cornell, M. E. (2018). Cyber Risk Analysis for a Smart Grid: How Smart is Smart Enough? A Multiarmed Bandit Approach to Cyber Security Investment. *IEEE Transactions on Engineering Management*.

[8] Wortman, P. A., Tehranipoor, F., &Chandy, J. A. (2018, June). An Adversarial Risk-based Approach for Network Architecture Security Modeling and Design. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE.

[9] Zhou, H., Wu, C., Yang, C., Wang, P., Yang, Q., Lu, Z., & Cheng, Q. (2018). SDN-RDCD: A Real-Time and Reliable Method for Detecting Compromised SDN Devices. *IEEE/ACM Transactions on Networking (TON)*, *26*(5), 2048-2061.

[10] Hong, J. B., Nhlabatsi, A., Kim, D. S., Hussein, A., Fetais, N., & Khan, K. M. (2019). Systematic identification of threats in the cloud: A Survey. *Computer Networks*, *150*, 46-69.

[11] Cambiaso, E., Chiola, G., & Aiello, M. (2019). Introducing the SlowDrop Attack. *Computer Networks*.

[12] Yang, K., Li, Q., & Sun, L. (2018). Towards automatic fingerprinting of IoT devices in the cyberspace. *Computer Networks*.

ISBN : 978-93-87793-79-8

[13] Trevisan, M., Drago, I., &Mellia, M. (2019). PAIN: A Passive Web performance indicator for ISPs. *Computer Networks*, *149*, 115-126.

[14] Chaturvedi, M. M., Gupta, M. P., & Bhattacharya, J. (2008). Cyber Security Infrastructure in India: A Study. *Emerging Technologies in E-Government ', CSI Publication*.

[15] Le, D. C., Khanchi, S., Zincir-Heywood, A. N., & Heywood, M. I. (2018, July). Benchmarking evolutionary computation approaches to insider threat detection. In *Proceedings of the Genetic and Evolutionary Computation Conference* (pp. 1286-1293).ACM.

[16] Lee, S., Lee, S., Kang, T., Kwon, M., Lee, N., & Kim, H. (2018). Resiliency of mobile OS security for secure personal ubiquitous computing. *Personal and Ubiquitous Computing*, *22*(1), 23-34.

[17] Välja, M., Korman, M., &Lagerström, R. (2017, April). A Study on Software Vulnerabilities and Weaknesses of Embedded Systems in Power Networks.In *Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids* (pp. 47-52).ACM.

[18] Saxena, S., &Soni, H. K. (2018, February). Strategies for Ransomware Removal and Prevention.In *2018 Fourth International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB)* (pp. 1-4).IEEE.

[19] Sajid, A., Abbas, H., &Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access*, *4*, 1375-1384.

[20] Gandotra, E., Bansal, D., &Sofat, S. (2014). Malware analysis and classification: A survey. *Journal of Information Security*, *5*(02), 56.

[21] Bailey, M., Cooke, E., Jahanian, F., Xu, Y., &Karir, M. (2009, March). A survey of botnet technology and defenses. In *Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology* (pp. 299-304). IEEE.

[22] Nazir, S., Teperi, A. M., &Polak-Sopińska, A. (Eds.). (2018). *Advances in Human Factors in Training, Education, and Learning Sciences: Proceedings of the AHFE 2018 International Conference on Human Factors in Training, Education, and Learning Sciences, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA* (Vol. 785). Springer.

[23] Liu, W., &Zhong, S. (2018). Modeling and analyzing the dynamic spreading of epidemic malware by a network eigenvalue method. *Applied Mathematical Modelling*, *63*, 491-507.

[24] Böck, L., Vasilomanolakis, E., Wolf, J. H., &Mühlhuser, M. (2019). Autonomously Detecting Sensors in Fully Distributed Botnets. *Computers & Security*.

[25] Oliveri, A., &Lauria, F. (2019). Sagishi: an undercover software agent for infiltrating IoT botnets. *Network Security*, *2019*(1), 9-14.

[26] Libicki, M. C. (2018, May). Drawing inferences from cyber espionage.In *2018 10th International Conference on Cyber Conflict (CyCon)* (pp. 109-122).IEEE.

[27] Yang, L. X., Li, P., Yang, X., Wen, L., Wu, Y., & Tang, Y. Y. (2017). Security evaluation of cyber networks under advanced persistent threats. *arXiv preprint arXiv:1707.03611*.

ISBN : 978-93-87793-79-8

[28] Godbole, N., &Belapure, S. (2011). Cyber Security, Understanding Computer Forensics and Legal Perspectives.

[29] INDIA's Cyber Security Challenges, IDSA Task Force Report March 2012

[30] http://dst.gov.in/basic-research-cyber-security

[31] cyber security issues . docx

[32] https://www.globalsign.com/en-in/blog/cybersecurity-trends-and-challenges-2018/

[33] Sood, A. K., &Enbody, R. J. (2013). Targeted cyberattacks: a superset of advanced persistent threats. *IEEE security & privacy*, *11*(1), 54-61.

[34] Marchetti, M., Pierazzi, F., Colajanni, M., & Guido, A. (2016). Analysis of high volumes of network traffic for Advanced Persistent Threat detection. *Computer Networks*, *109*, 127-141.