**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  03/02/2025 | **Entry:**  02 |
| Description | A phishing attack led to a malware infection on an employee's computer. The malicious file executed unauthorized processes, which triggered an alert from the intrusion detection system (IDS). |
| Tool(s) used | VirusTotal (for file hash analysis)  Wireshark (for network traffic inspection)  Sysinternals Autoruns (for persistence analysis)  EDR (Endpoint Detection & Response) tool (for threat containment) |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident?   An external attacker sent a phishing email containing a malicious attachment.   * **What** happened?   The employee opened a malicious file, which executed multiple unauthorized files.   * **When** did the incident occur?   1:11 p.m.: Employee received a phishing email.  1:13 p.m.: Employee opened the file.  1:15 p.m.: Malware created multiple unauthorized executables.  1:20 p.m.: IDS detected suspicious activity and generated an alert.   * **Where** did the incident happen?   The employee's workstation within the organization's internal network.   * **Why** did the incident happen?   The employee was tricked into opening a malicious file due to **social engineering**. |
| Additional notes | The **SHA256 hash** of the malware sample:  **54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b**  IoCs identified:   * **IP Address:** 104.115.151.81 * **Domain:** org.misecure.com |