session 5

Types of Malware and Their Characteristics

Malware, short for "malicious software," encompasses a variety of harmful programs designed to disrupt, damage, or gain unauthorized access to computer systems. Below are five common types of malware, their unique characteristics, behaviors, and real-life examples.

---

1. Viruses

Characteristics & Behaviors:

- A computer virus is a self-replicating program that attaches itself to a host file or program.
- It requires user interaction (e.g., opening an infected file) to spread.
- Once executed, it can corrupt files, slow down systems, or even render devices unusable.

How It Spreads:

- Through infected email attachments, downloads, or removable media like USB drives.
- Often hidden within seemingly harmless files such as Word documents or software installers.

Impact on Infected Systems:

- File corruption or deletion.
- System crashes or instability.
- Potential propagation of further malware.

Real-Life Example:

- **ILOVEYOU Virus (2000):** Spread via email attachments with the subject "ILOVEYOU." It overwrote files and caused approximately $10 billion in damages globally.

---

2. Worms

Characteristics & Behaviors:

- Worms are standalone programs that replicate themselves without needing a host file or user action.
- They exploit network vulnerabilities to spread rapidly across systems.

How It Spreads:

- Through network connections, email attachments, or file-sharing platforms.
- Often targets unpatched systems.

Impact on Infected Systems:

- Overwhelms network resources, causing slowdowns or outages.
- Can carry payloads for additional malicious activities like data theft.

Real-Life Example:

- **WannaCry (2017):** A ransomware worm that exploited a Windows vulnerability. It encrypted user files and demanded Bitcoin payments, affecting over 200,000 systems in 150 countries.

---

3. Trojan Horses

Characteristics & Behaviors:

- A Trojan appears as legitimate software but contains malicious code.
- Unlike viruses and worms, Trojans do not self-replicate.

How It Spreads:

- Through downloads of seemingly trustworthy software or attachments.
- Embedded in cracked software, games, or utility programs.

Impact on Infected Systems:

- Steals sensitive data, including login credentials or financial information.
- Provides backdoor access for attackers to control the system.

Real-Life Example:

- **Zeus Trojan:** Used to steal banking credentials. It infected millions of systems worldwide, targeting online banking platforms.

---

4. Ransomware

Characteristics & Behaviors:

- Encrypts files or locks systems, demanding payment (often in cryptocurrency) to restore access.
- Displays a ransom note with payment instructions.

How It Spreads:

- Through phishing emails containing malicious links or attachments.
- Via malicious websites or exploit kits targeting software vulnerabilities.

Impact on Infected Systems:

- Total loss of access to critical data.
- Severe financial losses due to ransom payments or downtime.

Real-Life Example:

- **CryptoLocker (2013):** A ransomware campaign that encrypted files on Windows systems. Victims were forced to pay hundreds of dollars to regain access.

---

5. Spyware

Characteristics & Behaviors:

- Designed to secretly monitor and collect user activity and data.
- Often runs in the background without the user’s knowledge.

How It Spreads:

- Bundled with legitimate software or downloaded from malicious websites.
- Delivered via phishing campaigns.

Impact on Infected Systems:

- Harvests sensitive data, such as keystrokes, passwords, or browsing history.
- Can lead to identity theft or unauthorized access to financial accounts.

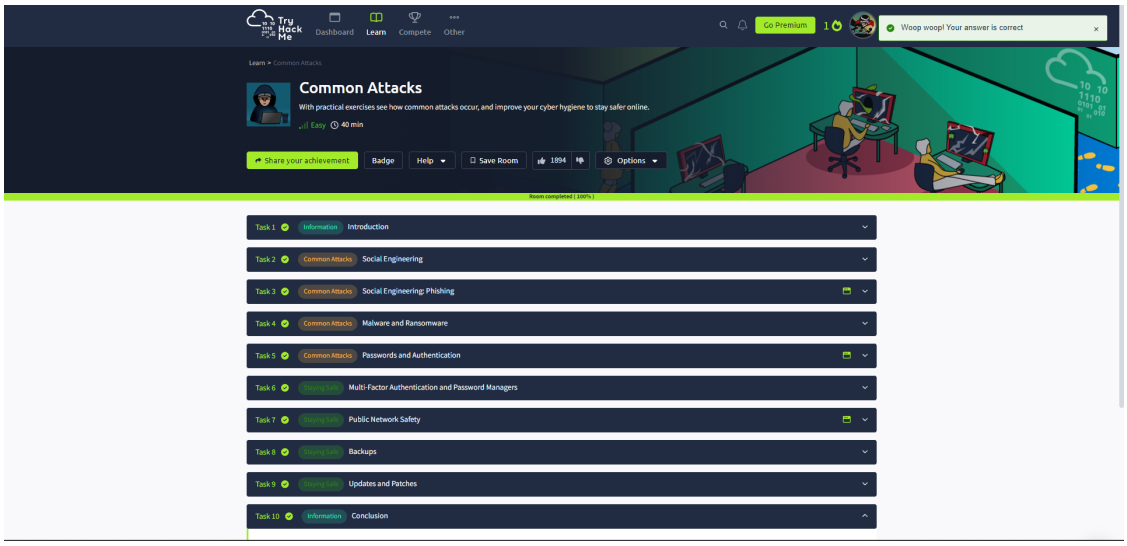
Real-Life Example:

- **Pegasus Spyware:** Used to infiltrate smartphones, enabling attackers to eavesdrop on calls, read messages, and track user locations. It targeted high-profile individuals, including journalists and activists.

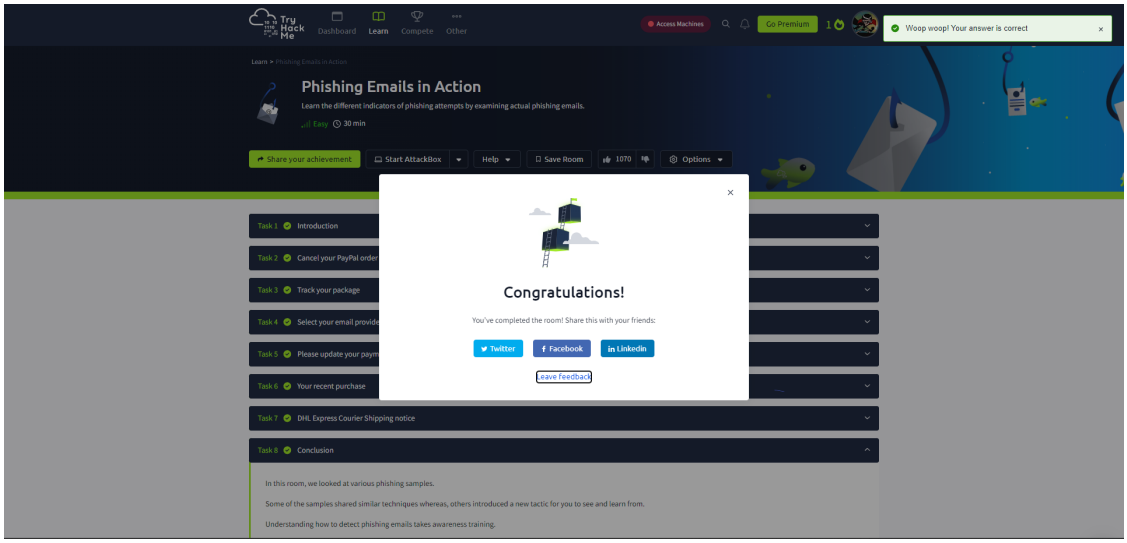
Conclusion

Malware comes in various forms, each with distinct characteristics and behaviors. Understanding these types helps in implementing effective security measures such as up-to-date antivirus programs, firewalls, and regular system updates to mitigate risks.

COMMON ATTACKS



Phishing Emails in Action


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
Woop woop! Your answer is correct
Learn > Phishing Emails in Action
Phishing Emails in Action
Learn the different indicators of phishing attempts by examining actual phishing emails.
Easy
30 min
Share your achievement
Start AttackBox
Help
Save Room
1070
Options
Task 1 Introduction
Task 2 Cancel your PayPal order
Task 3 Track your package
Task 4 Select your email provide
Task 5 Please update your paym
Task 6 Your recent purchase
Task 7 DHL Express Courier Shipping notice
Task 8 Conclusion
In this room, we looked at various phishing samples.
Some of the samples shared similar techniques whereas, others introduced a new tactic for you to see and learn from.
Understanding how to detect phishing emails takes awareness training.
Congratulations!
You've completed the room! Share this with your friends:
Twitter
Facebook
LinkedIn
Leave Feedback