WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Overview of Cyber Security

[1]Gopalam Venkata Sai Charan

[1]Student, Electrical and Electronics Engineering, Bapatla Engineering College, Bapatla, Andhra Pradesh.
Doi: https://doi.org/10.55248/gengpi.5.0424.1127

ABSTRACT:

Cyber security is a rapidly growing field that aims to protect computer systems, networks, and sensitive information from unauthorized access, use, disclosure, disruption, modification, or destruction. The field covers a wide range of topics, including network security, data security, cloud security, and mobile security, as well as legal and ethical issues related to cyber security. With the increasing dependence on technology in everyday life, it is essential for organizations and individuals to take appropriate measures to protect themselves against cyber-attacks. Research in cyber security focuses on developing new technologies and techniques to protect against cyber threats, as well as understanding the motivations and methods of attackers. This includes the development of secure software and hardware, the use of encryption and authentication, and the implementation of security policies and procedures. Additionally, research in the field also focuses on understanding the legal, ethical and societal implications of cyber security.

Keywords: Malicious, Stealing Identities, Vulnerabilities, Child Pornography, Cyber stalking.

1. INTRODUCTION

Cyber security is the process of defending against hostile assaults against computers, servers, mobile devices, networks, and data. It is often referred to as information security (IS) or information technology security (IT).Several levels of protection dispersed throughout the computers, networks, applications, or data that one hopes to keep safe are essential components of a good cyber security strategy. Control also includes safeguarding software and hardware against malicious actors' electronic assaults, including spammers, hackers, and cybercriminals. While some elements of cyber security are intended to launch an assault first, the majority of specialists working today concentrate more on figuring out how to best protect all assets—from computers and cell phones to networks and databases—against attacks. Cyber security refers to the methods used to safeguard a user's online surroundings. This environment consists of the user, as well as any and all software, devices, networks, and applications. The area of computer security that deals with the internet is called cyber security. The primary goal of security is to project the device according to different guidelines and to set up different defenses against online attacks. To improve internet security and stop cyber attacks, several strategies are employed. The prevalence of online activities and applications has led to a daily surge in cyber attacks.

2. THREATS

MALICIOUS SOFTWARE

An individual using a computer may occasionally be coerced into downloading dangerous software onto their device. They can be in the form of worms, Trojan horses, viruses, or other malware.

1. **VIRUS**

It's the kind of malicious software that, when run, changes other computer programs to copy itself. Computer viruses can lead to system failure, corrupt data, higher maintenance costs, and other financial harm.

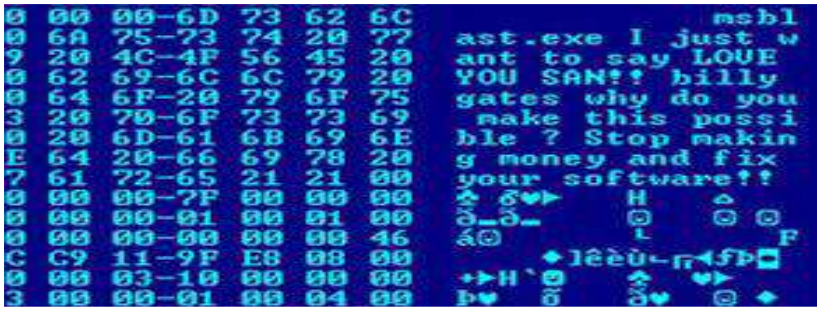

Fig 1: VIRUS

2. TROJAN HORSE

Trojan horses, also referred to as Trojans, are malicious software programs that masquerade as benign and are installed onto a user's computer against their consent. Email passwords, bank account information, and personal identities can all be compromised by Trojan horses. The impact extends to further network-connected gadgets.

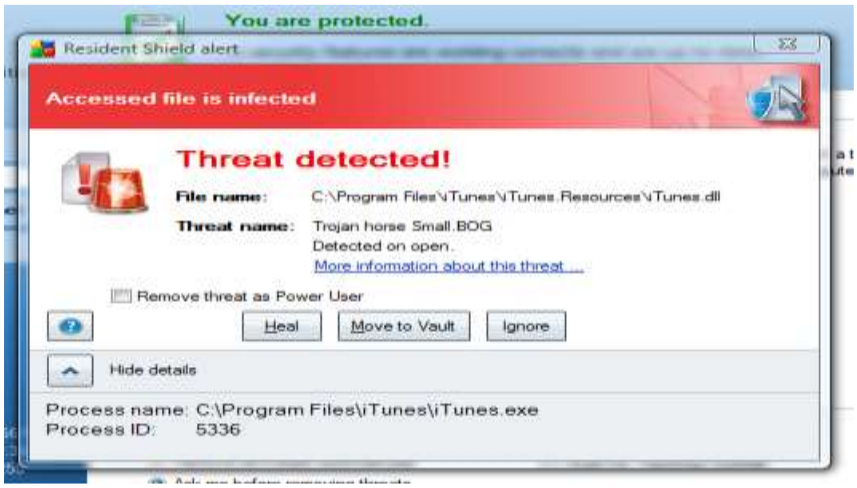

Fig 2: TROJAN HORSE

3. WORMS

A computer worm is a type of malware that operates independently and replicates itself on other computers. A lot of worms don't try to alter the systems they pass through; instead, their sole purpose is to proliferate.

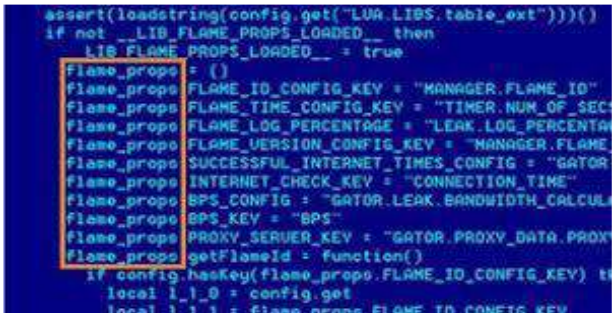

Fig 3: WORMS

4. MALWARE

Malicious software, or MALWARE for short, is designed to take down computer systems, obtain extremely sensitive data, or access private networks. Software that acts against the needs of the computer user and has malicious intent is classified as malware; this definition excludes programs that inadvertently do harm because of flaws in them. Malicious software and inadvertently destructive software are sometimes referred to as malware.

3. PHISHING

It is the attempt to obtain sensitive data, frequently with malicious intent, such as usernames, passwords, and credit card numbers. Phishing usually involves email or instant messaging spoofing, and it frequently involves tricking people into entering personal information on a fraudulent website. Links to malicious websites may be included in phishing emails. The most common example of social engineering tactics used to trick users and take advantage of holes in current web security is phishing.

PHISHING COMES IN VARIOUS FORMS.

1. CLONE PHISHING

This kind of phishing attack involves using the content and recipient address (es) of an email that contains an attachment or link to construct a cloned or nearly identical email.

2. SPEAR PHISHING

Spear phishing is the phrase used to describe phishing attempts that target specific individuals or corporations. With 91% of attacks, this is the most effective tactic being used on the internet. To improve their chances of success, the attackers use this to obtain information about the targets and the companies.

3. WHALING

Phishing attacks are known as "whaling" because they target high-profile individuals within firms, such as top executives.

4. ENCRYPTION AND DECRYPTION, WHICH ARE USED TO PROTECT SENSITIVE DATA

1. ENCRYPTION

Using an algorithm and a key, encryption is the act of transforming plaintext—normal, readable data—into cipher text, which is encoded, unreadable data. Data encryption is used to shield information from illegal access or interception. Two primary categories of encryption exist:

SYMMETRIC ENCRYPTION: In symmetric encryption, the encryption and decryption processes use the same key. This implies that the key must be the same for the sender and the recipient. The Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are two popular symmetric encryption methods.

A PAIR OF KEYS IS USED IN ASYMMETRIC ENCRYPTION: A public key and a private key. While the private key is needed for decryption, the public key is utilized for encryption. As a result, secure communication is possible without requiring prior key exchange. Elliptic curve cryptography (ECC) and Rivest-Shamir-Adleman (RSA) are two popular asymmetric encryption techniques.

2. DECRYPTION

The opposite of encryption is decryption. It entails employing the right key to translate cipher text back into plaintext. Authorized people can view the original, legible data after decryption.

In a variety of cyber security applications, including digital signatures, secure communication, and data storage, encryption and decryption are essential components in guaranteeing the confidentiality, integrity, and validity of data. They are crucial instruments for guaranteeing the security of digital transactions and preventing unwanted access to private data.

5. CYBER SECURITY USES FIREWALLS FOR A NUMBER OF CRUCIAL REASONS

1. **SAFETY OF THE NETWORK:** An organization's intranet and other internal networks are separated from external networks, such the internet, via firewalls. By enforcing predefined the security standards, they permit allowed traffic to go through while blocking unauthorized access.

2. CONTROL OF ACCESS: By analyzing incoming and outgoing network traffic and making decisions on whether to allow or restrict it based on parameters including source and destination IP addresses, ports, and protocols, firewalls implement access control policies. By doing this, businesses may better manage who has access to their network's resources and services.

3. THREAT PROTECTION: Firewalls guard against ransom ware, viruses, worms, malware, and unauthorized access attempts, among other cyber threats. Firewalls assist in preventing attacks from reaching susceptible systems and devices within the network by screening out malicious or suspicious traffic.

4. NETWORK MONITORING: By recording details about the connections they manage, firewalls give users insight into network activity. For monitoring and analytical reasons, such as detecting security incidents, resolving network problems, and verifying adherence to security policies, this data can be used.

5. COMPLIANCE REQUIREMENTS: Adding firewalls to an organization's cyber security architecture is mandated by a number of industry recommendations and regulatory standards. Firewalls are frequently required in order to secure sensitive data in accordance with regulations like the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

6. NETWORK SEGMENTATION AND ISOLATION: With firewalls, businesses can divide their networks into distinct zones or sub networks with varying degrees of protection. Firewalls assist reduce breaches and lessen the effect of security incidents by limiting the flow of traffic between these zones and preventing lateral movement within the network.

In general, firewalls are vital parts of successful cyber security strategies because they protect networks and data from illegal access, cyber attacks, and other security risks.

SECURITY TOKENS

On a security token, several websites allow users to enter a six-digit code that changes at random every 30 to 60 seconds. The token's keys have constructed calculations and altered numbers depending on the device's internal current time. This indicates that only a specific set of numbers can be entered correctly to gain access to the online account once every thirty seconds.

6. CONCLUSION

Essentially, the goal of this paper is to inform readers about the many types of assaults and the different security measures that may be taken to shield our device from harm. Additionally, it aids in overcoming a number of computer operating flaws. To sum up, cyber security is a serious problem that has an impact on people, companies, and governments all around the world. Since cyber dangers and attacks are on the rise due to technology's ongoing advancement, it is imperative that enterprises put in place strong security measures. Firewalls, encryption, security software, and staff education and training are some of these approaches. Organizations must also have incident response plans in place in order to react to security breaches promptly and efficiently. Together, public and commercial sectors should adopt rules and guidelines to guard against cyber threats and enhance the general security of cyberspace.

REFERENCE

[1] Dr. B .J. Mohite. “Literature Survey on Comparative Analysis of Different data Security Techniques Used in Networking”, SIBACA International Journal of Computing (SIJC), 2012.

[2] Sachin Shankar Bhosale "Research Paper on Cyber Security" I.C.S.COLLEGE OF ARTS COMMERCE AND SCIENCE KHED RATANGIRI Department of Information Technology Doctor of Philosophy.

[3] Nikhita Reddy Gade "A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies" Chaitanya Bharathi Institute of Technology | CBIT · Department of Computer Science and Engineering / Ugander G J Reddy.

[4] Saloni Khurana "A Review Paper on Cyber Security" Department of Electronics & Communication Vivekananda Institute of Technology, Jaipur, India.

[5] https://en.wikipedia.org/wiki/Phishing

[6] https://en.wikipedia.org/wiki/Internet_security#Phishing

[7] https://en.wikipedia.org/wiki/Malware