BOOK CHAPTER | Cyber Threats Anthologies

Anthologies of Major Threats in Cyberspaces

Iwayemi, A.[1] & Adebayo, S. O.[2]
[1]Department of Computer Engineering, The Federal Polytechnic, Ile-Oluji, Nigeria
[2]Dept of Computer Engineering Technology, Guru Nanak Dev University, Amritsar, India
E-mails: [1]iwayemiresearch@gmail.com; [2]suadey1@gmail.com
Phone: [1]+234-8034126840; [2]+234-8133837468

Abstract

Cyberspace is the digital technological environment in which computers, electronic equipment, and internet-of-things devices are interconnected online for communication and sharing of resources. It facilitates the quick sharing of data and information among persons and devices without physical transportation and delays. However, this high-tech solution did not surface without some challenges such as threats against the connected devices, the network of interconnectivity, and the shared data and information. This article presents ten major threats in the cyberspace. A review of relevant literature was conducted and a meta-analysis table comprising the name of each of the ten major threats, the sources of each of the threats, its intended goal, effects on systems, the examples or types, what is at risk by each threat, and possible solutions of the threats were presented. The result of the review shows that major cyber threats are targeted against confidential data and information in a bit to break their confidentiality, gain access control, steal them, and demand/steal funds. In conclusion, the enlightenment of internet users, use of upgraded security systems, security of networks, improved security schemes such as very strong passwords, multiple security questions, captchas, and multiple authentications are major ways to prevent most of the software and network-related threats while the use of protectors, padlocks, gates, extinguishers, restrictions, and detectors are useful in the physical security of the infrastructures.

Keywords: Cybersecurity, HTTPS, DNS, Malware Attack, Cyberspace

Introduction

In today's world, companies and organizations are competing to transform their businesses to an online and more scalable state. Cyber-attack is one of the major setbacks to this approach as many companies suffer severe losses due to identity theft, lawsuits, among other damages caused by cyber-attack. Individuals, organizations, and governments regularly fall victim to cyber-attacks. This has put cyber security in an important position for companies to consider before moving and maintaining their businesses online. The exponential increase in the use of the internet and cyberspace has resulted in to increase in cybercrime activities (Humayun et al., 2020). Cyberspace is being facilitated by the internet and web applications. Attackers exploit vulnerabilities of these systems to perform a coordinated attack and gain illegal access to the systems (Li et al., 2016).

Citation: Iwayemi, A. & Adebayo, S. O. (2022):). Anthology of Major Threats in Cyberspaces. SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series Book Chapter on Web of Deceit - African Multistakeholders' Perspective on Online Safety and Associated Correlates Using Multi-Throng Theoretical, Review, Empirical and Design Approaches. Pp 167 -172. www.isteams.net/bookchapter2022. DOI https://doi.org/ 10.22624/AIMS/BK2022-P28

The impacts of these attacks range from data leaks which can include sensitive personal information to interruptions of critical infrastructure operations (Khandpur et al., 2017).

Cyber Security

Cybersecurity defines the body of processes, technologies, and training that are designed to protect systems, networks, programs, and data from cyberattacks, damages, and unauthorized access (Alhayani et al., 2021). It can also be said to be the ability of a computer system or program to resist any action that compromises the confidentiality, integrity, or authenticity of the available information in the system. In other words, cyber security is used to achieve Confidentiality, Integrity, and Availability (CIA) as depicted in Figure 1.

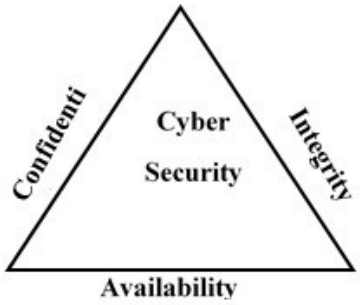

Fig 1: The Cyber Security Triad Model

Cyberattack

A cyberattack is an attempt to gain unauthorized access to hardware, software, processed or stored data, and network to cause damage or harm. The attackers simply exploit any loopholes or vulnerabilities through any digitally connected devices or entities. They can steal information, publicly display private information, stop vital business operations among other harms that can be caused. For each successful cyberattack, there is an interruption of people's activities, technology, or processes (Požár, 2019).

Cyber Security Threats

A threat is any operation that exploits security loopholes in a system and results in a negative impact (Brauch, 2011). As the world is going digital and more operations are being carried out in cyberspace, cyberspace has become an easy target for attackers and several threats are emerging in the space. Threats can be as a result of human action or as due to natural occurrences such as earthquakes, floods, volcanic eruptions, and Tsunami (Abomhara and Koien, 2015). Good disaster recovery and contingency plans will be enough to mitigate natural threats (Abomhara and Koien, 2015). Physical threats on the other hand are caused by human actions. Major physical threats are presented in Figure 2.

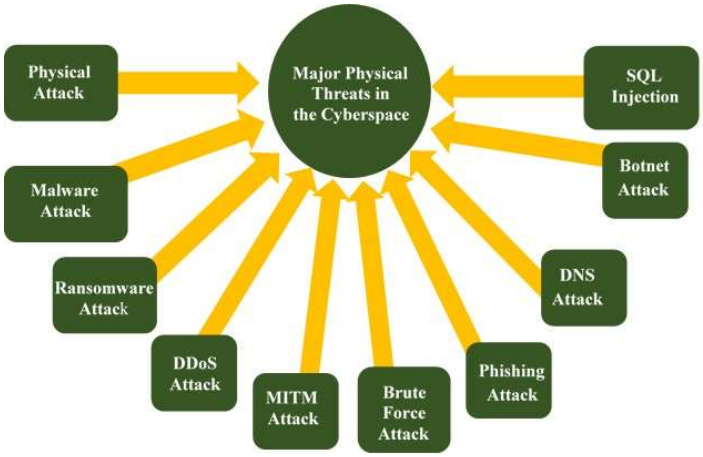

Figure 2: Major Physical Threats in the Cyberspace

Physical Attack

A physical attack is an attack performed on hardware infrastructure. This is often caused by an employee who has access to the data center premises or by a breach in the physical security of the premises.

Malware Attack

Malware is an abbreviated version of "malicious software" that is designed to harm or destroy a computer system. Malware includes ransomware, viruses, bots, trojans, worms, et cetera. This software can be installed to the system through various means including an authorized user clicking on dangerous links or emails.

Ransomware Attack

Ransomware is a malicious software virus that hijacks access to vital information and demands payment from the victims to get access to the information (Humayun et al., 2021). This data will be encrypted and the hackers will request a specific ransom payment (usually in form of cryptocurrency) to release the decryption keys. Scareware, Screen lockers, and Encrypting ransomware are three types of ransomwares (Kagita et al., 2020). Harmful consequences of ransomware include loss of sensitive data, loss of productivity, data destruction, and loss of reputation and business downtime (Humayun et al., 2021).

DDoS Attack

Distributed Denial of Services (DDoS) is an attack created without the intention of stealing data but to deny authorized users access to the resources. This is achieved by intentionally flooding the system (network, compute resource, server, database…) with fake traffic to overwhelm the capacities of the service and thereby resulting in a denial of services to authentic users.

MITM Attack

A Man-In-The-Middle attack occurs when an attacker position himself between two communicating systems either to eavesdrop or impersonate one of the parties and make the communication appears normal. Seven types of MITM attacks are IP spoofing, DNS spoofing, HTTPS spoofing, SSL hijacking, Email hijacking, Wi-Fi eavesdropping, and Stealing browser cookies (Kagita et al., 2020).

Brute Force Attack

In a brute force attack, the attacker uses many trial-and-error to guess the login information of an authorized user, to detect encryption keys or hidden web pages. The perpetrator uses password hashing or password cracker software to hit the server with the possible tries until the correct credentials are obtained (Kagita et al., 2020).

Phishing Attack
Phishing is the method by which a perpetrator attempts to obtain confidential information from the user to use it fraudulently (Benavides et al., 2020). The attackers send fraudulent messages (that seem to come from a trustworthy source) to the user and trick them to reveal sensitive information.

DNS Attack
Domain Name System (DNS) attack is simply exploiting the vulnerabilities in the DNS or trying to compromise the network's DNS.

Botnet Attack
Botnets are tiny bots otherwise known as a group of malicious codes that can hinder the whole security system without the knowledge of the user (Majumdar et al., 2021). Botnet attacks are common in IoT devices. The aim is of a botnet attack is to collapse as much as IoT devices as possible and gain access to the important information of a target system (Majumdar et al., 2021).

SQL Injection
SQL injection is a technique that exploits the security vulnerabilities at the database layer of a web application (Farooq, 2021). It extracts the content of the databases without the proper permission to do so. The attackers supply certain SQL statements instead of a user input and in return get access to database information that was not intended to be displayed.

Review of the Major Cyber Threats
A meta-analysis of the major threats in the cyberspace is presented in Table 1. Ten major threats, with some of their major sources; the medium through which they attack; the effects of their attack; examples or types of the threat; risks associated with such attack; and possible preventions or solutions to the attack are presented in the table.

Table 1: Major Threats in the Cyber Space

N	Threats	Source	Goal	Medium of Attack	Effects	Examples	Risks	Solution
1	Physical Attack	Employees, intruders, or human thieves	Destruction or theft of cyber infrastructure	Physical by humans, robots, or use of explosives	Destruction and loss of data, resources, jobs, and finances	Setting a network router on fire or carting away with it.	Data, and Infrastructure.	Protection, Padlocks, Gates, Extinguisher, restrictions, detectors, and so on
2	Malware Attack	Dangerous links or emails	Harm or destroy a computer system	Software	Theft of private information, reduced efficiency of systems	Viruses, worms, Trojan, spyware, and so on	Data, information, and efficiency	Anti-malware
3	Ransomware Attack	Hackers	Hijack access to vital information and demand for ransom	Software	Loss of sensitive data, reputation, productivity, data destruction, and 4business downtime	Scareware, Screen lockers, and Encrypting	Sensitive data, reputation	Backups, Pay the ransom, increase in security
4	DDoS Attack	Hackers	Deny authorized users access to their resources	Software, network, attack from multiple locations	Authorized users are denied access to the system	Protocol, volumetric, application attack	Network, compute resource, server, database	Anti-DDOS, Reliable hosting, cloud

N	Threats	Source	Goal	Medium of Attack	Effects	Examples	Risks	Solution
5	MITM Attack	Hackers	Eavesdropping or impersonation in a network	Software, network, communication medium	Theft of private information such as login details, passwords, etc	Spoofing: IP, DNS, and HTTPS; SSL hijacking; Email hijacking; Wi-Fi eavesdropping; and Stealing browser cookies	Confidential information	Improved security systems such as VPN, HTTPS (as against HTTP), etc
6	Brute Force Attack	Hackers cyber criminals	To gain illegal access to information	Guessing or trial-and-error Software, network	Theft of private information such as login details, passwords, etc	Password guesser, botnets, dictionary attacks, etc	Data, server, financial resources associated with data	Improved security systems such as strong passwords, security questions, captchas, multiple authentications, etc
7	Phishing Attack	Hackers, cyber criminals	To steal sensitive information through deceit	Software, emails, websites, network	Loss of data, resources, and funds; deceived into unintended actions	Vishing, spear, email, whaling, etc	Confidential Data, financial resources, opportunities, etc	Vigilance, awareness, use HTTPS (against HTTP) security upgrades
8	DNS Attack	Hackers	To compromise the network's DNS.	Software, Network.	Loss of Funds, loss of reputation	Domain, DNS food, DNS Hijack, Cache poisoning, DNS tunneling, etc	Data, business, network	Internet access controls, security of DNS
9	Botnet Attack	Attackers	To collapse as much as IoT devices as possible and gain access to important information	Software, Network.	Theft of private information.	Centralized and Distributed (Yimu & Shangdong, 2019)	Data, server, funds, resources, IoT devices.	Improved security of IoT devices, Cryptography, vigilance, and awareness
10	SQL Injection	Attackers	To get access to database information	SQL, Software, Network	Loss of data, illegal alterations of data	Retrieving hidden data, Subverting, Union attack, etc	Databases	Security of databases

Conclusion

The increase in cyber-attacks is mainly due to the increase of enormous valuable information hosted in the cyber-space. Cyber threats are expected to keep increasing as new technologies are deployed. In recent years, cyber-attacks are growing rapidly in each domain of life targeting individuals, government, and organizations. Cyber threats will continue to grow as hackers will keep on seeking vulnerabilities in new software, applications, and facilities.

Cyberspace users should be protected by appropriate security measures when interacting with the space, use updated security software and application, and most importantly be properly educated on best practices, different possible attacks, and how to mitigate them. Companies should create continuous training and awareness for their employees and contractors to ensure safety in cyberspace.

The use of upgraded security systems, improved security schemes such as very strong passwords, multiple security questions, captchas, and multiple authentications are major ways to prevent most of the software and network-related threats while the use of protectors, padlocks, gates, extinguishers, restrictions, ad detectors are useful in the physical security of the cyberinfrastructures.

References

1. Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. *Journal of Cyber Security and Mobility*, 65-88.
2. Alhayani, B., Abbas, S. T., Khutar, D. Z., & Mohammed, H. J. (2021). Best ways computation intelligent of face cyber attacks. *Materials Today: Proceedings*.
3. Benavides, E., Fuertes, W., Sanchez, S., & Sanchez, M. (2020). Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review. *Developments and advances in defense and security*, 51-64.
4. Brauch, H. G. (2011). Concepts of security threats, challenges, vulnerabilities and risks. In *Coping with global environmental change, disasters and security* (pp. 61-106). Springer, Berlin, Heidelberg.
5. Farooq, U. (2021). Ensemble Machine Learning Approaches for Detection of SQL Injection Attack. *Tehnički glasnik*, *15*(1), 112-120.
6. Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021). Internet of things and ransomware: Evolution, mitigation and prevention. *Egyptian Informatics Journal*, *22*(1), 105-117.
7. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*(4), 3171-3189.
8. Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2020). A review on cyber crimes on the Internet of Things. *arXiv preprint arXiv:2009.05708*.
9. Khandpur, R. P., Ji, T., Jan, S., Wang, G., Lu, C. T., & Ramakrishnan, N. (2017, November). Crowdsourcing cybersecurity: Cyber attack detection using social media. In *Proceedings of the 2017 ACM on Conference on Inf. and Knowledge Management* (pp. 1049-1057).
10. Li, Z., Zou, D., Xu, S., Jin, H., Qi, H., & Hu, J. (2016, December). Vulpecker: an automated vulnerability detection system based on code similarity analysis. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (pp. 201-213).
11. Majumdar, P., Singh, A., Pandey, A., & Chaudhary, P. (2021). A Deep Learning Approach Against Botnet Attacks to Reduce the Interference Problem of IoT. In *Intelligent Computing and Applications* (pp. 645-655). Springer, Singapore.
12. Požár, J. Cyber Attacks on Critical Information Infrastructure: Definitions, Threats and the Czech Perspective. *Security in Central and Eastern Europe: Cyberspace, Police, Prisons, Transport, Addictions, the Media*, 65.
13. Yimu, J. and Hangdong, L. (October 1st 2019). Threats from Botnets, Computer Security Threats, Ciza Thomas, Paula Fraga-Lamas and Tiago M. Fernández-Caramés, IntechOpen, DOI: 10.5772/intechopen.88927. Available from: https://www.intechopen.com/chapters/69332