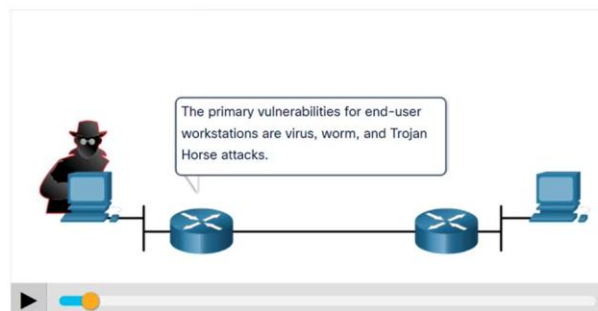


Module 14: Common Threats and Attacks

CyberOps Associate v1.0

Common Threats and Attacks Types of Malware

- Malware is a code or software designed to damage, disrupt, steal, or inflict some other 'bad' or illegitimate action on data, hosts, or networks.
- The three most common types of malware are Virus, Worm, and Trojan horse.
- Play the animation to view examples of the different malware types.



14.1 Malware

Viruses

- A virus is a type of malware that spreads by inserting a copy of itself into another program.
- After the program is run, viruses spread from one computer to another, thus infecting the computers.
- A simple virus may install itself at the first line of code in an executable file.
- Viruses can be harmless, for those that display a picture on the screen, or they can be destructive. They can also modify or delete files on the hard drive.
- Most viruses spread by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are a common type of virus.

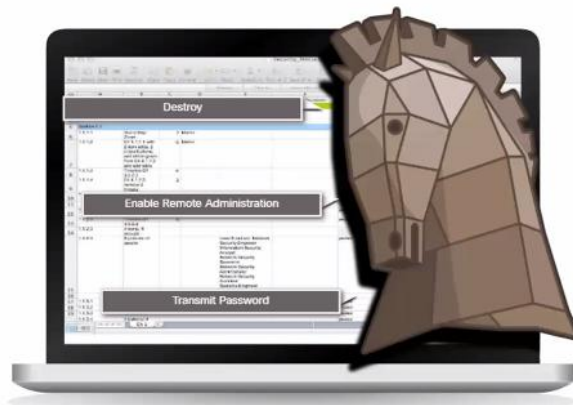
sono tutti programmi che devono essere eseguiti

Trojan Horses

- Trojan horse malware is a software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it.
- Trojans are found attached to online games.
- Users are commonly tricked into loading and executing the Trojan horse on their systems
- The Trojan horse concept is flexible.
- It can cause immediate damage, provide remote access to the system, or access through a back door.
- Custom-written Trojan horses with a specific target are difficult to detect.

Trojan Horses Classification

- Trojan horses are usually classified according to the damage that they cause, or the manner in which they breach a system.



Trojan Horses Classification (Contd.)

The types of Trojan horses are as follows:



Type of Trojan Horse	Description
Remote-access	Enables unauthorized remote access. ←
Data-sending	Provides the threat actor with sensitive data, such as passwords. ←
Destructive	Corrupts or deletes files. ←
Proxy	Uses the victim's computer as the source device to launch attacks and perform other illegal activities. ←
FTP	Enables unauthorized file transfer services on end devices.
Security software disabler	Stops antivirus programs or firewalls from functioning.
Denial of Service (DoS)	Slows or halts network activity.
Keylogger	Actively attempts to steal confidential information, such as credit card numbers, by recording keystrokes entered into a web form.

Common Threats and Attacks

Worms

- Computer worms are similar to viruses because they replicate themselves by independently exploiting vulnerabilities in networks.
- Worms can slow down networks as they spread from system to system.
- Worms can run without a host program.
- However, once the host is infected, the worm spreads rapidly over the network.
- In 2001, the Code Red worm had initially infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers.



Initial Code Red Worm Infection



Code Red Infection 19 hours later

Common Threats and Attacks

Worms (Contd.)

- The initial infection of the SQL Slammer worm is known as the worm that ate the internet.
- SQL Slammer was a Denial of Service (DoS) attack that exploited a buffer overflow bug in Microsoft's SQL Server.
- The number of infected servers doubled in size every 8.5 seconds.
- The infected servers did not have the updated patch that was released 6 months earlier.
- Hence it is essential for organizations to implement a security policy requiring updates and patches to be applied in a timely fashion.



Initial SQL Slammer Infection



SQL Slammer Infection 30 minutes later

Worm Components

Click Play in the figure to view the three components of worm attacks.



Worm Components (Contd.)

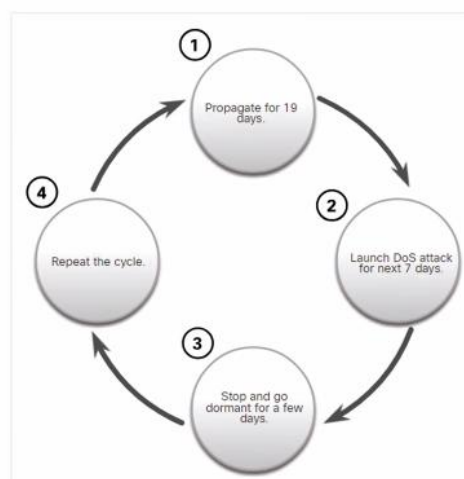
The three worm components are as follows:

- **Enabling vulnerability** - A worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse, on a vulnerable system.
- **Propagation mechanism** - After gaining access to a device, the worm replicates itself and locates new targets.
- **Payload** - Any malicious code that results in some action is a payload. Most often this is used to create a backdoor that allows a threat actor to access the infected host or to create a DoS attack.

- exploit
- vulnerability
- malicious (threat)

Worm Components (Contd.)

- Worms are self-contained programs that attack a system to exploit a known vulnerability.
- Upon successful exploitation, the worm copies itself from the attacking host to the newly exploited system and the cycle begins again.
- This propagation mechanism is commonly deployed in a way that is difficult to detect.
- **Note:** Worms never stop spreading on the internet. After they are released, worms continue to propagate until all possible sources of infection are properly patched.



Code Red Worm Propagation


Ransomware

- Ransomware is a malware that denies access to the infected computer system or its data.
- Ransomware frequently uses an encryption algorithm to encrypt system files and data.
- Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns.
- Social engineering is also used, when cybercriminals pretending to be security technicians make random calls at homes and persuade users to connect to a website that downloads ransomware to the user's computer.



Other Malware

The examples of modern malware are as follows:

Type of Malware	Description
Scareware 	Includes scam software which uses social engineering to shock or induce anxiety by creating the perception of a threat. It is generally directed at an unsuspecting user and attempts to persuade the user to infect a computer by taking action to address the bogus threat.
Phishing	Attempts to convince people to divulge sensitive information. Examples include receiving an email from their bank asking users to divulge their account and PIN numbers.
Rootkits	Installed on a compromised system. After it is installed, it continues to hide its intrusion and provide privileged access to the threat actor.
Spyware	Used to gather information about a user and send the information to another entity without the user's consent. Spyware can be a system monitor, Trojan horse, Adware, tracking cookies, and key loggers.
Adware	Displays annoying pop-ups to generate revenue for its author. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.



Common Malware Behaviors

- Computers infected with malware often exhibit one or more of the following symptoms:
 - Appearance of strange files, programs, or desktop icons
 - Antivirus and firewall programs are turning off or reconfiguring settings
 - Computer screen is freezing or system is crashing
 - Emails are spontaneously being sent without your knowledge to your contact list
 - Files have been modified or deleted
 - Increased CPU and/or memory usage
 - Problems connecting to networks
 - Slow computer or web browser speeds
 - Unknown processes or services running
 - Unknown TCP or UDP ports open
 - Connections are made to hosts on the Internet without user action
 - Strange computer behavior
- **Note:** Malware behavior is not limited to the above list.



