Network Security v1.0

/ Network Threats / Malware

Network Security

1 Securing Networks
1.0 Introduction
1.0.1 First Time in This Course
1.0.2 Student Resources
1.0.3 Ethical Hacking Statement
1.0.4 Inclusive Language
1.0.5 Video - Download and Install Packet Tracer
1.0.6 Video - Getting Started in Cisco Packet Tracer
1.0.7 Why Should I Take this Module?
1.0.8 What Will I Learn in this Module?
1.1 Current State of Affairs
1.2 Network Topology Overview

# Malware

2.3.1

## Types of Malware

End devices are especially prone to malware attacks. Therefore, the focus of this topic is on threats to end devices. Malware is short for malicious software or malicious code. It is code or software that is specifically designed to damage, disrupt, steal, or generally inflict some other “bad” or illegitimate action on data, hosts, or networks. It is important to know about malware because threat actors and online criminals frequently try to trick users into installing malware to help exploit security gaps. In addition, malware morphs so rapidly that malware-related security incidents are extremely common because antimalware software cannot be updated quickly enough to stop the new threats.

Play the animation to view examples of the three most common types of malware; virus, worm, and Trojan horse.

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

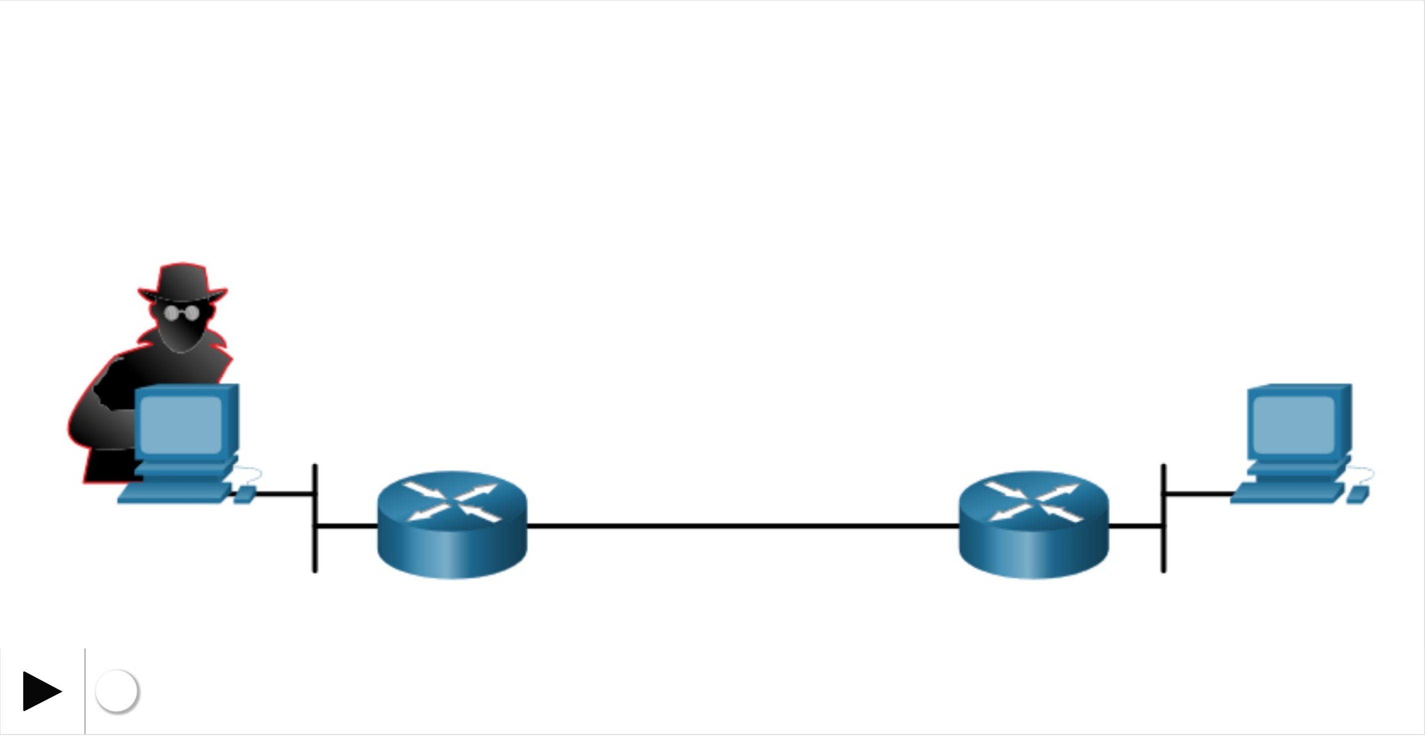
1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview



2.3.2

## 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 then spread from one computer to another, infecting the computers. Most viruses require human help to spread. For example, when someone connects an infected USB drive to their PC, the virus will enter the PC. The virus may then infect a new USB drive, and spread to new PCs. Viruses can lay dormant for an extended period and then activate at a specific time and date.

A simple virus may install itself at the first line of code in an executable file. When activated, the virus might check the disk for other executables so that it can infect all the files it has not yet infected. Viruses can be harmless, such as those that display a picture on the screen, or they can be destructive, such as those that modify or delete files on the hard drive. Viruses can also be programmed to mutate to avoid detection.

Most viruses are now spread by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are a common type of virus.

2.3.3

# Trojan Horses

The term Trojan horse originated from Greek mythology. Greek warriors offered the people of Troy (the Trojans) a giant hollow horse as a gift. The Trojans brought the giant horse into their walled city, unaware that it contained many Greek warriors. At night, after most Trojans were asleep, the warriors burst out of the horse, opened the city gates, and allowed a sizeable force to enter and take over the city.

Trojan horse malware is software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it, as shown in the figure.

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

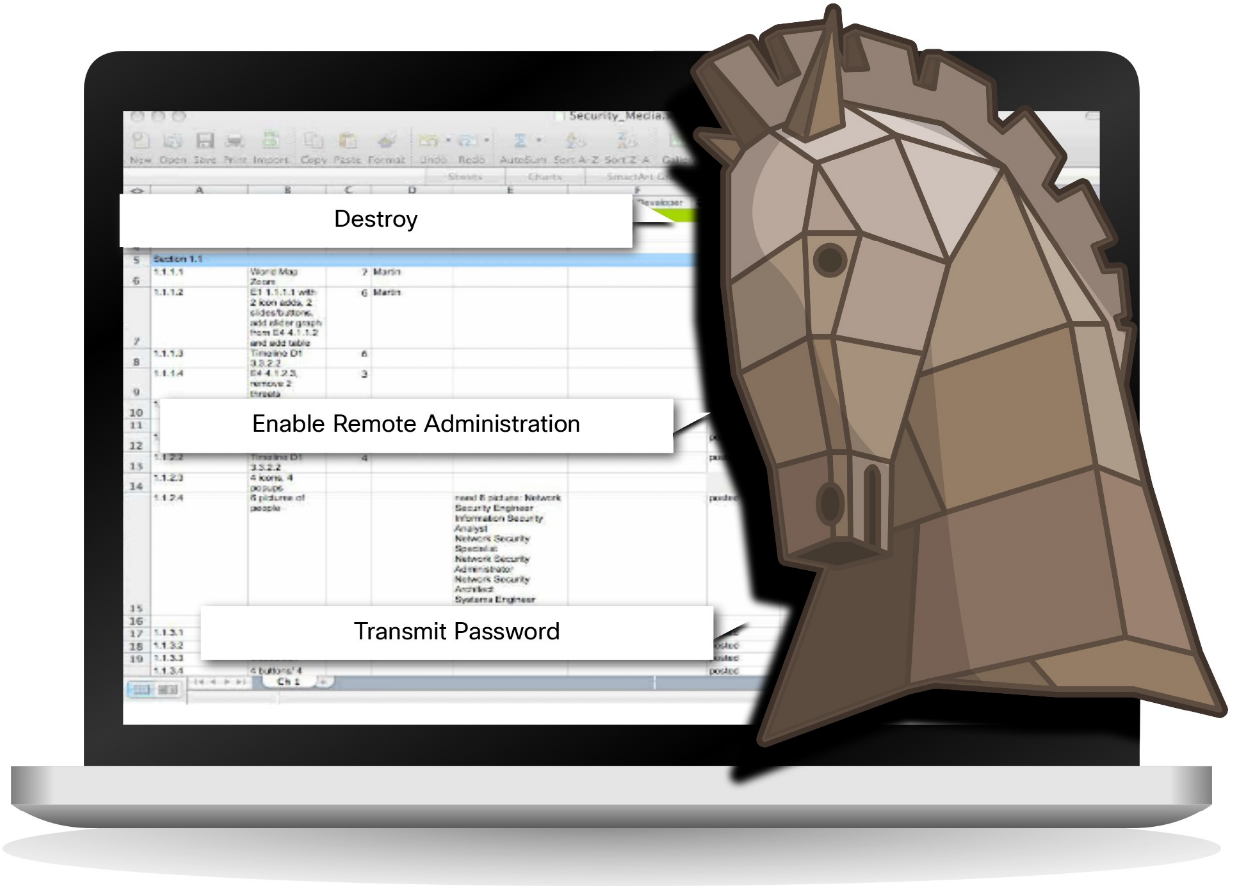
1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview



Often, Trojans are found attached to online games. Users are commonly tricked into loading and executing the Trojan horse on their systems. While playing the game, the user will not notice a problem. In the background, the Trojan horse has been installed on the user's system. The malicious code from the Trojan horse continues operating even after the game has been closed.

The Trojan horse concept is flexible. It can cause immediate damage, provide remote access to the system, or access through a back door. It can also perform actions as instructed remotely, such as "send me the password file once per week." This tendency of malware to send data back to the cybercriminal highlights the need to monitor outbound traffic for attack indicators.

Network Security

1 Securing Networks
1.0 Introduction
1.0.1 First Time in This Course
1.0.2 Student Resources
1.0.3 Ethical Hacking Statement
1.0.4 Inclusive Language
1.0.5 Video - Download and Install Packet Tracer
1.0.6 Video - Getting Started in Cisco Packet Tracer
1.0.7 Why Should I Take this Module?
1.0.8 What Will I Learn in this Module?
1.1 Current State of Affairs
1.2 Network Topology Overview

Custom-written Trojan horses, such as those with a specific target, are difficult to detect.

2.3.4

## Trojan Horse Classification

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

| 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. |

2.3.5

## Worms

Computer worms are similar to viruses because they replicate and can cause the same type of damage. Specifically, worms

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview

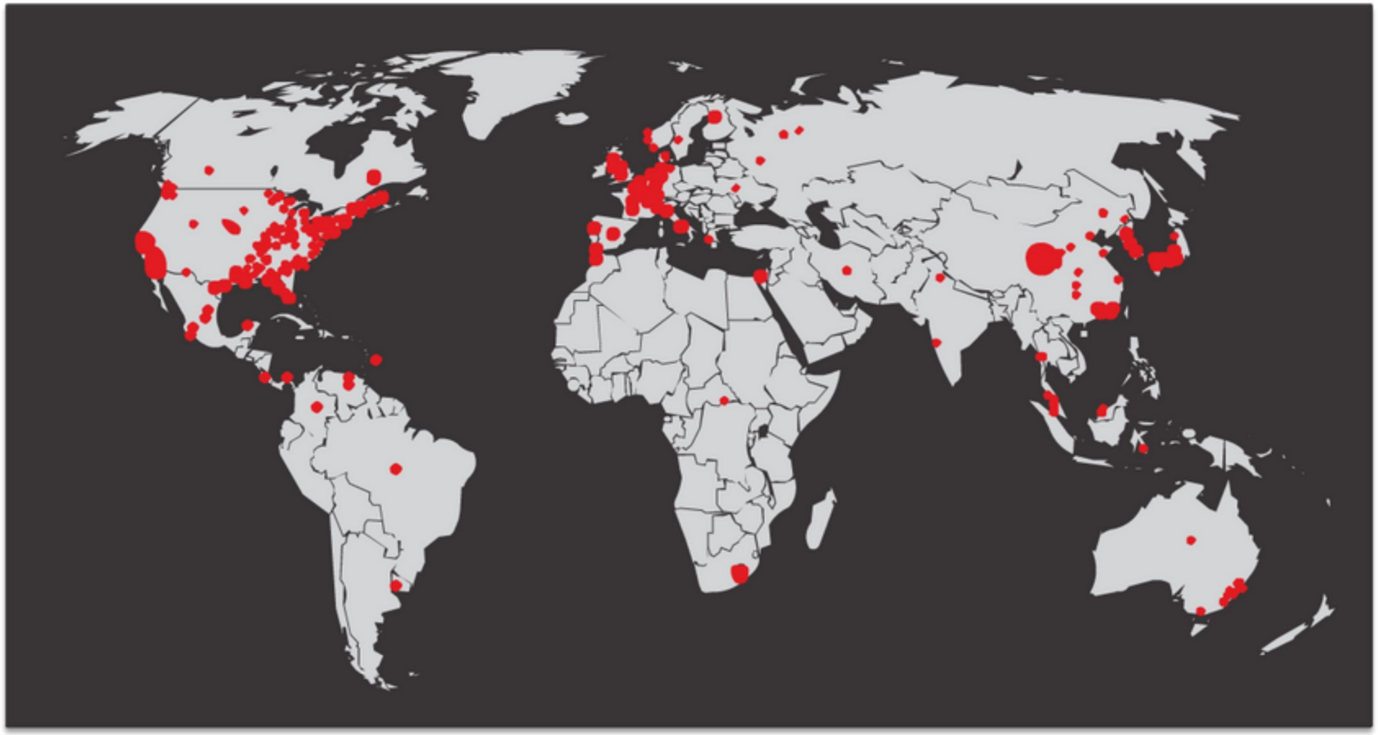
replicate themselves by independently exploiting vulnerabilities in networks. Worms can slow down networks as they spread from system to system.

Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, they no longer require user participation. After a host is infected, the worm is able to spread very quickly over the network.

Worms are responsible for some of the most devastating attacks on the internet. 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



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. At its peak, the number of infected servers doubled in size every 8.5 seconds. This is why it was able to infect 250,000+ hosts within 30 minutes. When it was released on the weekend of January 25, 2003, it disrupted the internet, financial institutions, ATM cash machines, and more. Ironically, a patch for this vulnerability had been released 6 months earlier. The infected servers did not have the updated patch applied. This was a wake-up call for many organizations to implement a security policy requiring that updates and patches be applied in a timely fashion.

Network Security

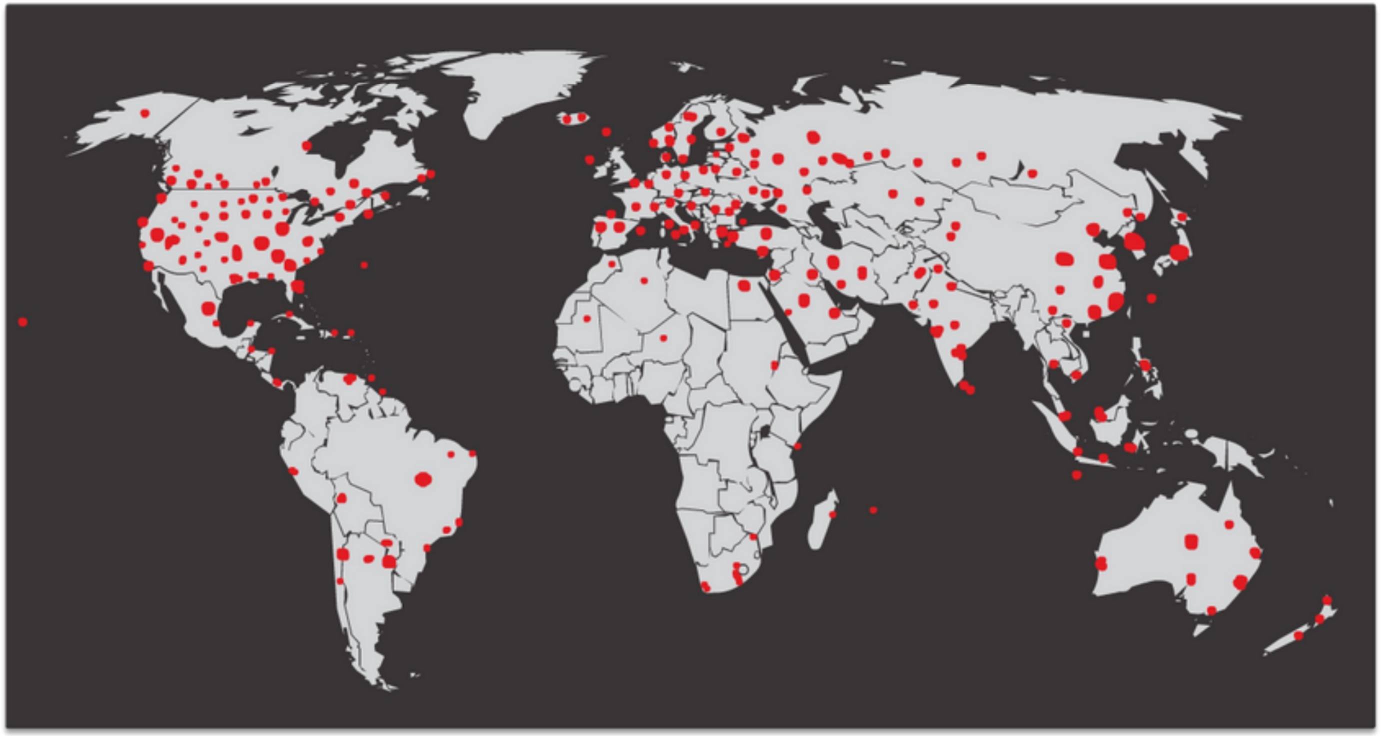
1 Securing Networks
1.0 Introduction
1.0.1 First Time in This Course
1.0.2 Student Resources
1.0.3 Ethical Hacking Statement
1.0.4 Inclusive Language
1.0.5 Video - Download and Install Packet Tracer
1.0.6 Video - Getting Started in Cisco Packet Tracer
1.0.7 Why Should I Take this Module?
1.0.8 What Will I Learn in this Module?
1.1 Current State of Affairs
1.2 Network Topology Overview

Network Security

1 Securing Networks
1.0 Introduction
1.0.1 First Time in This Course
1.0.2 Student Resources
1.0.3 Ethical Hacking Statement
1.0.4 Inclusive Language
1.0.5 Video - Download and Install Packet Tracer
1.0.6 Video - Getting Started in Cisco Packet Tracer
1.0.7 Why Should I Take this Module?
1.0.8 What Will I Learn in this Module?
1.1 Current State of Affairs
1.2 Network Topology Overview

Initial SQL Slammer Infection

SQL Slammer Infection 30 minutes later



Worms share similar characteristics. They all exploit an enabling vulnerability, have a way to propagate themselves, and they all contain a payload.

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview

2.3.6

# Worm Components

Despite the mitigation techniques that have emerged over the years, worms have continued to evolve and pose a persistent threat. Worms have become more sophisticated over time, but they still tend to be based on exploiting weaknesses in software applications.

## Common Worm Pattern

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

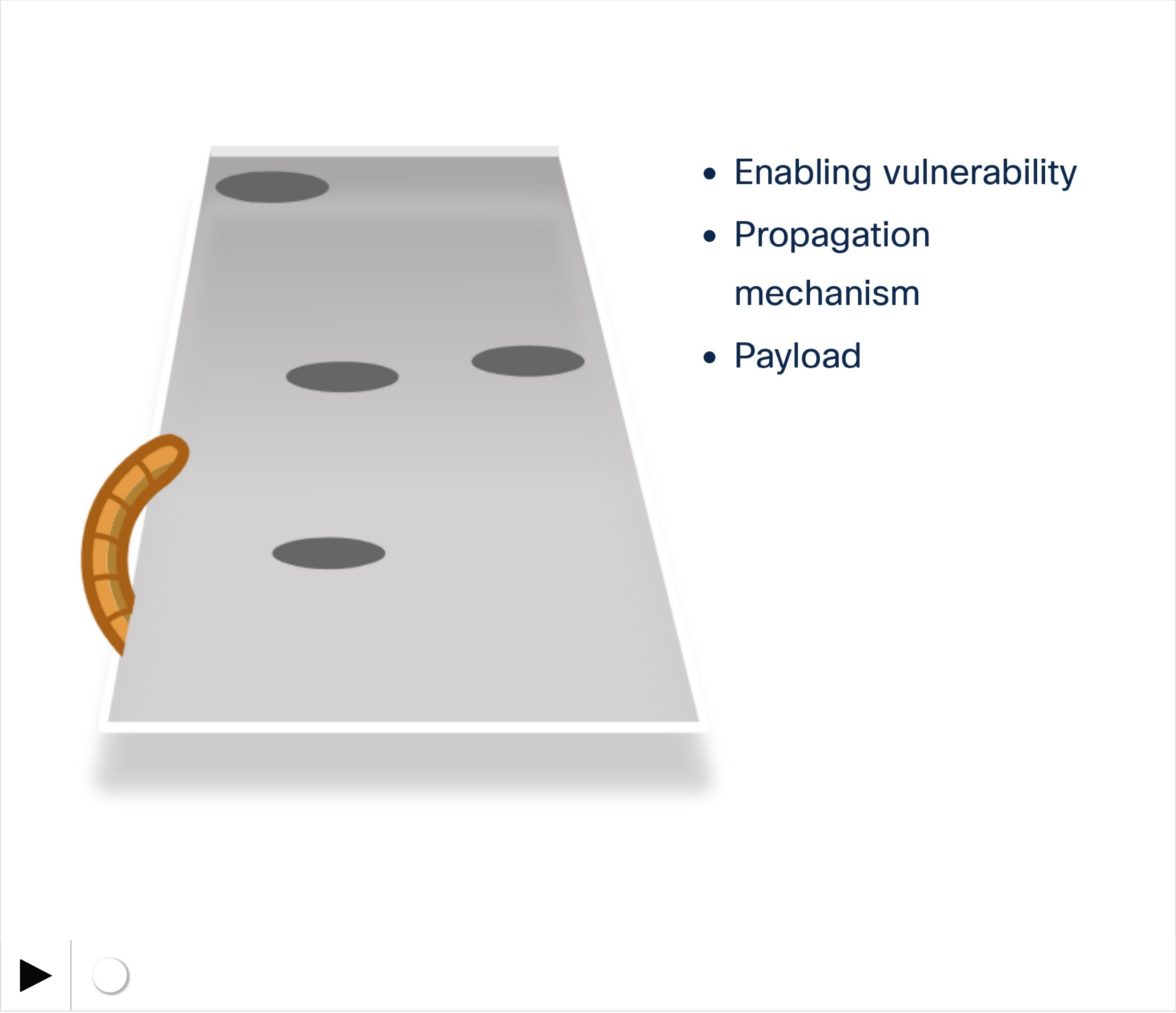
1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview



- Enabling vulnerability
- Propagation mechanism
- Payload

Most worm attacks consist of three components, as listed in the animation above.

- **Enabling vulnerability** - A worm installs itself using an exploit mechanism, such as an email attachment, an executable file,

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview

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 access to the infected host or to create a DoS attack.

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. Their propagation mechanisms are commonly deployed in a way that is difficult to detect.

The propagation technique used by the Code Red worm is shown in the figure.

## Code Red Worm Propagation

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

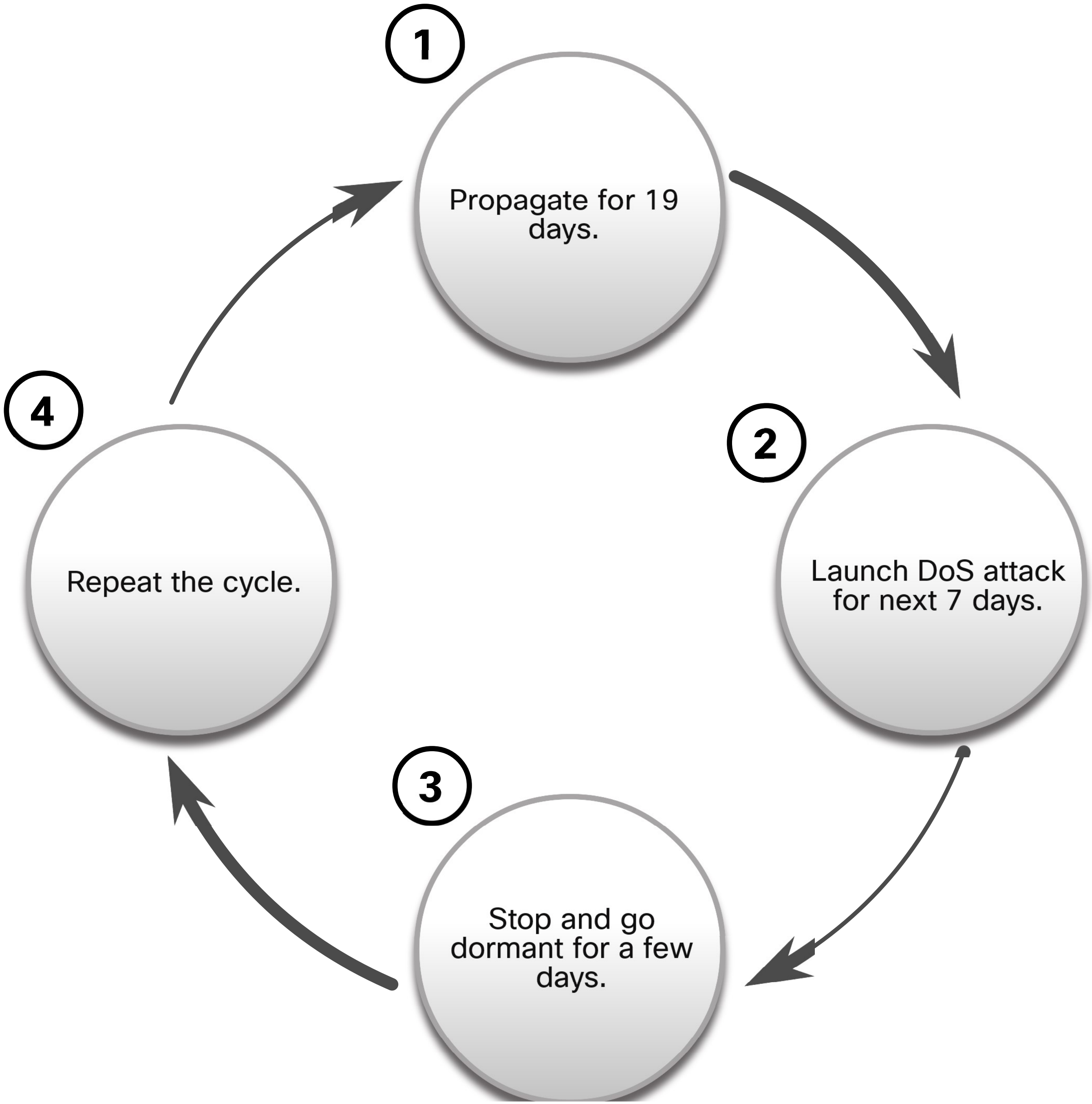
1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview



1 Propagate for 19 days.

2 Launch DoS attack for next 7 days.

3 Stop and go dormant for a few days.

4 Repeat the cycle.

1.3 Securing Networks Summary

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview

**Note**: Worms never really stop spreading on the internet. After they are released, worms continue to propagate until all possible sources of infection are properly patched.

2.3.7

## Ransomware

Threat actors have used viruses, worms, and Trojan horses to carry their payloads and for other malicious reasons. However, malware continues to evolve.

Currently, the most dominating malware is ransomware. Ransomware is malware that denies access to the infected computer system or its data. The cybercriminals then demand payment to release the computer system.

Ransomware has evolved to become the most profitable malware type in history. In the first half of 2016, ransomware campaigns targeting both individual and enterprise users became more widespread and potent.

There are dozens of ransomware variants. Ransomware frequently uses an encryption algorithm to encrypt system files and data. The majority of known ransomware encryption algorithms cannot be easily decrypted, leaving victims with little option but to pay the asking price. Payments are typically paid in Bitcoin because users of bitcoin can remain anonymous. Bitcoin is an open-source, digital currency that nobody owns or controls.

Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns. Social engineering is also used, as when cybercriminals who identify themselves as security technicians call homes and persuade users to connect to a website that downloads the ransomware to the user’s computer.

2.3.8

## Other Malware

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview

These are some examples of the varieties of modern malware:

| **Type of Malware** | **Description** |
|---|---|
| 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. |
| 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. |

This list will continue to grow as the internet evolves. New malware will always be developed. A major goal of cybersecurity operations is to learn about new malware and how to promptly mitigate it.

2.3.9

# Common Malware Behaviors

Cybercriminals continually modify malware code to change how it spreads and infects computers. However, most produce similar symptoms that can be detected through network and device log monitoring.

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

Network Security

1 Securing Networks
1.0 Introduction
1.0.1 First Time in This Course
1.0.2 Student Resources
1.0.3 Ethical Hacking Statement
1.0.4 Inclusive Language
1.0.5 Video - Download and Install Packet Tracer
1.0.6 Video - Getting Started in Cisco Packet Tracer
1.0.7 Why Should I Take this Module?
1.0.8 What Will I Learn in this Module?
1.1 Current State of Affairs
1.2 Network Topology Overview

- 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.

2.3.10

## Check Your Understanding - Malware

Check your understanding of malware by answering the following questions.

1. What type of malware executes arbitrary code and installs copies of itself in the memory of the infected computer? The main purpose of this malware is to automatically replicate from system to system across the network.

○ trojan horse
○ adware
○ ransomware
○ worm

2. What type of malware typically displays annoying pop-ups to generate revenue for its author?

○ adware

Network Security

1 Securing Networks

1.0 Introduction

1.0.1 First Time in This Course

1.0.2 Student Resources

1.0.3 Ethical Hacking Statement

1.0.4 Inclusive Language

1.0.5 Video - Download and Install Packet Tracer

1.0.6 Video - Getting Started in Cisco Packet Tracer

1.0.7 Why Should I Take this Module?

1.0.8 What Will I Learn in this Module?

1.1 Current State of Affairs

1.2 Network Topology Overview

○ ransomware

○ scareware

○ phishing

3. What type of malware encrypts all data on a drive and demands payment in Bitcoin cryptocurrence to unencrypt the files?

○ phishing

○ scareware

○ ransomware

○ virus

4. What type of malware attempts to convince people to divulge their personally identifable information (PII)?

○ phishing

○ rootkit

○ ransomware

○ trojan horse

Check

Show Me

Reset

‹ 2.2 Threat Actor Tools

2.4 Common Network Attacks - Reconnaissance, Access, ... ›