**Incident Response Testing Scenario: Operation Cyber Shield**

**Background**

**Company**: AviaTech Solutions Ltd  
**Industry**: Aviation  
**Size**: 5959 employees

**Threat Actor Information**

**Threat Actor Group**: MuddyWater  
**Tactics and Techniques**:  
The MuddyWater threat actor group is planning to target AviaTech Solutions Ltd. They employ a wide array of tactics and techniques to compromise the company's security defenses and extract sensitive information.

**Tactics and Techniques**

**Reconnaissance (Phase: reconnaissance)**

1. **Email Addresses (T1589.002)**: The threat actors gather email addresses associated with the target organization for potential spearphishing targets.

**Resource Development (Phase: resource-development)**

1. **Web Services (T1583.006)**: MuddyWater establishes web services to aid in their operations and interactions with the target's infrastructure.
2. **Tool (T1588.002)**: The attackers develop or acquire tools to facilitate their campaign.

**Initial Access (Phase: initial-access)**

1. **Spearphishing Attachment (T1566.001)**: The threat actors employ spearphishing emails with malicious attachments to gain initial access.
2. **Spearphishing Link (T1566.002)**: MuddyWater uses spearphishing emails containing malicious links to trick recipients into accessing malicious websites.
3. **Exploit Public-Facing Application (T1190)**: The attackers exploit vulnerabilities in publicly accessible applications to gain initial access.

**Execution (Phase: execution)**

1. **PowerShell (T1059.001)**: Threat actors use PowerShell to execute commands and scripts for various purposes.
2. **Windows Management Instrumentation (T1047)**: MuddyWater utilizes Windows Management Instrumentation (WMI) for executing commands.
3. **Malicious Link (T1204.001)**: The attackers send users to malicious websites to initiate downloads or malicious payloads.
4. **JavaScript (T1059.007)**: Threat actors use JavaScript for execution of malicious code.
5. **Exploitation for Client Execution (T1203)**: MuddyWater exploits client applications to execute malicious code.
6. **Malicious File (T1204.002)**: The attackers deliver and execute malicious files on the compromised system.
7. **Scheduled Task (T1053.005)**: Threat actors use scheduled tasks to automate execution of malicious commands.
8. **Component Object Model (T1559.001)**: MuddyWater uses COM for execution of malicious code.
9. **Visual Basic (T1059.005)**: Threat actors employ Visual Basic scripts for execution.
10. **Windows Command Shell (T1059.003)**: MuddyWater uses Windows command shell for execution of commands.
11. **Dynamic Data Exchange (T1559.002)**: The attackers use Dynamic Data Exchange (DDE) for code execution.
12. **Python (T1059.006)**: MuddyWater utilizes Python scripts for execution.

**Persistence (Phase: persistence)**

1. **Office Template Macros (T1137.001)**: The threat actors use malicious macros embedded in office templates for persistence.
2. **DLL Side-Loading (T1574.002)**: MuddyWater side-loads malicious DLLs to maintain persistence.
3. **Registry Run Keys / Startup Folder (T1547.001)**: The attackers add entries to the registry run keys or startup folder for automatic execution.

**Privilege Escalation (Phase: privilege-escalation)**

1. **Bypass User Account Control (T1548.002)**: MuddyWater bypasses User Account Control (UAC) to escalate privileges.

**Defense Evasion (Phase: defense-evasion)**

1. **Mshta (T1218.005)**: The threat actors use mshta.exe to execute HTML applications and evade detection.
2. **Steganography (T1027.003)**: MuddyWater hides malicious code within seemingly innocent files using steganography.
3. **Match Legitimate Name or Location (T1036.005)**: The attackers use legitimate names or locations to evade detection.
4. **Compile After Delivery (T1027.004)**: MuddyWater compiles scripts or code after delivery to avoid detection.
5. **Disable or Modify Tools (T1562.001)**: The threat actors disable or modify security tools to avoid detection.
6. **Deobfuscate/Decode Files or Information (T1140)**: MuddyWater deobfuscates or decodes files to reveal their malicious content.
7. **CMSTP (T1218.003)**: The attackers use the Connection Manager Profile Installer (CMSTP) to run malicious code.
8. **Command Obfuscation (T1027.010)**: MuddyWater obfuscates commands to evade detection.
9. **Rundll32 (T1218.011)**: The threat actors use rundll32.exe to execute malicious code.

**Credential Access (Phase: credential-access)**

1. **Credentials from Password Stores (T1555)**: MuddyWater retrieves credentials from password stores for unauthorized access.
2. **Credentials In Files (T1552.001)**: The attackers search for credentials stored in files.
3. **Cached Domain Credentials (T1003.005)**: MuddyWater obtains cached domain credentials for lateral movement.
4. **LSA Secrets (T1003.004)**: The threat actors access LSA secrets for credential theft.
5. **LSASS Memory (T1003.001)**: MuddyWater targets LSASS memory to steal credentials.
6. **Credentials from Web Browsers (T1555.003)**: The attackers extract credentials stored in web browsers.

**Discovery (Phase: discovery)**

1. **Domain Account Discovery (T1087.002)**: MuddyWater seeks information about domain accounts to exploit access privileges.
2. **System Network Connections Discovery (T1049)**: The threat actors identify active network connections on the compromised system.
3. **Software Discovery (T1518)**: MuddyWater identifies installed software to target known vulnerabilities.
4. **Process Discovery (T1057)**: The attackers identify running processes on the compromised system.
5. **System Owner/User Discovery (T1033)**: MuddyWater determines system owners or users for lateral movement.
6. **File and Directory Discovery (T1083)**: The threat actors gather information about file and directory structures for navigation.
7. **System Information Discovery (T1082)**: MuddyWater retrieves detailed system information to aid in exploitation.
8. **Security Software Discovery (T1518.001)**: The attackers identify security software to avoid detection.
9. **System Network Configuration Discovery (T1016)**: MuddyWater gathers information about network configuration settings.

**Lateral Movement (Phase: lateral-movement)**

1. **Exploitation of Remote Services (T1210)**: The threat actors exploit remote services for lateral movement within the network.

**Collection (Phase: collection)**

1. **Archive via Utility (T1560.001)**: MuddyWater archives sensitive data using utilities for later exfiltration.
2. **Local Data Staging (T1074.001)**: The attackers stage data locally before exfiltration.
3. **Screen Capture (T1113)**: MuddyWater captures screenshots to gather sensitive information.

**Command and Control (Phase: command-and-control)**

1. **Standard Encoding (T1132.001)**: The threat actors use standard encoding for obfuscating communication.
2. **Remote Access Software (T1219)**: MuddyWater uses remote access software for controlling compromised systems.
3. **Web Protocols (T1071.001)**: The attackers use web protocols for command and control communication.
4. **Ingress Tool Transfer (T1105)**: MuddyWater transfers tools between compromised systems to maintain persistence.
5. **Bidirectional Communication (T1102.002)**: The threat actors establish bidirectional communication channels for control.
6. **External Proxy (T1090.002)**: MuddyWater uses an external proxy for routing malicious traffic.
7. **Symmetric Cryptography (T1573.001)**: The attackers encrypt communication to hide their activities.
8. **Multi-Stage Channels (T1104)**: MuddyWater establishes multi-stage channels for command and control.

**Exfiltration (Phase: exfiltration)**

1. **Exfiltration Over C2 Channel (T1041)**: The threat actors exfiltrate data over their established command and control channel.

**Incident Response Testing Scenario**

**Operation Cyber Shield**

**Objective**: To assess AviaTech Solutions Ltd's incident response capabilities against potential attacks orchestrated by the MuddyWater threat actor group.

**Scenario**:

1. **Preparation**:
   * Create a controlled testing environment that mirrors the company's network infrastructure.
   * Deploy various security tools and monitoring solutions to capture and analyze network activities, system logs, and behaviors.
2. **Simulation**:
   * Emulate the tactics and techniques identified from the MuddyWater playbook.
   * Initiate a spearphishing campaign with crafted emails containing malicious attachments.
   * Simulate exploitation of public-facing applications to gain initial access.
3. **Execution**:
   * Trigger execution of various techniques such as PowerShell, WMI, malicious links, JavaScript, and more.
   * Simulate persistence techniques including office template macros and DLL side-loading.
4. **Detection and Response**:
   * Monitor for suspicious activities, communication, and execution patterns.
   * Detect and respond to attempted privilege escalation and evasion tactics.
5. **Containment and Eradication**:
   * Contain the compromised systems to prevent lateral movement.
   * Eradicate malicious artifacts, including registry entries and malicious files.
6. **Threat Intelligence Collaboration**:
   * Collaborate with the Cyber Threat Intelligence team to gather relevant threat data.
   * Analyze indicators of compromise (IoCs) and tactics to enhance detection capabilities.

**Recommended Actions**

**Cyber Analysts**

* **Detection and Response**:
  + Monitor network traffic for any unusual or unauthorized communication.
  + Analyze system logs for any signs of execution of suspicious commands or scripts.
  + Implement behavioral analysis to identify patterns indicative of malicious activities.
  + Respond promptly to detected threats, isolate compromised systems, and investigate further.
  + Capture and analyze memory dumps for evidence of credential theft.
* **Containment and Eradication**:
  + Isolate compromised systems from the network to prevent lateral movement.
  + Remove malicious artifacts such as registry entries, scheduled tasks, and malicious files.
  + Conduct thorough system scans to ensure complete eradication of the threat.

**Cyber Threat Intelligence Team**

* **Threat Analysis**:
  + Gather intelligence on MuddyWater's recent activities, tools, and techniques.
  + Monitor open-source intelligence (OSINT) and dark web forums for chatter related to MuddyWater.
  + Collect and analyze malware samples associated with the threat actor group.
* **IoC and TTP Sharing**:
  + Share identified IoCs and TTPs with relevant security communities and partners.
  + Collaborate with industry peers to enhance threat detection and response capabilities.
* **Attribution and Motivation**:
  + Analyze MuddyWater's motivations, objectives, and potential targets.
  + Attribute observed activities to the threat actor group based on historical data and techniques.

By simulating and responding to this comprehensive incident response testing scenario, AviaTech Solutions Ltd can evaluate and enhance their incident response capabilities against potential threats posed by the MuddyWater threat actor group.