Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 5- Issue 1, Paper 34 January 2022

A Survey of Cyber Crimes and Cyber Security

Dr K. Chithra[1], M. Parijatham[2]
Department of Computer Science,
ShrimathiDevkunvarNanalal Bhatt Vaishnav College for Women

***Abstract*—The cyber world of the internet is a perilous area where unwitting people might fall prey to cyber thieves. The objective of this study is to direct an exhaustive examination concerning these attacks to raise information about the different kinds of attacks and how they work so that appropriate network protection countermeasures can be taken. This helps to safeguards internet users from cybercrime and cyberattacks, as well as to create a platform to protect themselves.**

***Keywords*-Cyber Crime, Cyber Security, Cyber attacks**

I. INTRODUCTION

THEprotection of computer systems and networks against data loss, theft, or damage to their hardware, software, or electronic data, as well as service disruption or misdirection, is known as cyber security. This industry is critical due to the ever-increasing reliance on computers and the internet [3][4].

The term cybercrime is utilized to depict an unlawful action wherein electronical gadgets, for example, cell phones, tablets, Personal Digital Assistants (PDAs).The focus of cybercrime is on monetary wrongdoing for personal gain, and it is typically conducted by those with a destructive and criminal mentality, either for retaliation, ravenousness, or experience [1][2].

A cybercriminal, frequently known as a programmer, is somebody who utilizes a PC or other computerized innovation, like the web, to take part in criminal operations. The crook might utilize PC abilities, information on human way of behaving, and an assortment of devices and administrations to accomplish their objective.Hacking, fraud, online tricks and extortion, constructing and engendering malware, and assaults on PC frameworks and sites are for the most part prospects [1].

II. CLASSIFICATION OF CYBER ATTACKS

The Cyber-attacks are commonly classified into the following categories.

- Based on Purpose
- Legal Classification
- Based on Severity of Involvement
- Based on Scope
- Based on Network Type [6].

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 1, Paper 34 January 2022

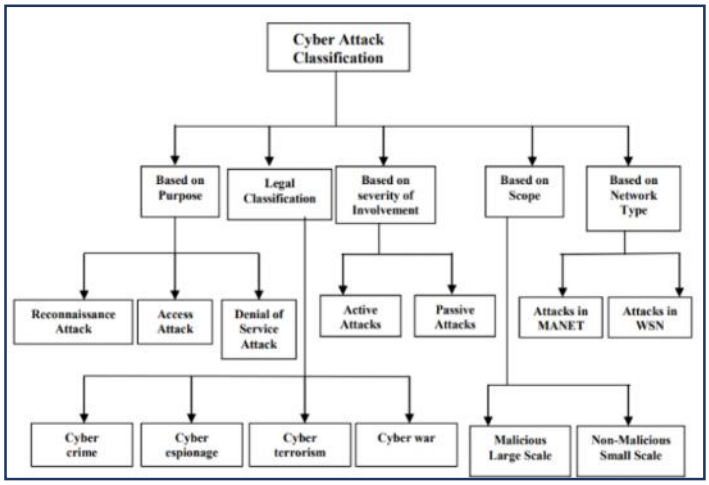

Fig. 1 Classification of Cyberattacks[13]

A. Based on Purpose

The attacks based on the purpose are

1) **Reconnaissance Attack**
   Unauthorized detection, system mapping, and services are all examples of reconnaissance assaults. It's similar to the theft rate in a community for residences that are vulnerable to break-ins due to being deserted, having weak doors, and having unsecured windows [5]. Example: Packet sniffers, Port scanning, Ping sweeps and DNS (Distributed Network Services) Queries.
2) **Access Attacks**
   An assault wherein an interloper accesses a gadget to which he doesn't have permission[5]. Example: Port trust use, Port redirection, Man-in-the-center assault,Social-designing assaults, Phishing [7].
3) **Denial of Service Attack**
   Attackers who threaten financial exchanges in fields such as insurance, train, and aeroplane services can do so by restricting authorised users of public sector information from all government entities[5]. Example: Smurf, SYN Flood, DNS assaults and DDOS (Distributed Denial of Services) [5][6].

B. Legal Classification

The cyberattacks are also classified based on legal classification they are,

1) **Cyber Crime**
   Cybercrime's goal is to turn the device into a crime tool and the computer into a crime accessory. Because of their privacy, data storage space, operating device vulnerability, and lack of user understanding, computers are used to commit crimes [5]. Example-Identity theft, Credit card fraud [5].
2) **Cyber Espionage**
   The act of utilizing the web to assemble data about individuals to get a benefit. Example-Tracking cookies, RAT controllable. [5][7].
3) **Cyber Terrorism**
   Cyberterrorism is defined as the use of the internet in conjunction with psychological oppression. It alludes to illegal attacks and the dangers of attacks on computers, organizations, and the data stored on them in order to alarm or coerce a government or its citizens to pursue political or social goals[10]. Example- Model Crashing the power frameworks by al-Qaeda by means of an organization, Poisoning of the water supply [5][7].
4) **Cyber War**
   A country's demonstration of upsetting one more country's organization to acquire strategic and military advantages. Example-Russia's conflict on Estonia (2007), Russia's conflict on Georgia (2008) [5][7].

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 5- Issue 1, Paper 34 January 2022

C. Based on*Severity of Involvement*

The cyberattacks based on severity of involvement is explained as follows:

1) Active Attack

The attackers alter the data during an active attack. Its primary purpose is to lower network performance. ExampleMasquerade, Reply, Modification of message [11].

2) Passive Attack

An Attackers simply pays attention to or monitors information or data being sent between two gatherings in this assault. Thereis no change or manufacture. Example- Traffic analysis, Release of message contents [11][12].

D. Based on Scope

The cyberattacks based on scope

1) Malicious

A malicious large-scale attack is carried out by a single individual or a group of people for personal gain or to cause chaos and disruption. On a global scale, these attacks damage thousands of systems, resulting in system failures and the loss of a significant amount of data, as well as the company's credibility[9][8].

2) Non-Malicious

These are mainly accidental attacks or injury caused by a poorly qualified person's mismanagement or technical errors, which can result in modest data loss or device crashes. In these cases, just a few network resources are compromised, therefore data is usually recoverable. It has something to do with decreased prices [9].

E. Based on Network Type

The cyberattacks based on Network type are discussed below:**Attack in MANET**A mobile ad hoc network is a wireless network that arises spontaneously without any prior infrastructure and in which each node can act as a router (MANET) [13][14]. Example- Black Hole Attack, Flood Rushing Attack, Byzantine Wormhole Attack [9].

1) Attack in WSN

An attack on the sensors that prevents them from detecting and transmitting data across the organisation. Application Layer Attacks, Transport Layer Attacks, Network Layer Attacks, and Multi-Layer Attacks are all examples of WSN (Wireless Sensor Network) [9].

III. PROTECTION BASED ON PURPOSE

A. Reconnaissance Attack

Only necessary traffic should pass through the firewall, which should also be set up to log numerous connections from the same IP address. Block sweeps such as FIN, NULL, and XMAS are ensured, and SYN checks are recognised, thanks to the firewall's state fulness. It is advised that an interruption identification system (IDS) such as Snort be used to examine traffic and detect odd behaviours. Snort should be able to tell apart various associations that originate from the same IP address. NAT is an excellent concept because it only displays one IP address and inhibits OS fingerprinting attempts. To obstruct weak destinations, apply all of the most recent upgrades [15].

B. Access Attack

It ensures that all communications between databases and other system objects follow the laws and regulations of the database system. There has been no tampering by any opponent, internal or external, and as aresult, the databases are safe from potential inaccuracies**.** Errors in a company's operations might have serious ramifications. Controlling access privileges can also help to lessen the likelihood of a database security breach. If an entry in the table is unintentionally removed or access is changed, for example, the impact can be reversed, but their deletion can be limited using the access control strategy. [16][17].

C. Denial of Service

Criminal assaults and threats on computers, networks, and the information stored on them are used to coerce or compel a government or its citizens to accomplishpolitical or social aims[18].

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 1, Paper 34 January 2022

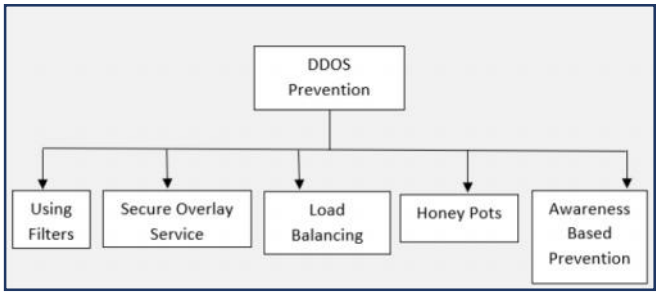

Fig. 2 DDOS Prevention[18]

IV. PROTECTION BASED ON LEGAL CLASSIFICATION

A. Cyber Crime

Antivirus software should be installed and updated on a regular basis to keep you safe from viruses. Confirm that the website with which you are conducting business is legitimate. Protect yourself from "Web-Spoofing." Do not click on email links to visit websites. Only use secure sites to send payment card information. Never give out your address, phone number, hangout areas, or connections to other websites or pages where you can get this information[19].

B. Cyber Espionage

Controlling and limiting the access of potential adversaries to equipment, specialized technical skills, and computational resources that might be used to launch deadly cyber-attacks are examples of procedures that can be utilized to achieve this purpose. This stage also includes a number of preventative safety measures, such as enforcing stringent computer security rules on hardware and software manufacturers and conducting drills to discover and correct existing system weaknesses. International treaties and agreements are also included in this category[20].

C. Cyber Terrorism

Cyber terrorism dangers must be made known to the general public. Cert-in should collaborate with academic institutions and take a risky approach. All government offices, including security forces, are working together to find competent, gifted professors for the deployment of countermeasures. [21][22].

V. PROTECTION BASED ON SEVERITY OF INVOLVEMENT AND NETWORK TYPE

A. Identity Privacy

In Mobile Ad-Hoc Networks, ALERT can guarantee Identity Privacy. Data is disseminated to k different nodes in the target zone by providing k-anonymity to the destination node. In order to protect the source's anonymity, ALERT has a policy of hiding the data source among a number of initial nodes [23].

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)
Volume 5- Issue 1, Paper 34 January 2022

B. Location Privacy

Eavesdropping on route request and route response packets and then using length checking to determine the distance from the source or destination is the current concept underlying Location Privacy attacks. The "notify and go" approach will increase location privacy by creating ambiguity for the adversary [24]. By creating ambiguity for the adversary, the "notify and go" approach will increase location privacy.

C. Route Anonymity

Route Anonymity's current assaults are based on traffic research. A random selection of random forwarders is maintained with hierarchical partition route privacy [25][26].

D. Wireless Senor Network (WSN)

Sensor networks with limited processing, storage, bandwidth, and resources necessitate the use of unique safety approaches. Because of the hardware and power limitations of the sensors, meeting the security needs of ad hoc networks in terms of availability, integrity, authentication, and freshness is difficult [27].

1) Availability

While sending information from a single source to the appropriate user, availability ensures responsiveness and response time protection. The approach also demonstrates that network operations are available to legitimate parties in the event of a denialof service attack, and that network services are maintained even when a denial of service attack is conducted (DoS) [28].

2) Integrity

It is a service that ensures that information is not modified during communication. Integrity protects the network from insertion or modification of communications.

3) Authentication

It is a service that ensures that information is not modified during communication. Integrity protects the network from insertion or modification of communications.

4) Freshness

WSNs provide only a few time metrics to ensure that each packet is fresh. The packet's refresh indicates that it is new, and that no malicious node is replaying prior packets[29].

VI. Protection Based on Scope

A.Signature Based Malware Detection

Antivirus scanners look for a pattern of bytes inside a programme code to identify and report malicious code using signature-based malware detection. Virus mark data sets should be updated with the most recent infection definitions on a regular basis [30]. This technique, however, is limited since it ignores instruction semantics, allowing malware to be disguised during programme execution. However, antivirus software is unable to detect zero-day hazardous exploit software, which can beprevented by doing a file content analysis to identify strange files [31].

B. Behavior Based Detection

Surface scanning is performed through behaviour-based detection, which also identifies the malware's action by creating a database of dangerous actions. Support vector machines (SVM) are trained using data mining techniques to easily distinguish between malicious and non-malicious programmes, making them highly efficient in detecting metaphoric malware[31].

VII. Conclusion

This paper gives brief information about classification of cyberattacks with various example as well as gives protection against the cyberattacks with various counter measures and detection. Prevention is better than cure, this may help everyone to protect from various attacks as well as their network, internet, sensitive data form cybercrime.

Journal of Current Research in Engineering and Science
Bi-Annual Online Journal (ISSN : 2581 - 611X)

Volume 5- Issue 1, Paper 34 January 2022

REFERENCES

[1] KomalBankar, MayuriKakad, ShelarPawarand AishwarayaShelar,"Cyber Security and Women Safety Application (International journal for TechnologicalResearch inEngineering),"vol. 5, no. 7, pp.3325-3328 ,2018,
[2] www.tech-crats.com
[3] Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security".
[4] en.wikipediya.org
[5] M. Uma and G. Padmavathi," A Survey on Various Cyber Attacks and Their Classification(International Journal of Network Security)", vol.15, no.5, pp.390-396, 2013.
[6] ijns.jalaxy.com.tw
[7] www.legalserviceindia.com
[8] www.ukessays.com
[9] S.Sujayraj and M.Chethan," Classification of Cyber Attacks and its Associated Laws (JETIREV06045 Journal of Emerging Technologies and Innovative Research (JETIR)),"2019 JETIR February 2019, vol. 6, no. 2 , pp.289-298, 2019 .
[10] MathihaNehla Hani and AswathyRajan," A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack (International Journal of Pure and Applied Mathematics)," vol. 119 no. 17, pp.1617-16362018,
[11] Pooja Chahal, Gaurav Kumar Tak and Anurag Singh Tomar ,"Comparative Analysis of Various Attacks on MANET (International Journal of Computer Applications , vol.111 , no. 12, pp.1721-1727,2015
[12] research.ijcaonline.org
[13] G.S. Mamatha & S.C. Sharma," Robust Approach to Detect and Prevent Network Layer Attacks in MANETS(International Journal of Computer Science and Security)," vol. 4, no.3, pp.275-284 , year
[14] docplayer.net
[15] H. P. Sanghvi, M. S. Dahiya, "Cyber Reconnaissance: An Alarm before Cyber Attack,International Journal of Computer Applications,vol.63, no.6, pp.36-38,2013.
[16] SnehRathore and Anupam Sharma," Data Base security- Attacks, Threats and Challenges(International journal of Engineering Research &Technology (IJERT))," ICCCS-2017, vol. 5, no. 10, pp.1-4 , 2017.
[17] www.ijert.org
[18] TasnuvaMahjabin, Yang Xiao, Guang Sun and Wangdong Jiang," A survey of distributed denial-of-service attack, prevention, and mitigation techniques", International Journal of Distributed Sensor Networks, vol.13, no.12, pp.2-32,2017.
[19] Ms M Lakshmi Prasanthi and Tata A S K Ishwarya,"Cyber Crime: Prevention & Detection, "International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, no. 3,pp.45-48 ,2015.
[20] ItaiBarsade, Louis Davis, Kathryn Dura, Rodrigo Ornelas, and Ariel Smith," Prevention in the Cyber Domain(World House Student Fellows)," 2016-2017.
[21] 1Mathiha Nehla Hani and 2Aswathy Rajan," A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack(International Journal of Pure and Applied Mathematics),"vol. 119,no. 17, pp.1617-1636 2018,.
[22] academicscience.co.in
[23] ink.library.smu.edu.sg
[24] ElaheSheklabadi and MehiBerenjkoub,"An anonymous secure routing protocol for mobile ad hoc networks", International Symposium on Computer Networks and Distributed Systems, (CNDS)),2011.
[25] Rohini Y. Sarode, "Active Attack Detection and Unavailability over ALERT Protocol in MANET", International Journal on Recent and Innovation Trends in Computing and Communication, vol. 5, no.1, pp.1-5 ,2017.
[26] Sk.Md. Mizanur Rahman,"Anonymous Secure Communication in Wireless Mobile Ad-hoc Networks(Lecture Notes in Computer Science)," 2007.
[27] Ashwani Kush and C. Jinshong Hwang. "Proposed Protocol for Secured Routing in Ad Hoc Networks", International Association of Computer Science and Information Technology-Spring Conference,2009.
[28] turcomat.org
[29] Jaya Kaushika and DR. NareshGroverb , "Security Techniques Against Power Exhausting Attacks in WSN: A Fundamental Study", Turkish Journal of Computer and Mathematics Education,vol.12 , no.10, pp.377-391,2021
[30] docplayer.net
[31] Muni PrashneelGounder and Mohammed Farik, "New Way to Fight Malware", International Journal of Science &Technology Research, vol.6, no 06, pp.318-323 ,2017.