Incident Response Playbook

1. Identify and Categorize the Incident

Incident Description:

- Employees reported suspicious emails with malicious links. One employee clicked a link, which led to suspicious activity on their system.
- **Category:** Phishing attempt with malware payload (potentially a **Remote Access Trojan** or **Backdoor** based on the C2 communication and file type).

Indicators of Compromise (IOCs):

- **Email Header:**
  - Sender: attacker@example.com
  - Subject: "Urgent Account Verification Required!"
  - URL: http://malicious-site.com/reset
- **Network Logs:**
  - Suspicious outbound traffic from employee workstation (192.168.10.25) to external IP (203.0.113.99)
  - Malicious file download: invoice.pdf.exe
- **EDR Report:**
  - Process flagged: invoice.pdf.exe (MD5 Hash: 7c9e3a5b6d8f12a4abc9d5678912efab)
  - Connection to C2 server: 198.51.100.88

2. Contain the Incident

Containment Actions:

- **Immediate Actions:**
  - Disconnect the affected workstation (192.168.10.25) from the network to prevent further spread of the malware.
  - Block the external IP addresses (203.0.113.99, 198.51.100.88) in the firewall to halt communication with the C2 server.
  - Block the malicious URL (http://malicious-site.com/reset) on the network perimeter to prevent further phishing attempts.
  - Isolate the downloaded file (invoice.pdf.exe) on the affected workstation and restrict its execution.
- **Long-term Containment:**
  - Implement network segmentation to limit the spread of malware.
  - Update network monitoring to alert on outbound traffic to known C2 servers or suspicious external IPs.

3. Analyze the Threat

File Analysis:

- Investigate the malicious file (invoice.pdf.exe):
    - Check for signs of a trojan or backdoor.
    - Use sandboxing and reverse engineering to understand the payload's behavior and functionality.
    - Correlate with external threat intelligence feeds to identify if the hash (7c9e3a5b6d8f12a4abc9d5678912efab) has been previously flagged by other sources.

Process and Connection Analysis:

- The suspicious process (`invoice.pdf.exe`) connects to an external C2 server (198.51.100.88). Track the behavior to determine if it establishes persistence on the system or attempts lateral movement.
- Correlate with previous incidents to check for patterns of attack.

4. Eradicate the Threat

Eradication Actions:

- **Remove Malicious File:** Delete the infected file (`invoice.pdf.exe`) from the affected workstation and any other systems that may have been infected.
- **Close Malicious Connections:** Terminate all connections to the external C2 server (198.51.100.88).
- **Patch Vulnerabilities:**
    - Review system logs for any vulnerabilities or misconfigurations that may have been exploited.
    - Apply patches or updates for any outdated software or OS vulnerabilities that were targeted.
- **Change Passwords:** Force a password reset for the affected employee and all users who may have been impacted.

5. Recover and Restore Operations

Recovery Actions:

- **System Cleanup:**
    - After verifying the system is clean, perform a full scan using updated antivirus or anti-malware tools.
    - Use backup images of the system to restore it to a known good state if needed.
- **Reintegrate Workstation:** After testing, reconnect the affected workstation to the network once it has been verified to be clean and free of threats.

- **Verify Network Integrity:** Conduct a full network scan to ensure no other systems were affected or compromised during the incident.

6. Post-Incident Review and Reporting

Incident Report:

- **Incident Summary:** A phishing attack led to the download and execution of a malicious file (invoice.pdf.exe), which connected to a C2 server. The attack was contained through network isolation and blocking of malicious IPs, followed by file eradication and patching.
- **Lessons Learned:**
    - The incident was detected early due to network traffic monitoring, which flagged suspicious outbound connections.
    - Employees must be reminded not to click on suspicious email links and to report any phishing attempts immediately.
- **Gaps Identified:**
    - Lack of robust email filtering may have allowed the phishing email to bypass defenses.
    - Employee awareness of phishing emails could be improved.

Recommendations for Improvement:

- **Improve Email Filtering:** Implement advanced email filtering solutions to detect and block phishing emails more effectively.
- **Enhance Network Monitoring:** Continue to improve detection of abnormal outbound traffic and connections to known malicious IPs.
- **Staff Training:** Conduct regular phishing awareness training to help employees recognize and report phishing attempts.

7. Proactive Monitoring and Preventative Actions

Monitoring Enhancements:

- **Set up custom rules** in the SIEM system to alert on suspicious email attachments (e.g., .exe files disguised as PDFs).
- **Monitor outbound traffic** for patterns indicative of C2 communication, such as connections to IPs outside of the company's approved ranges or known bad IPs.

Preventative Measures:

- **Regular Security Audits:** Schedule periodic security audits to ensure all systems are up to date with patches and configurations.
- **Multi-factor Authentication (MFA):** Implement MFA across all user accounts to reduce the impact of compromised credentials.

- **Phishing Drills:** Conduct simulated phishing attacks to improve staff response and awareness.

This Incident Response Plan ensures a comprehensive approach to dealing with phishing attacks while providing clear steps for analysis, containment, eradication, recovery, and future prevention.