Discussion Questions: Stuxnet Malware

Watch the following video to learn more about the Stuxnet (14 minutes).

<https://www.youtube.com/watch?v=nd1x0csO3hU>

*1) What are some of the key components of the Stuxnet malware and their functions?*

**ANSWER:**

Rootkit (stealth), payload (PLC manipulation), propagation (exploits).

**Possible Wrong Answers:**

Spyware (data theft), keylogger (password capture), worm (network spread)

Adware (advertising), ransomware (data encryption), Trojan (backdoor access)

Antivirus (protection), firewall (security), sandbox (isolation)

*2) What were the vulnerabilities that Stuxnet exploited?*

**ANSWER:**

Zero-Day

**Possible Wrong Answers:**

Known vulnerabilities with patches available

Social engineering vulnerabilities

Hardware vulnerabilities

*3) What impact did Stuxnet have on the targeted industrial control systems?*

**ANSWER:**

Damaged centrifuges, disrupted uranium enrichment.

**Possible Wrong Answers:**

Increased production efficiency, reduced downtime

Enhanced security measures, improved control systems

Increased power output, reduced energy consumption

*4) Discuss the geopolitical implications of the Stuxnet attack on the Siemens Industrial Control Software. Who were the suspected authors?*

**ANSWER**:

Increased cyber warfare awareness; Israel/US suspected.

**Possible Wrong Answers:**

Increased international tension; China suspected

Decreased global cooperation; Russia suspected

Reduced cybersecurity focus; France/Brazil suspected

*5) What were the long-term global effects this attack had?*

**ANSWERs:**

Increased focus on industrial cybersecurity

Increased awareness of state-sponsored cyber warfare

**Possible Wrong Answers:**

reduced global cybersecurity budgets

Enhanced privacy regulations,