### **Discussion Questions for the Mirai IoT Botnet in DDoS Attacks**

Answer the following questions based on the information provided about the Mirai IoT botnet. You are encouraged to use diagrams and charts to illustrate your ideas.

**1. What happened during the Mirai IoT botnet attacks of 2016?**

* A) Hackers stole sensitive data from IoT devices and sold it on the dark web.
* B) The Mirai botnet exploited IoT devices with weak security settings to carry out massive Distributed Denial of Service (DDoS) attacks on major websites and services.
* C) IoT devices were used to spread ransomware to corporate networks.
* D) Mirai targeted only mobile devices, shutting down global cellular networks.

**Answer: B) The Mirai botnet exploited IoT devices with weak security settings to carry out massive Distributed Denial of Service (DDoS) attacks on major websites and services.**

**2. What are two effective security mechanisms to prevent vulnerabilities in IoT devices like those exploited by the Mirai botnet?**

* A) Require unique, strong passwords for all devices and ensure firmware updates are regularly applied.
* B) Allow default passwords to stay unchanged for ease of use.
* C) Disable firewalls to improve device performance.
* D) Only use encryption when sending data over local networks.

**Answer: A) Require unique, strong passwords for all devices and ensure firmware updates are regularly applied.**

**3. As a cybersecurity consultant, how would you advise manufacturers to improve the security of IoT devices?**

* A) Require unique default credentials, implement regular automatic firmware updates, and provide user-friendly security configuration tools.
* B) Use the same default credentials for all devices to simplify user setup.
* C) Avoid updating device software to reduce complexity.
* D) Rely on users to manually secure devices after purchase.

**Answer: A) Require unique default credentials, implement regular automatic firmware updates, and provide user-friendly security configuration tools.**

**4. How can companies defend against DDoS attacks originating from botnets like Mirai?**

* A) Use DDoS mitigation services, implement rate limiting, and deploy Web Application Firewalls (WAFs) to block traffic from malicious sources.
* B) Increase bandwidth to handle all incoming traffic without restrictions.
* C) Shut down all external-facing services.
* D) Only allow traffic during business hours.

**Answer: A) Use DDoS mitigation services, implement rate limiting, and deploy Web Application Firewalls (WAFs) to block traffic from malicious sources.**

**5. How can organizations enhance security monitoring for IoT networks to detect malware like Mirai?**

* A) Implement network traffic analysis tools, deploy Intrusion Detection Systems (IDS) specifically designed for IoT, and use automated threat intelligence to detect suspicious behavior.
* B) Disable logging to save storage space.
* C) Perform manual device checks only once a year.
* D) Only monitor traditional IT devices, ignoring IoT systems.

**Answer: A) Implement network traffic analysis tools, deploy Intrusion Detection Systems (IDS) specifically designed for IoT, and use automated threat intelligence to detect suspicious behavior.**

**6. As the person responsible for IoT security at a large company, what measures would you implement to enhance security while maintaining operational efficiency?**

* A) Use network segmentation to isolate IoT devices, implement device-level authentication, and conduct regular vulnerability assessments to ensure security without disrupting operations.
* B) Disable all security measures for IoT devices to improve performance.
* C) Allow IoT devices to be accessed from any network without restrictions.
* D) Avoid updating IoT devices to prevent downtime.

**Answer: A) Use network segmentation to isolate IoT devices, implement device-level authentication, and conduct regular vulnerability assessments to ensure security without disrupting operations.**

**7. How should companies enforce strong password practices for IoT devices?**

* A) Mandate unique, complex passwords for all devices, enforce password expiration policies, and require multi-factor authentication where possible.
* B) Use default credentials for all devices for consistency.
* C) Disable password requirements to speed up device access.
* D) Only require passwords for remote access.

**Answer: A) Mandate unique, complex passwords for all devices, enforce password expiration policies, and require multi-factor authentication where possible.**

**8. What steps should the cybersecurity community take to mitigate the risks associated with open-source malware like Mirai?**

* A) Share threat intelligence, collaborate on patch development, and encourage manufacturers to harden devices against exploitation of open-source malware.
* B) Disable all updates on vulnerable devices to avoid further exploits.
* C) Ignore open-source malware to reduce unnecessary panic.
* D) Provide instructions for companies to develop their own malware defenses privately.

**Answer: A) Share threat intelligence, collaborate on patch development, and encourage manufacturers to harden devices against exploitation of open-source malware.**

**9. What IT weaknesses were present in IoT devices targeted by Mirai?**

* A) Use of default or weak credentials, lack of automatic firmware updates, and poor access control settings.
* B) Excessive monitoring of internal traffic.
* C) Strong, unique passwords on all devices.
* D) Constant firmware updates that slowed device performance.

**Answer: A) Use of default or weak credentials, lack of automatic firmware updates, and poor access control settings.**

**10. As the person responsible for securing a network of IoT devices, how would you improve overall IoT security to prevent botnet attacks like Mirai?**

* A) Implement unique credentials for all devices, use network segmentation, ensure regular software updates, and deploy IoT-specific security monitoring tools.
* B) Disable all device updates to improve performance.
* C) Allow unrestricted network access to IoT devices for ease of use.
* D) Use the same credentials for all devices to simplify management.

**Answer: A) Implement unique credentials for all devices, use network segmentation, ensure regular software updates, and deploy IoT-specific security monitoring tools.**