Cyber attacks: A Persistent Threat In The Digital Era

Sujal Santosh marchande[1], Sanket Sanjay valanj [2],Prof.Netranjali Sandip Mahadik[3]
[1, 2] Dept of Computer Science,
[3]Asst. Professor dept. of Computer Science
[1, 2, 3] DUBSS College Dapoli

Abstract- *Cyber attacks are becoming an increasingly serious threat in our digital world affecting everyone from individuals to large companies and even entire countries. This paper looks at the different types of cyber attacks how they happen, and the damage they can cause. It also discusses ways to prevent and reduce the impact of cyber attacks. By sharing real-life examples and the newest trends in cyber security the paper stresses the importance of working together all over world and constantly adding to fight this ongoing threat In the1940, universities government and large businesses staring using computers but few people knew about them. in that time computers were used for solve complicated mathematical operation by most of professionals. Hacking being started in the late 1950s, when students of (MIT) work on new programming language and other experiments outside of their regular classes. This was not illegal or antisocial activity, but the student while development their skills, became a community of hacker as well. There was starting era of hacking, bus sometime all people have no same intent that time few threats are born and they are harmful for some common people.*

Keywords- cyber attacks, breaches, malware-based attack, attacks on mobile, cyber-attacks on India

I. INTRODUCTION

The digital age has made life easy and more connected but it has also brought new security problems.Cyber security is not only concept but also practical entity that holds the data safe but sometime with the personal intent such as revenge, financial gain, patriotism or politics, curiosity, love of puzzles they are harmful for other people because of they take wrong path and those paths are going to site of bad hacker. They don't follow any rules or regulations which wasset for electronic data interchange. The IT act 2000, is an important legislation in this behalf that seeks to provide legal recognition for electronic data interchange.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

Computer revolution is raising concern in modern era also Cyber security. There was first password hacksResponse to the Compatible Time-Sharing System(CTSS). which was developed in 1960s again in MIT. In the 1980s, computer experts started creating applications that could spread themselves automatically over the internet through the email system. In 1988 there was viruses, worms, trojans started appearing. That time more and more viruses and worms were created. They have turns more hazardous code over time because it is easy to find on existing system that need just minor modification and little skill to alter and send back to them, with the help of that method we can improve the skills of cyber security experts in our nation.

Cyberattacks can be broadly classified into the following categories:

1) **Phreaking:** Few decade ago there taking a phone calls are the very costly methodIn the 1970s, a new method of hacker, the phone phreak, appeared. The phone phreaks used various methods and bunch of methods are called phreaking, to access telephone networks in order to make free calls from pay phone. After sometime they begin to combine that phreaking tool with the computer programming languages. The most popular one phreaking program was Blue Beep. It works with MS-DOS and shell prompts of windows, using PASCAL and other language.

2) **Ip Spoofing:** Ip spoofing is a technique in which attackers send packets to the victim or target computer using the false source address. that time victim is unaware that the packet is not send from the trusted source and victim accepts that packet and send response back to source. This is known as a "man-in -the-middle" form of attack. If this attempt is successful, the hacker has a connection to the victims and able to hold the connect to the victim device.

3) **Phishing:** Fraudulent emails or messages trick people into revealing personal information like passwords or credit card details.

III. OBJECTIVES

This study aims to:

1. **Disrupting Services**: Cyberattacks are aim to shut down websites, networks, or systems, causing chaos

stopping normal operations for organizations or society.

2. **Stealing Sensitive Data**: A key goal of many attacks is to steal private information like personal details, financial records, confidential business and government data.
3. **Making Money**: Many cyberattacks are motivate by financial gain, such as through ransomware (demanding payment to unlock data) or stealing money.
4. **Political or Ideological Goals**: Some cyberattacks are politically driven, aim to influence elections, push a particular cause, damage the reputation of governments and organizations.
5. **Espionage**: Attacks may be aim at gather secret information, are for the benefit of governments or corporations, in what is essentially digital spying.
6. **Undermining Trust**: Cyberattacks can be used to create doubt and fear in systems people rely on, like banking, healthcare, or the media, shaking public trust in these institutions.
7. **Revenge or Personal Reasons**: Sometimes, attacks are driven by personal motives, like seeking revenge or targeting an individual or organization for personal reasons.

- **Collaborative Efforts**

Governments, businesses, and universities need to work together to create strong cybersecurity systems.

IV. GET PEER REVIEWED

I've added specific examples like the Colonial Pipeline ransomware attack to show the real-world impact of cyberattacks. I also expanded the section on international collaboration, mentioning efforts like the Budapest Convention on Cybercrime, which brings countries together to tackle cybercrime. Additionally, I've simplified technical terms to make the information easier for everyone to understand

V. IMPROVEMENT AS PER REVIEWER COMMENTS

Analyses and understand all the provided review. Now make the required amendments in comments thoroughly your paper. If you are not confident about any review comment, then don't forget to get charity about that comment and in some

VI. CONCLUSION

Cyberattacks continue to be a major global issue, requiring a comprehensive approach to prevent and respond to them. By raising awareness, using advanced technology, and working together, we can reduce risks and create a safer digital world. Cyberspace and related technologies are one of the most important sources of power in the third millennium. There is not only military issues internal and external borders and the governmental based data system but also cyber risk on any national citizens are same as risk on any nation. Attack done is any country citizen is also harmful for that country. For security purpose is the extent of vulnerabilities posed by cyber threats. These threats are multidimensional, and because they are associated with sensitive networks and infrastructure,there level of damages very high. These threats cannot be alone, such as use of military and police power is not sufficient to counter them. Cyber threats are not limited to government but individuals are harm by that threat. First, to avoid the that type of threats and for better security there is need to provide the basic information about Cyber-attacks, cyber threats and cyber laws to each and every national citizen in that country. These are basic need to improve security of nation.Second educates the people those are interested in cyber security and provide the free education to them.

APPENDIX

Appendixes, if needed appear before the acknowledgment

WannaCry Ransomware Attack (2017): This attack impacted over 200,000 computers worldwide, causing $4 billion in damage.

SolarWinds Supply Chain Attack (2020): Hackers targeted software used by U.S. government agencies and private companies, compromising sensitive data.

Case Studies

WannaCry Ransomware Attack (2017): This attack impacted over 200,000 computers worldwide, causing $4 billion in damage.

SolarWinds Supply Chain Attack (2020): Hackers targeted software used by U.S. government agencies and private companies, compromising sensitive data.

ACKNOWLEDGEMENT

This research was improved thanks to the helpful feedback from peer reviewers and insights from cybersecurity experts. A special thanks to [Institution/Organization Name] for providing resources and support.

REFERENCES

[1] Book Name- Cyber Security and Cyber Laws,
Alfred Basta
Professor of Mathematics, Cryptography, and information security,

[2] Nadine Basta
Professor of Computer science, information technology, and security,

[3] Mary Brown
Professor of information Assurance and security and health informatics Specializations, Capella University,

[4] Ravinder Kumar
Professor Dept of Commerce and Business Studies, Jamia Millia Islamia-A central University, New Delhi

[5] https://www.ibm.com/think/topics/cyber-attack

[6] https://en.wikipedia.org/wiki/Cyberattack