International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

A REVIEW ARTICLE ON CYBER SECURITY

Vivek Kumar Arya, Vishant Panwar, Asst Prof. Rakesh Kumar (Guide)

Department of C.S.E,

Tula's Institute Dehradun, Uttarakhand India

Abstract

Cyber security is a critical component in today's digital age, comprising methods, procedures, and technology aimed to protect digital systems, networks, and data against harmful assaults. As our reliance on technology grows, so does the scope and complexity of cyber threats, necessitating strong safeguards against unauthorized access, data breaches, and cyber-attacks. This paper explores the multidimensional aspect of cyber security, evaluating its role in risk mitigation and digital fortification.

KEYWORDS

- Threats
- Malicious Software
- Trojan Horse
- Phishing
- Data Protection
- Antivirus
- Internet Security Products

INTRODUCTION

Cyber security refers to a set of methods, technologies, and measures used to safeguard digital systems, networks, and data from unwanted access, attacks, and damage. In an age of interconnection and digital dependence, cyber security is critical. It entails tactics for detecting and combating cyber threats like malware, phishing, ransomware, and others.

The primary security goal is to develop the device using various rules and to develop various defenses against internet-based attacks. There are numerous strategies for preventing online attacks and improving internet security.

THREATS.

1. Malicious Software

Malicious software, sometimes known as malware, is a class of malicious programs that are designed to infiltrate, damage, or compromise computer systems, networks, and data. Cybercriminals create malware to exploit vulnerabilities, steal information, disrupt operations, and launch Cyber attacks. It consists of Viruses, Worms, Trojan horses, and Ransomware.

- VIRUS.

A computer virus is a form of malicious software that can multiply and expand across computers and networks by attaching itself to legitimate programs or files. It can have several negative consequences, including data corruption, system crashes, and illegal access. Viruses are frequently designed to do certain acts, such as deleting or changing files, and they can be spread by infected files, emails, or removable storage devices.

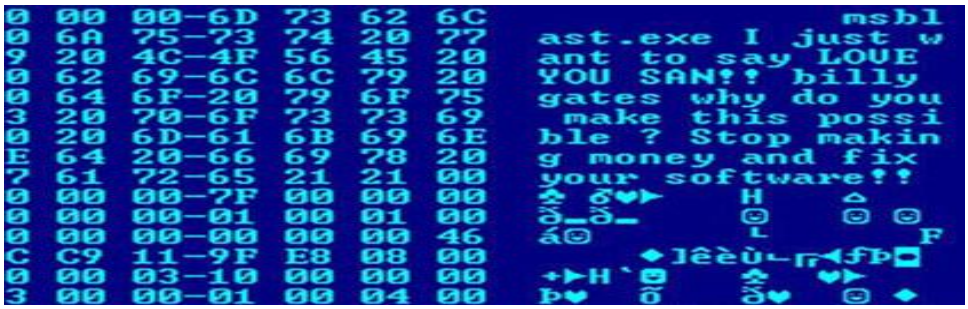

Fig.1.1Virus

- WORMS

Computer worms are a type of harmful software that spreads autonomously over computer networks, frequently without the interaction of the user. Worms, unlike viruses, do not require a host software to attach to and can self-replicate. They take advantage of flaws in operating systems or programs to spread quickly and create disruptions, data loss, or illegal access to infected systems. Worms can be used for a variety of purposes, including stealing sensitive data and establishing a network of compromised machines for future cyber attacks.

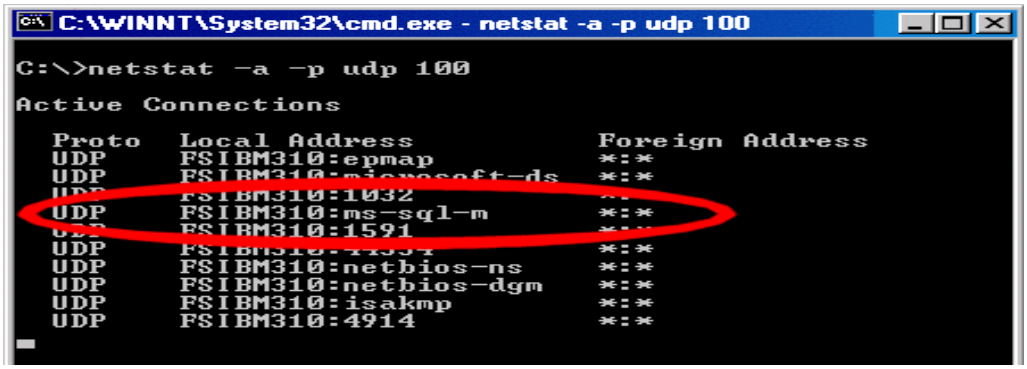

Fig.1.2 Worms

2. TROJAN HORSE

A Trojan Horse Virus is a kind of malware that infiltrates a computer while acting as a genuine program. Typically, an attacker will employ social engineering to embed harmful code within real software to acquire system access to their program.

Unusual behavior, such as unexpected changes to computer settings, can indicate the presence of a Trojan on a system.

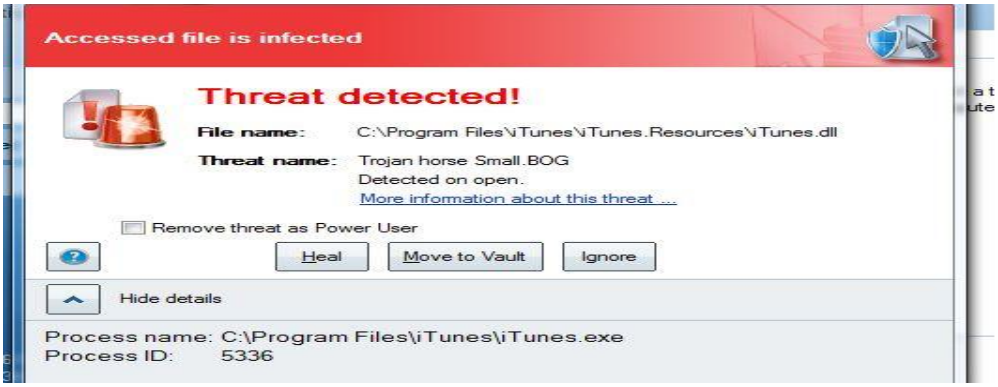

Fig.2 Trojan Horse

3. PHISHING

Phishing is often carried out through instant messaging or email spoofing, and it frequently urges people to enter personal information on a fraudulent website. Phishing emails may contain links to malware-infected websites. Phishing is the most common example of social engineering tactics used to trick users and exploit vulnerabilities in existing web security.

There are various kinds of phishing.

SPEAR PHISHING

Spear phishing refers to phishing attempts focused on specific individuals or businesses. With 91% of attacks, this is the most successful tactic on the internet today. The attackers acquire information about the companies and their targets to boost their chances of success.

Phishing by clone It is a sort of phishing attempt in which an email with an attachment is sent.

CLONE PHISHING

Phishing by clone It is a sort of phishing attack in which the content and recipient address of an email including an attachment or link are stolen and utilized to construct an almost identical or cloned email.

WHALING

Whaling Several phishing attempts have been launched expressly against top executives and other high-profile targets within corporations, and these types of attacks are known as whaling.

4. MALWARE

Malware is an expression for malicious software, which is used to break down computer operations, collect highly sensitive information, or obtain access to private computer systems. Malware is defined by its harmful intent, operating against the computer user's requirements, and does not include software that causes accidental harm due to a flaw. Malware is sometimes used to refer to malicious software and accidentally destructive software.

DATA PROTECTION

- Firewall

  The access between networks is controlled by a computer firewall. It includes filters that are specific to one or both firewalls. A firewall is essentially a computer security system that regulates and analyzes network traffic based on security rules. A firewall, in essence, creates a barrier between a trusted, secure Internet network and other outside networks, such as the Internet, that are not regarded as safe or trustworthy.

INTERNET SECURITY PRODUCT

1. Antivirus Software

   Antivirus software and internet security programs can protect a programmable device from viruses by identifying and removing them. Antivirus software was utilized in the early days of the internet, but with the advancement of technology, various free security programs are now available on the internet
2. Password Managing

   Password managers are software applications that store and arrange passwords. Password managers typically store passwords encrypted, necessitating the creation of a master password; a single, preferably very strong password that grants the user access to their entire password database.
3. Security Suits

The security suites include firewalls, anti-virus, anti-spyware, and other tools. They also provide free theft detection, portable storage device safety checks, private internet browsing, and security-related decisions.

4. End Point Security

The security suites include firewalls, anti-virus, anti-spyware, and other tools. They also provide free theft detection, portable storage device safety checks, private internet browsing, and security-related decisions.

CONCLUSION

This document tries to explain several cyberattacks and security solutions that can be used to protect our equipment from being hacked. It also aids in closing many gaps in their computer operation.

REFERENCES:

1. Anti-phishing group tech reports: https://www.antiphishing.org/phish Reports Archieve.html
2. https://en.wikipedia.org/wiki/malware
3. https://en.wikipidea.org/wiki/Internet-security