| **Date:**  31st July,2025 | **Entry:**  #2 | | |
| --- | --- | --- | --- |
| Description | Investigation of a phishing email that delivered a password-protected spreadsheet containing a malicious payload. The file was downloaded and opened by an employee, triggering unauthorized executable creation. | | |
| Tool(s) used | * VirusTotal (for file hash analysis) * Intrusion Detection System (alert source) | | |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? An employee at the financial services company * **What** happened? Opened a malicious spreadsheet file from a phishing email * **When** did the incident occur? August 3, 2025, between 1:11 p.m. and 1:20 p.m. * **Where** did the incident happen? On the employee’s workstation * **Why** did the incident happen? The email appeared legitimate and included the password to open the file, leading to execution of a malicious payload | | |
| Additional notes | * SHA256 hash of malicious file: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * VirusTotal verdict: Malicious (detected as *Backdoor:Win32/Kryptik*) | | |