Exercise Week 6: Malware Incidents (Individual)

Due Feb 27 at 11:59pm **Points** 7 **Questions** 7
Available until Feb 27 at 11:59pm **Time Limit** None

Instructions

Answer the following questions applying concepts from NIST 800-83 Guide to Malware Incident Prevention and Handling. For each incident, identify the type of malware attack.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	8 minutes	7 out of 7

Score for this quiz: **7** out of 7
Submitted Jan 24 at 12:23pm
This attempt took 8 minutes.

Question 1

1 / 1 pts

The Machiavellian malware attacked its victims by taking control of their computer. The attackers lured the victim to a compromised website where the malware was downloaded onto the victim's computer. The malware installed itself on the first part of the computer's hard drive to be read on startup. The malware then made changes to the Windows kernel to hide its existence while attackers took control.

What type of malware attack was this?

- Ransomware
- Rootkit

Correct!

- Whaling
- Malicious Mobile Code

Question 2

1 / 1 pts

The Storm Worm malware attacked its victims using an email with the subject line "230 dead as storm batters Europe." When a victim opened the email and clicked on the link, the malware downloaded into their computer. The downloaded malware contained a program that was executed to make the compromised computer part of a botnet to facilitate the attacker's purpose such as executing a Denial of Service attack on another victim.

What kind of malware attack was this?

Correct!

- (selected) Trojan Horse
- Spear Phishing
- Rootkit
- Whaling

Question 3

1 / 1 pts

The Stuxnet malware attacked industrial control systems after being installed on a connected computer, likely using a thumb drive. Once introduced, it quietly spread throughout the SCADA equipment over

years. While the damage was significant, it was not catastrophic. This allowed the attackers to escape discovery over this long period of time.

What kind of malware attack was this?

- Drive-By-Download
- Spear Phishing
- Advanced Persistent Threat

Correct!

- Keystroke Logger

Question 4

1 / 1 pts

The Bandook malware attacked executives by stealing their data. Attackers sent carefully crafted emails to CEOs that appeared to be from the Better Business Bureau providing details of a complaint. When the victim downloaded the false case documents, their computer was infected with the malware that harvested sensitive information from the executive.

What kind of malware attack was this?

- Malicious Mobile Code

Correct!

- Whaling
- Ransomware
- Rootkit

Question 5

1 / 1 pts

The MyDoom malware attacked its victims using an infected email attachment. Once installed on the victim's computer, it listened for commands on TCP port 3127. The attackers were able to send commands through this port to send infected email to everyone in the victim's address book. The infected computers were also used to launch Denial of Service attacks on other victims.

What kind of malware attack was this?

- Web Browser Plug-In
- Backdoor

Correct!

- Ransomware
- Keystroke Logger

Question 6

1 / 1 pts

The Olympic Vision malware attacked its victims by stealing information. The malware was installed on the victim's computer when they opened a file attached to a spear phishing email. Once executed, the malware connected to an external site where the attacker could now capture sensitive information such as usernames, passwords, and account numbers as the victim entered them throughout the day.

What kind of malware attack was this?

- Web Browser Plug-In
- Malicious Mobile Code
- Drive-By-Download
- Keystroke Logger

Correct!

Question 7

1 / 1 pts

The WannaCry malware attacked its victims by exploiting a Microsoft Windows operating system vulnerability. Despite a security patch developed two months before the attack began, the attackers found many victims that had not yet applied the patch. The malware encrypted files on the victim's computer making them inaccessible to the victim. The attackers threatened to delete the files unless the victim paid hundreds of dollars in bitcoin.

What kind of malware attack was this?

- Web Browser Plug-In
- Advanced Persistent Threat
- Rootkit
- Ransomware

Correct!

Quiz Score: **7** out of 7