Question: You are a security operations system analyst and helpful cybersecurity assistant that generates detailed incident response playbooks based on NIST guidelines. please generate a playbook for a potential attacks similar to Havex malware incidents effectively?

Answer:

Title: Incident Response Playbook for Potential Attack Similar to Havex Malware

1. Preparation:

Objective: Establish contacts, define procedures, and gather information to save time during an incident.

- \*\*Internal Preparation\*\*:

- \*\*Communication Plan\*\*:

- Prepare strategies for informing stakeholders about potential Havex malware incidents.

- Test and refine deployment procedures for incident notifications.

- \*\*Deploy Security Protocols\*\*:

- Implement and regularly update DKIM, DMARC, and SPF for email security.

- Enforce multi-factor authentication (MFA) for critical systems.

- \*\*Monitor Threat Landscape\*\*:

- Continuously monitor cybersquatted domains and gather abuse information for takedown requests.

- \*\*Internal Contacts\*\*:

- Maintain an updated list of personnel involved in domain registration and cybersecurity decision-making.

- Ensure contracts allow rapid decisions during cyber incidents.

- \*\*External Contacts\*\*:

- Establish and maintain 24/7 contact channels (dedicated email, web forms, social media).

- Maintain takedown contacts (hosting companies, registries, email providers).

- Collaborate with global CERTs for incident assistance.

- \*\*Awareness and Training\*\*:

- \*\*Customer Awareness\*\*:

- Educate customers about phishing and malware risks.

- \*\*Internal Awareness\*\*:

- Conduct periodic phishing and malware awareness campaigns.

- Train staff on safe handling of attachments and URLs.

2. Detection and Analysis:

Objective: Detect the incident, determine its scope, and involve appropriate parties.

- \*\*Detection\*\*:

- \*\*Monitor Entry Points\*\*:

- Continuously monitor email, web forms, and other contact points.

- Deploy spam traps and use phishing repositories (PhishTank, Google Safe Browsing).

- \*\*Web Logs\*\*:

- Check logs for suspicious referrers indicating phishing redirects.

- \*\*Scoping the Attack\*\*:

- Assess impact by determining targeted users and compromised accounts.

- \*\*Analyzing the Malware\*\*:

- Analyze messages and attachments in sandbox environments.

- Use threat intelligence services to analyze links, domains, and hostnames.

- \*\*Evidence Collection\*\*:

- Document phishing pages using tools like HTTrack and capture screenshots of related pages.

3. Containment:

Objective: Mitigate the attack’s effects on the targeted environment.

- \*\*Block IOCs\*\*:

- Block network indicators on DNS, firewalls, or proxies.

- Filter emails based on identified malicious senders and artifacts.

- \*\*Purge Malicious Emails\*\*:

- Attempt to delete phishing emails from user inboxes.

- \*\*DNS Sinkhole\*\*:

- Apply DNS sinkholes for suspicious URLs.

- \*\*Communication\*\*:

- Inform collaborators and deploy alert pages about the phishing attack.

4. Eradication:

Objective: Remove the threat.

- \*\*Credential Management\*\*:

- Change or temporarily block compromised account credentials.

- \*\*Law Enforcement and Regulators\*\*:

- Contact law enforcement and regulators if targeted.

- \*\*Patch Vulnerabilities\*\*:

- Identify and patch vulnerabilities exploited by Havex malware.

- \*\*CERT Coordination\*\*:

- Engage with local CERTs for support and information sharing.

5. Recovery:

Objective: Restore systems to normal operations.

- \*\*Ensure Remediation\*\*:

- Verify fraudulent pages and email addresses are taken down.

- Monitor fraudulent URLs to ensure they do not reappear.

- \*\*Infrastructure Recovery\*\*:

- Recover authentication and infrastructure following malware compromise guidelines.

- \*\*System Validation\*\*:

- Validate ICS and related systems before resuming normal operations.

- \*\*Remove Warning Pages\*\*:

- Remove warning pages after the phishing campaign ends.

6. Lessons Learned:

Objective: Document the incident’s details, discuss lessons learned, and adjust plans and defenses.

- \*\*Reporting\*\*:

- Document the incident cause, actions, timelines, successes, failures, and cost in a crisis report.

- \*\*Post-Incident Review\*\*:

- Assess preparation steps to improve future response efficiency.

- Update contact lists and identify useful relationships for future incidents.

- \*\*Security Enhancements\*\*:

- Implement lessons-learned security measures and update policies regularly.

- \*\*Legal Considerations\*\*:

- Collaborate with legal teams for potential legal actions.

- \*\*Continuous Improvement\*\*:

- Regularly review and refine incident response capabilities.