Cyber-attack and Measuring its Risk

Mihret Sheleme[1], R. Rajesh Sharma[2]

[1]Student, Computer Science and Engineering, Adama Science and Technology University, Adama, Ethiopia
[2]Assistant Professor, Adama Science and Technology University, Adama, Ethiopia

E-mail: [1]mihretsheleme2016@gmail.com, [2]sharmaphd10@gmail.com

Abstract

In this short research, cyber-attack and the well-known attacking methods are discussed. Moreover, how many attacks were made in 2021 compared to the attacks in the previous year is found, to determine how fast this malicious activity is growing and the reasons which motivate such cyber-attacks are studied. The risk measurement methods are also discussed in this article based on some previous research. The conclusions are made on the suitable solution for cyber-attack, reviewed based on the point of view of different research.

Keyword: Cyber-attacks, malicious, risk, vulnerability

1. Introduction

Nowadays, different communication technologies being invented with the data sharing and data storing activity on the internet, on the cloud, on database and on different devices are increasing. As the information stored on the internet, cloud, and different devices gets increased, the cyber-attack is growing to be a very serious and more dangerous global issue [1, 2].

Cyber-attacks are evil activities performed to steal, expose, corrupt, alter, damage or destroy information through unauthorized access to the computer system or is an assault launched by attackers which use single or multiple computers to attack other computers and networks [3, 4]. Cyber-attacks can be considered as cyber terrorism, like hacktivists.

Cyber-attacks are done for different reasons that can be categorized into three main reasons: criminal, political and personal. Hackers who possess criminal mind seeking financial gain through money theft, data theft, or business disruption are categorized into criminal cyber-

DOI: https://doi.org/10.36548/jsws.2021.4.002
Received: 09.11.2021, received in revised form: 26.11.2021, accepted: 18.12.2021, published: 29.12.2021

attack. Sometimes disgruntled current or former employees, steal money to disrupt a company's system and those hackers are personally motivated attackers. Even if some hackers seek retribution, socio-political motivated attackers seek attention for their causes, and as a result, they try to make their attacks known to the public, which is also known as hacktivism [5, 6].

1.1 How many cyber-attacks happened in 2021?

The data breaches through the year till 30 September 2021, exceeded the breaches happened in the year of 2020 by 17 percent. According to cyber-attack statistics studied in 2021;

- Globally, 30,000 websites are hacked daily.
- 64% of companies experienced different kinds of cyber-attack.
- Around 20M breaches have happened in March 2021.
- Ransomware cases have grown by 150% in 2020.
- Around 94% of malwares were through email.
- Attackers try to breach a system every 39 seconds somewhere on the web.
- An average of around 24,000 malicious mobile apps are blocked daily on the internet.

1.2 There are several types of cyber-attacks as follows:

A. Phishing attack

Phishing is an attack by sending a fraudulent message designed to trick a victim into revealing sensitive information to the penetrator or deploy malicious software on the computer or the network infrastructure like ransomware [7].

B. Man-in-the-middle (MITM) attack

It is an active wiretapping attack in which the attacker intercepts the system and selectively modifies the communicated data, alter the data in the middle and hence called the man in the middle [8].

C. Denial-of-service (DOS) attack

A denial-of-service attack is the type of attack in which the attacker makes the network resources or the machine unavailable and inaccessible for the authorized user, temporarily or indefinitely [9].

D. SOL injections

This type of attack is a common attack that works by injecting a malicious SQL code to the backend database and manipulate the information that was not intended to be displayed. This attack allows attackers to steal items, sensitive company data, user lists or private customer detail [10].

E. Zero-day exploit

A zero-day attacker, exploits the vulnerability contained by computer system, which is unknown or known to those who are interested in its mitigation and a patch has not been yet developed. Until the vulnerability is known and mitigated, those attackers can exploit it maliciously using the resources, and affect programs, data, other computers or a network [11].

F. Password attack

A password attacker use any method to steal the password of the system or to maliciously authenticate into password-protected accounts. These attackers may use softwares that expedites cracking or guessing passwords [13].

G. Cross-site scripting attack

This is a vulnerability that can be found in web applications. It will inject client-side script into web pages which can be visited by any other user. Attackers use a cross-site scripting vulnerability to bypass access control that has the same origin policy [14].

1.3 The summary of the differences between attacks are mentioned below:

- Phishing sends email or any other links to pretend and penetrate into the victim's system.
- Man-in-the-middle attack (MITM) works by intercepting the system and modifying the data.

- Denial-of-service (DoS) attack deny the user of system from using it.
- SQL injection works by injecting malicious code to the database.
- Zero-day exploit uses the vulnerability of the system for penetrating in.
- Password attack is done by guessing or using any technique to find the password.
- Cross-site scripting attack works by injecting the client-side script into the web.

2. Reviewed research

Every system cannot avoid vulnerabilities completely from their system and that makes way to exploit by adversary (ies) in attempt to disrupt system operations [1,15]. This paper suggests Entropic Value at Risk (EVaR) as a measure of cybersecurity risk. While EVaR gains popularity as a measure of financial risk and has been extended to robust engineering of systems of various types, EVaR application to cybersecurity risk presents new opportunities and challenges. This paper, which is a work in progress, outlines some of them. Analysis of a simple networked system indicates that CyEVaR is a more adequate measure of cybersecurity risk than the conventional measures at least in the case of highly determined and capable attacker.

Cyberspace is an endless space known as the Internet. Computer transactions, especially transactions between different computers, can be viewed as a space [2]. Cybercrime is a series of organized criminal attack cyberspace and cybersecurity. Cybercrime such as hacking into computer, can be done through a network system and clicking on unfamiliar links when connected to unrecognized WiFi, downloading software and files from unsafe sites, consuming energy, electromagnetic radiation waves, and more. Cybercrime types are:

1. Terrorism of Cyber
2. Online Assisted Kidnaping
3. Fraud Identity Theft
4. Internet Pornography
5. Hacking

As many individuals, corporate bodies and government entities rely on ICTs and computer networks to perform simple and complex tasks, cybersecurity should be given serious attention.

Data mining applications can be used to detect future cyber-attacks by analysis, program behavior, browsing habits and so on. Data mining applications are used for threat analysis and detection with special approach for malware detection with high precision and less time [3]. Data mining techniques like classification, SVM, regression, decision tree, graph mining, KNN algorithms can be integrated with anti-threat system that helps to detect malware before it enters the system, hence protects IT infrastructure from further attack.

2.1 The summary of the review

The researchers have agreed that every system cannot avoid its vulnerability completely. The paper [2] has described cybercrime and cyberspace, paper [1] has recommended Entropic Value at Risk (EVaR) as a measure of cybersecurity risk, and paper [3] has explained data mining as an application to prevent future cyber-attack.

3. Comparative analysis

The paper discusses the measurement of cybersecurity risk which were proposed recently. It has explained Entropic Value at Risk (EVaR) as a measure of cybersecurity risk [1, 3]. The work summarizes how future cyber-attack can be avoided by the analysis of program behavior, browsing habits and other features, using data mining applications.

The article analyses cyber-attack as a crime which attack in an organized and series way, cyberspace, and cybersecurity. It explains that if a computer has a picture of a building that allows to walk in and see the nature of design and architecture, then the building is said to be in cyberspace [2].

4. Conclusion

As cyber-attack is a major risk for communication, security to reduce the risk of cyber-attacks using mechanisms like reducing data transfers, download discernment, strong passwords, software updates, monitor data leakage, develop a breach response plan etc., should be strengthened. Moreover, applying the risk measurement techniques provided by researchers and measuring the risk, will help the organizations or any individual to alarm if, when and by

whom attack tries to penetrate the system. This helps to prevent cyber-attack before happening or damage the system by checking the vulnerability hole in the system or in the network.

References

[1] Vladimir Marbukh (2021). Towards Robust Security Risk Metrics for Networked Systems: Work in Progress. International symposium on integrated network management (IEEE), 658-661

[2] Sunil. C. Pawar, Dr. R. S. Mente & Bapu. D. Chendage (2021). Cyber Crime, Cyber Space and Effects of Cyber Crime. International Journal of scientific Research in computer science engineering and information technology (IJSRCSEIT), 7(1), 210-214

[3] Varsha P.Desai Assistant Professor, Dr.K.S.Oza Assistant Professor, Dr.P.G.Naik Professor (2021). Data Mining Approach for Cyber Security. International journal of computer applications technology and research (IJCATR), 10(01), 035-041

[4] Mugunthan, S. R. (2019). Soft computing based autonomous low rate DDOS attack detection and security for cloud computing. J. Soft Comput. Paradig (JSCP), 1(02), 80-90

[5] Vivekanandam, B (2021). Design an Adaptive Hybrid Approach for Genetic Algorithm to Detect Effective Malware Detection in Android Division. Journal of Ubiquitous Computing and Communication Technologies, 3(2), 135-149

[6] Kirubakaran, S. Stewart (2020). Study of Security Mechanisms to Create a Secure Cloud in a Virtual Environment with the Support of Cloud Service Providers. Journal of trends in Computer Science and Smart technology (TCSST), 2(03), 148-154

[7] Manoharan, J. Samuel (2021). A Novel User Layer Cloud Security Model based on Chaotic Arnold Transformation using Fingerprint Biometric Traits. Journal of Innovative Image Processing (JIIP), 3, 36-51

[8] Joe, C. Vijesh, and Jennifer S. Raj (2021). Deniable Authentication Encryption for Privacy Protection using Blockchain. Journal of Artificial Intelligence and Capsule Networks, 3(3), 259-271

[9] Jambhale, Tejas, and M. Sudha (2020/2021). A Privacy Preserving Hybrid Neural-Crypto Computing-Based Image Steganography for Medical Images. In Intelligent Data Communication Technologies and Internet of Things: Proceedings of (ICICI), 57, 277-290

[10] Gautam, Apurv Singh, Yamini Gahlot, and Pooja Kamat (2019). Hacker forum exploit and classification for proactive cyber threat intelligence. In International Conference on Inventive Computation Technologies, 98, 279-285

[11] Banu, S. Aashiq, M. S. Sucharita, Y. Leela Soundarya, Lankipalli Nithya, R. Dhivya, and Amirtharajan Rengarajan (2021). Robust Image Encryption in Transform Domain Using Duo Chaotic Maps—A Secure Communication. In Evolutionary Computing and Mobile Sustainable Networks, 271-281

[12] Saroja Roy Grandhi, Priyanka Kacker (2020). Cybercrime Investigation through BEOS profiling. A global journal of interdisciplinary studies (ISSN), 3(2), 67-72

[13] Reghav Gupta (2021). Effects of Cybercrime in Real Word. International Journal of Research in Science and technology (IJRST), 11(3), 42-48

[14] Rincy Raphael (2019). Various data mining techniques to detect the android malware application: a case study. International journal of new technology and research (IJNTR), 5(6), 65-72

[15] Rupali Komatwar, Manesh Kokare (2020). A survey on malware detection and classification. Journal of Applied Security Research (JASR), 16(12), 1-31.

Author's biography

Mihret Sheleme is from Adama city and a Computer Science and Engineering student at Adama science and technology university, Adama, Ethiopia. Her research interest includes cyber security and web risk analysis.

R. Rajesh Sharma is a Computer Vision and Robotics SIG Coordinator in the department of Computer Science and Engineering in School of Electrical Engineering and Computing in Adama Science and Technology University, Adama, Nazret, Ethiopia. He has more than 8 years of academic experience. His areas of research are networking, probabilistic computing, fuzzy, bio- inspired computing, data visualization, fault diagnosis, robotics, internet of things, neurocomputing, information retrieval, human-machine interface and network security. He has published more than 20 international and national journals. He is a life member of International Association of Engineers and Indian Society of Technical Education, and member of IAENG, IACSIT and AACE.