Cyber Security

Submitted To:
Mr. Boopathi Subramani
Dept. Of Computer Science

Submitted By:
Name Sanjeev Kumar
RDOC14 A10

Introduction

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Network security

Network Security is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

Application security

Application security focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

Information security

Information security protects the integrity and privacy of data, both in storage and in transit.

Operational security

Operational security includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

End-user education

End-user education addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.

The scale of the cyber threat

The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year. A report by RiskBased Security revealed that a shocking 7.9 billion records have been exposed by data breaches in the first nine months of 2019 alone. This figure is more than double (112%) the number of records exposed in the same period in 2018.

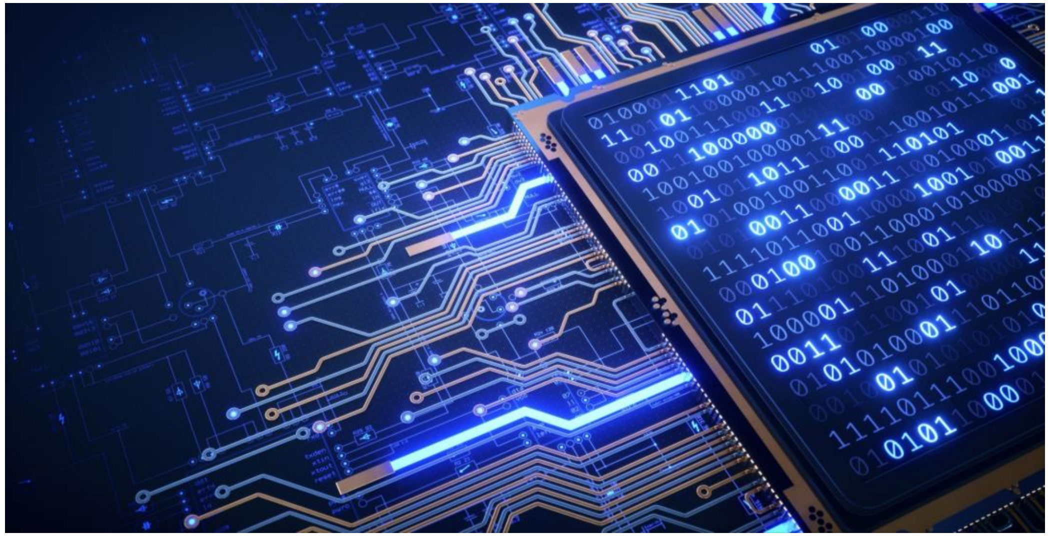
Types of cyber threats

The threats countered by cyber-security are three-fold:

1. **Cyber Crime** - includes single actors or groups targeting systems for financial gain or to cause disruption.

2. **Cyber-attack** often involves politically motivated information gathering.

3. **Cyber terrorism** is intended to undermine electronic systems to cause panic or fear.

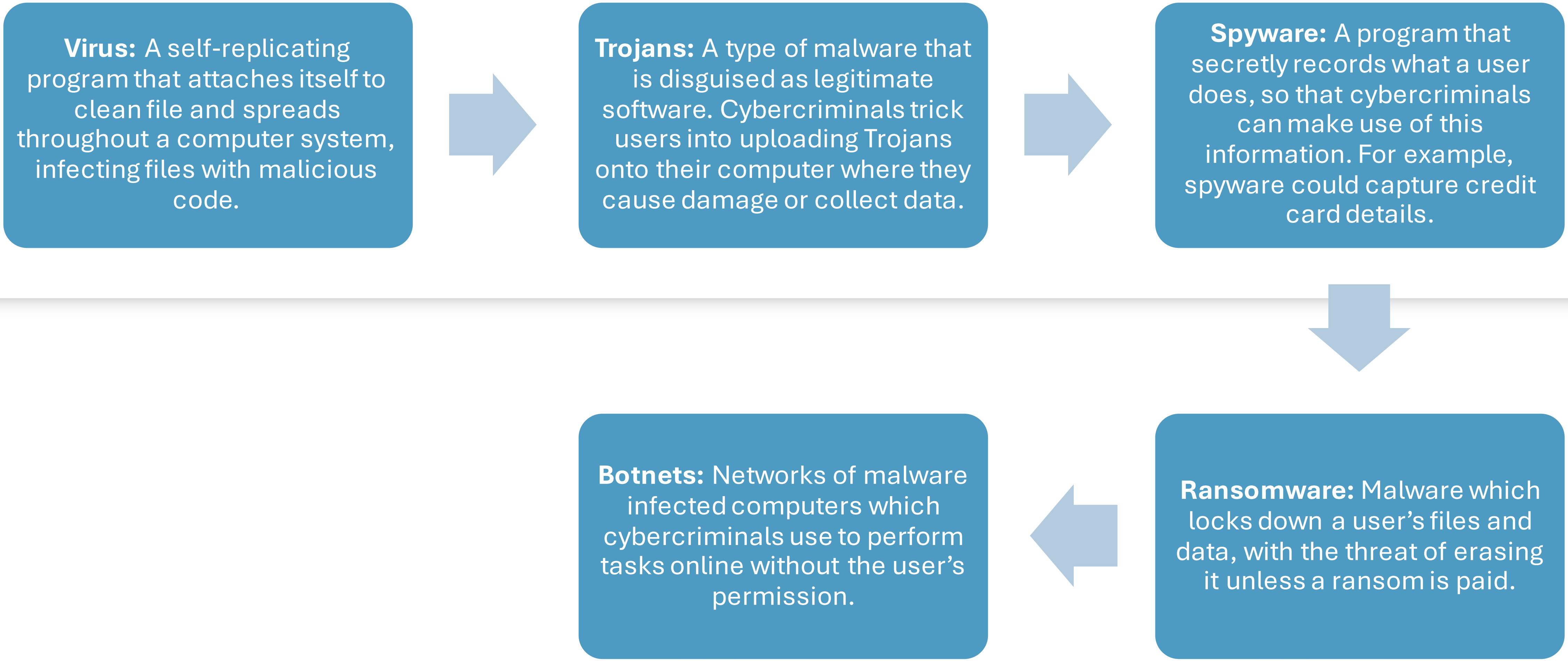


So, how do malicious actors gain control of computer systems? Here are some common methods used to threaten cyber-security ?

Malware

Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user's computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks.

There are a number of different types of malware, including:



Virus: A self-replicating program that attaches itself to clean file and spreads throughout a computer system, infecting files with malicious code.

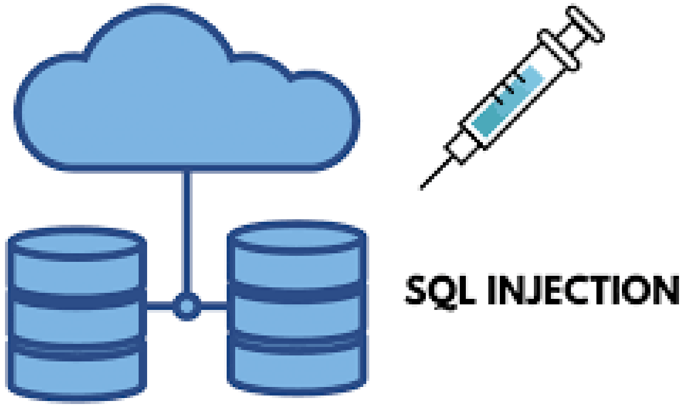
Trojans: A type of malware that is disguised as legitimate software. Cybercriminals trick users into uploading Trojans onto their computer where they cause damage or collect data.

Spyware: A program that secretly records what a user does, so that cybercriminals can make use of this information. For example, spyware could capture credit card details.

Ransomware: Malware which locks down a user's files and data, with the threat of erasing it unless a ransom is paid.

Botnets: Networks of malware infected computers which cybercriminals use to perform tasks online without the user's permission.

SQL injection



An SQL (structured language query) injection is a type of cyber-attack used to take control of and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to insert malicious code into a databased via a malicious SQL statement. This gives them access to the sensitive information contained in the database.

Phishing

Phishing is when cybercriminals target victims with emails that appear to be from a legitimate company asking for sensitive information. Phishing attacks are often used to dupe people into handing over credit card data and other personal information.

Man-in-the-middle attack

A man-in-the-middle attack is a type of cyber threat where a cybercriminal intercepts communication between two individuals in order to steal data. For example, on an unsecure Wi-Fi network, an attacker could intercept data being passed from the victim’s device and the network.

Denial-of-service attack

A denial-of-service attack is where cybercriminals prevent a computer system from fulfilling legitimate requests by overwhelming the networks and servers with traffic. This renders the system unusable, preventing an organization from carrying out vital functions.

☺

Any queries ?