Journal of Science and Technology
ISSN: 2456-5660 Volume 06,Special Issue 01, August 2021,

www.jst.org.in *DOI: https://doi.org/10.46243/jst.2021.v6.i04.pp312-317*

A Review on Cyber Security and Cyberattacks

G. P. Gawali
Assistant Professor and Head, Department of Computer Science.
R.A.Arts, Shri M.K.Commerce, and Shri S.R.Rathi Science College,
Washim, Maharashtra, India.
gg020988@.com

To Cite this Article
G. P. Gawali*"*A Review on Cyber Security and Cyberattacks*", Journal of Science and Technology, Vol. 06, Special Issue 01, August 2021, pp312-317: .*

Article Info
Received: 15.07.2021 *Revised: 24.07.2021* *Accepted:10.08.2021* *Published: 16.08.2021*

Abstract: *The cybercrimes have become very common and the **c**yber-attack is the buzzword in today's world. Cybercrimes are increasing every hour and the intensity of loss is also increasing rapidly. To provide security to defend cyber-attacks has become more important phenomena in this digital world. Ensuring cyber-security is a verycomplex task, it requires a thorough understanding of the attacks, attackers mind and the capability of analyzing the possibility of threats. The main challenge of cybersecurity is the progressive nature of the attacks. The proposed paper is an attempt to present the importance of cyber-security with associated various risks that are present in the current digital world. The study was done on the different cyber-attacks and the results shows the intensity of these different attacks.In this paper the various cyber-security threats are presented with the MLA (machine learning algorithms) that can be applied to analyze cyber-attacks.*

Keywords*: cyber-security; cyber-attack; machine learning; cybercrime; security; algorithms.*

Introduction:

As a result of increased reliability and the application of the Internet, virtually all the industries, government, and also the financial organizations have switched their transactions on to the cyber platforms. This increases the vulnerability of the cyber system to cyber-attacks. A cyber-attack is a malicious attempt by one person or organization to violate another person's or organization's information system. Cyber-attacks target the commercial organization, the military, the government, or other financial institutions, such as banking services, either to hack protected information or to obtain a ransom.

There is a significant increase in the quantity and knowledge of cyber-attack technologies. It becomes a significant danger to the cyber industry. According to the available data, around 98% of web applications tested were susceptible to cyber-attacks, 90% of the members of the large organizations and 74% of the members of the small organizations were victims of security and data breaches[1]. In this way, the term cyber-security have become the quiet important area of research. Cyber-security maintains the confidentiality, availability of information, and integrity of information in cyberspace [2]. Although cyber-security is a unique terminology, to ensure and enhance security, and it is the coordination of the various other areas.

These areas are briefly described below.

- Security of applications implementing different measures to enhance the security of an application. This is often accomplished by monitoring the application and locating, correcting, and preventing security vulnerabilities.
- Information security is a set of procedures or practices intended to maintain the confidentiality, integrity, and availability of commercial data and information in a variety of formats.
- Network security is a process designed to protect the ease of use and integrity of the network and its data and to provide secure access to the network. Network security is always inclusive of both hardware and software technologies.

- Operational security is a process of identifying and protecting non-classified critical information that is often appealing to the competitor or adversary to obtain real information.
- Internet security entails a variety of security procedures that are used to ensure the safety of online transactions. It involves establishing exact rules and regulations to safeguard browsers, networks, operating systems, and other applications from assaults.
- ICT security is the ability to protect an organization's digital information assets' Confidentiality, Integrity, and Availability.

The relationship between the above domains is pictured in the following figure 1.

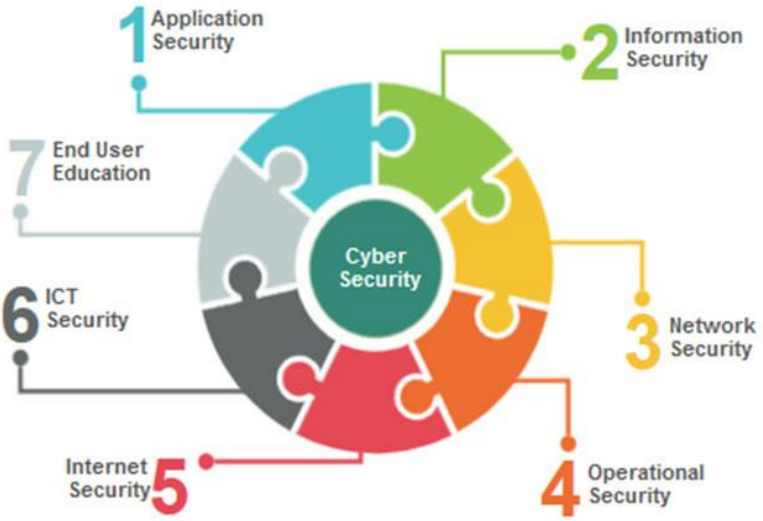

Figure 1: The Cyber-Security and its various domains

- Because humans are the weakest edges in the cyber-security big picture, end-user knowledge is crucial. 50 percent of cyber-attacks are caused by a lack of user awareness of cybersecurity threats, while nearly 90% of cyber-attacks are triggered by human behavior.

Cybercriminals, on the other hand, are becoming more sophisticated, and they are employing new ways and technologies to carry out effective attacks. They frequently uncover security flaws and vulnerabilities in secure systems, allowing them to steal information or do damage in less time[3]. People undertake all of their key day-to-day activities online in this digital era, thus enhanced cybersecurity using innovative tactics is critical. To counter cyber-attacks, cybersecurity must expand at the same rate as attacks. Despite the fact that multiple new strategies have been proposed by many researchers and that many strategies are now in use, the impact of an attack continues to grow. Cybersecurity has to protect any private, personal, or government data from attacks by focusing on three main tasks[4].

Cybersecurity must focus on three primary objectives in order to secure any private, personal, or government data from threats.

1. Taking precautions to safeguard equipment, software, and the data they contain.
2. Assuring the state or quality of protection from various risks;
3. Putting these efforts into action and enhancing them.

Many non-profit programs and many organizations has been launched in recent years with the goal of combating security issues. The (OWASP)Open Web Application Security Project is one of them.They have detail the top 10 most serious software vulnerability; Injection, Broken Authentication and Session Management, Broken Access control, Sensitive Data Exposure, (XSS)Cross-Site Scripting, (XXE)XML External Entities, Insecure Deserialization, Security Misconfigurations, Using Components with Known Vulnerabilities, and Insufficient Logging and Monitoring are the top ten vulnerabilities listed by the OWASP[5].

Statistics on cyber-attacks:

According to purples Technologies, 2021 trends report, cybercrime raised up 600% due to the COVID-19 pandemic. This number is far greater than the previous year. When compared to the previous years, the number of malicious mobile application packages increased drastically according to Kaspersky Labs. However, Norton claims that 99.9% of those application packages are from unapproved "third party" app store, making them easier to avoid.

The City of Atlanta spent $ 2.7 million to fix damage caused by a ransom ware assault, as per the report published by the Atlanta Journal-Constitution newspaper – www.ajc.com. According to the 2018 IT Professionals Security Report Survey, 76 percent of firms have encountered a phishing attack in the last year, while 49 percent have seen a DDoS attacks. Up to 7 million copies of the 'Adult Swine' malware were installed across 60 children's games apps. Cryptojacking Malware affects about 20% of enterprises every week, and Crypto miners affected 40% of enterprises.

Over 106 million people downloaded over 300 malware-infected apps from the Google Play store. Chinese government hackers allegedly stole 614 Giga Bytes of data linked to the weapons, the sensors, and the communication system from a US Navy contractor[6].Check Point's global attack sensors were subjected to a survey of new vulnerabilities discovered in the previous ten years[7].

In the last people based attacks have also been increased drastically. The following table shows the cost of damage and percentage of growth in different attacks from year 2017 to 2018.

Table no 1: Cost of damage and percentage of growth in different attacks.

Name of Attack	Cost of damage in 2017	Cost of damage in 2018	% Increase
Mlaware	$2,364,806	$2,613,952	+11%
Web-based attack	$2,014,142	$2,275,024	+13%
Denial of service	$1,565,435	$1,721,285	+10%
Malicious insider	$1,415,217	$1,621,075	+15%
Phishing and social engineering	$1,298,978	$1,407,214	+8%
Malocious code	$1,282,324	$1,396,603	+9%
Ransomware	$532,914	$645,920	21%

The Cyber Security Threats:

The purpose of most cyber-attacks is to shut down or acquire access to the target system. Various attacks on the target system can be used to achieve the goal. Several cyber-attacks exist, and they are always evolving.

Malware:

Malware is a type of malicious programwhich is created to harm a single computer or a network[8]. This category includes both traditional malicious programs such as Worms, Viruses, and Trojans, as well as more current malicious programs such as Spyware and Ransom ware. When a user use a harmful link, opens an attachment in an email, or installs harmful software, the virus infects the system or network. The essential element to keep in mind is that when malware interacts with another system or device, it reproduces or spreads. Blocking network access, installing new malicious software, and gathering information are some of the causes. 92% of malware is delivered by email.Malware for mobile devices is on the rise, with the number of new malware variants for mobile devices increasing by 54% in 2018. Android devices are the target of 98 percent of mobile malware. The following image shows total malware infection growth rate of last decade.

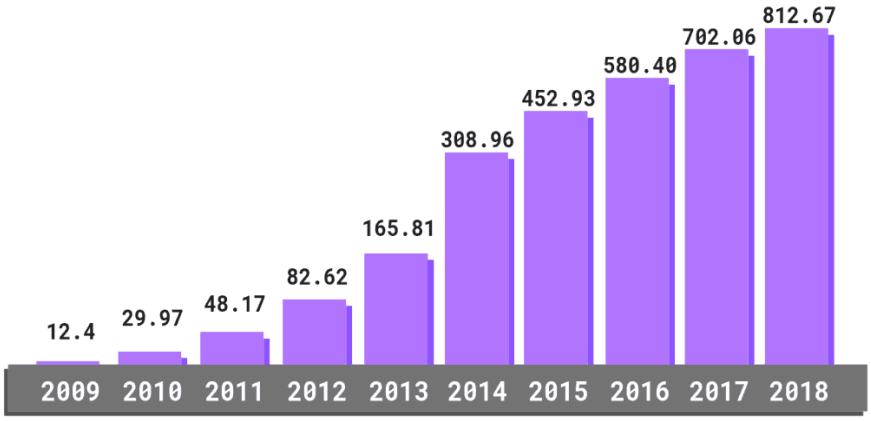

Figure 2: Total malware infection growth rate

Phishing:
Phishing is the practice of sending false emails that appear to come from a legitimate source. The purpose is to steal sensitive data such as credit card and login information or to infect the victim's computer with malware. Phishing is becoming a more widespread cyber threat. Phishing is one of the well-organized criminal enterprises of the twenty-first century. It's a type of malware or a phrase for when someone sends out a faked email to random recipients in the hopes of obtaining personal information[9]. Phishing is a criminal activity that employs social engineering tactics to fraudulently obtain sensitive information such as usernames and passwords by emailing users of prominent websites fake versions of the website to which they must enter their credentials.

Man-in-the-middle Attack:
When attackers inject themselves into a two-party transaction, this is known as a man-in-the-middle (MitM) attack. After interrupting the traffic, the attackers can filter and steal data. It's commonly referred to as eavesdropping attacks[10]. There are several types of MITM attacks, including password stealing, credential forwarding, and so on. Normally, attackers can put themselves between a visitor's device and the network on an insecure public Wi-Fi network. The visitor unwittingly transmits all information to the attacker. In some circumstances, the attacker uses malware to install software that collects information about the victim.

Crypto-jacking:
Cryptojacking is the practice of mining bitcoin using one's computer resources without the user's knowledge. By introducing malicious JavaScript code onto the page, this can be accomplished. In order to compute hashes, the malicious JavaScript code uses system resources. Most traditional cryptocurrencies, such as bitcoin, monero, and webchain, are based on the CryptoNight proof-of-work (POW) algorithm, which is CPU-bound.

Denial-of-Service Attack:
During a denial-of-service assault, traffic is flooded into systems, servers, or networks in order to exhaust resources and bandwidth. As a result, legitimate requests are unable to be processed by the system. This attack can also be launched using many compromised devices. Instead of conducting a single attack, the attacker attacks the target multiple times. A distributed-denial-of-service (DDoS) assault is what this is called. In the last few years, 24% of businesses have been subjected to a DDoS attack[11].

SQL Injection:
SQL injection is a frequent attack that occurs when an attacker injects malicious code into a server that utilizes SQL, forcing the server to divulge information that it would not ordinarily divulge. SQL injection is one of the most critical security flaws in Web application systems; the majority of these flaws are caused by a lack of input validation and the use of SQL parameters.

Zero-Day Exploit:
A zero-day exploit occurs after a network vulnerability has been identified but before a patch or solution has been deployed. During this period, attackers will focus on the publicly revealed vulnerability. The discovery of zero-day vulnerabilities necessitates ongoing alertness.

Spam:
It is undesired e-mail communication. Spam e-mails can be a time-consuming task for receivers, but they may also be a source of Java applets that run automatically when the message is viewed.
Apart from the risks listed above, the SANS Institute has identified the following malicious spyware behaviors as the most common:
•disabling antivirus and antispyware tools,
- installing rogue certificates,
- changing network settings,
- logging keystroke
- turning on the camera and/or microphone ,
- impersonating an antispyware or antivirus product,
- Form scraping, screen scraping, and URL monitoring
- setting up a bot to provide the attacker remote control,
- search resultsediting,
- spam relay act,
- installing a rootkit or modifying the system to prevent removal,

•setting up a sniffer.

Machine Learning and Cyber-Security:

In the literature, many approaches and processes for detecting dangers in cyberspace have been established. Machine learning has recently made a significant contribution to cybersecurity. In the instance of the spam detection, filters are used to analyze the content in order to determine whether or not the communication is spam. Machine Learning approaches including Bayesian classifier, SVM[12], MapReduce[13,] Behavior-based spam detection using neural networks, Text detection method for image spam filtering were recommended.
Malware detection based on statistical analysis was first introduced in [14]. Machine learning was offered as a method for detecting malware in [15]. Shijo and Salim proposed statistical and dynamical malware detection methods[16].Principal component analysis and multiclass support vector machines were used to detect internet worm malcodes. The random forest machine learning technology was used to detect phishing emails[17]. To detect phishing sites, several supervised learning algorithms were introduced[18]. As a result, clustering algorithms and the classification algorithms like Random Forest SVM, Nave Bayes Classifier, fuzzy-based classifierand neural network are extensively employed in detecting security threats including malware, spam, and phishing.

Conclusion:

Because of technological advancements, cyber-attacks and cybersecurity have improved and grown significantly over the last 20 years. Even while this is true, most firms have not developed and are still using older cybersecurity, despite the advancement of new technology. Mega assaults are large-scale and fast-moving cyber-attacks that have occurred recently. Traditional, static detection-based security systems, which are utilized by the majority of today's enterprises, are easily bypassed by these sophisticated attacks. As a result, enterprises should build the most up-to-date security infrastructures to secure their networks, clouds, and mobile infrastructure against the latest assaults. To summarize, organizations and individuals must become more aware of cyber-attacks and their consequences, as well as the security solutions available. Everyone should utilize technology only after weighing the benefits and drawbacks, as well as the risks of security breaches, and taking precautions to protect their personal information. Future work will focus on developing an improved security framework to safeguard online digital infrastructures, such as cloud, mobile, and network infrastructure.

References:

[1] Trustwave Global Security. Report retrieved from:https://www2.trustwave. com/ rs /8 15- R FM 693 /i ma ge s/ 20 15_ TrustwaveGlobalSecurityReport.pdf

[2] International Organization for Standardization. ISO/IEC 27032:2012. Information technology— Security techniques— Guidelines for cybersecurity. 2012

[3] Chowdhury, "Recent cybersecurity attacks and their mitigation approaches–An Overview," International conference on applications and techniques in information security, Springer, Singapore. 2016; pp 54-65.

[4] Fischer EA,"Creating a national framework for cybersecurity: an analysis of issues and options." Technical report. Congressional Research Service. 2005.

[5] The Open Web Application Security Project OWASP Top ten most critical web application security risks. The OWASP Foundation. 2018.

[6] Check Point Mobile Threat Research Publications. 2017. Available Online: https:// research.checkpoint.com/ check-point- mobile-research-team-looks-back-2017/

[7] Cyber Attack Trends Analysis Key Insights to Gear Up for in 2019. Available Online:http://www.snt.hr/ boxcontent/ CheckPointSecurtyReport2019_vol01.pdf

[8] Li Qian, Zhenyuan Zhu, Jun Hu, and Shuying Liu, "Research of SQL injection attack and prevention technology," 2015 International Conference on Estimation, Detection and Information Fusion (ICEDIF), 2015, pp. 303-306, doi: 10.1109/ICEDIF.2015.7280212.

[9] Vayansky, Ike & Kumar, Sathish, "Phishing – challenges and solutions", Computer Fraud & Security. 2018. 15-20. 10.1016/S1361-3723(18)30007-1.

[10] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, third quarter 2016, doi: 10.1109/COMST.2016.2548426.

[11] Z. Chao-yang, "DOS Attack Analysis and Study of New Measures to Prevent," International Conference on Intelligence Science and Information Engineering, 2011, pp. 426-429, doi: 10.1109/ISIE.2011.66.

[12] Hsu W.C., Yu T.Y,"E-mail spam filtering based on support vector machines with Taguchi method for parameter selection", J Converg Inf Technol 2010. 5(8):78–88.

[13] Caruana G., Li M., Qi M,"A MapReduce based parallel SVM for large scale spam filtering", In: IEEE eighth international conference on fuzzy systems and knowledge discovery (FSKD), 2011; pp 2659–2662.

[14] Dhaya R., Poongodi M,"Detecting software vulnerabilities in android using static analysis", 2015; pp 915–918.

[15] Markel Z., Bilzor M,"Building a machine learning classifier for malware detection", In: Second workshop on anti-malware testing research (WATeR). IEEE. Canterbury. UK. 2015.

[16]Shijo P.V., Salim A,"Integrated static and dynamic analysis for malware detection", Procedia Comput Sci. 2015; 46:804–811.

[17] Divya S., Padmavathi G,"A novel method for detection of internet worm malcodes using principal component analysis and multiclass support vector machine", Int J Secur Appl. 2014; 8(5):391–402

[18] Santhana Lakshmi V., Vijaya M.S.,"Efficient prediction of phishing websites using supervised learning algorithms", Procedia Eng. 2012; 30:798–805.