









Incident handler's journal

 Date: July 16th, 2025	 Entry#: 002
 Description	<p>As a Level 1 Security Operations Center (SOC) analyst at a financial services company, I received an alert regarding the download of a suspicious file on an employee's workstation.</p> <p>Upon investigation, I discovered that the employee had received a phishing email containing a password-protected spreadsheet attachment, with the password provided in the email body. The employee downloaded the file and entered the password, triggering the execution of a malicious payload.</p> <p>I retrieved the file and generated a SHA256 hash (54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93ba b527f6b). Using VirusTotal, I analyzed the hash to identify associated indicators of compromise (IoCs).</p> <p>VirusTotal results confirmed the file was malicious, flagged by multiple antivirus vendors and accompanied by a negative community score. The report revealed behavioral indicators, such as the creation of unauthorized executables and connections to known malicious IPs and domains.</p> <p>I documented the findings and categorized key IoCs using the Pyramid of Pain model for further escalation and threat intelligence enrichment.</p>
 Tools Used During the Incident	<ul style="list-style-type: none">● VirusTotal – Threat analysis and IoC discovery● SHA256 hashing – For uniquely identifying the malicious file

 The 5 W's of the Incident	<ul style="list-style-type: none"> Who caused the incident? An unidentified threat actor leveraging phishing and malware to compromise internal systems. What happened? An employee received a phishing email with a password-protected spreadsheet. Opening the file executed malware that created unauthorized files and contacted external infrastructure. When did the incident occur? Initial phishing email received at 11:00 p.m.; the file was opened by the employee at 1:13 p.m., and suspicious activity was flagged by IDS at 1:20 p.m. Where did the incident occur? On an employee's computer within the corporate network of a financial services organization. Why did the incident happen? The attacker exploited human error through phishing, successfully bypassing email security. The employee's action initiated malware execution and network compromise.
 Additional Notes & Recommendations	Indicators of Compromise (IoCs) Identified: <ol style="list-style-type: none"> Hash (SHA-1): c95ec50c1e2a6c1224f9c7ec97b1e42a9cfccf37 IP Address: 185.225.19.240 (flagged as malicious) Domain Name: osnewage[.]ru (associated with malware)

activity)

4. Network/Host Artifact:

C:\Users\[REDACTED]\AppData\Roaming\winload.exe

5. Tool Used: AutoHotKey (used in payload execution)

6. TTP (MITRE ATT&CK):

6.1. T1059.001 – Command and Scripting Interpreter: PowerShell

6.2. T1204.002 – User Execution: Malicious File

6.3. T1566.001 – Phishing: Spearphishing Attachment

Suggested Preventive Measures:

1. Email Security Filters

Implement anti-phishing gateways that analyze and sandbox attachments before delivery.

2. Endpoint Detection & Response (EDR)

Monitor endpoints for post-execution behaviors and block suspicious processes.

3. Employee Security Awareness Training

Reinforce phishing awareness and proper email handling procedures.

4. Threat Intelligence Integration

Incorporate IoC feeds from trusted platforms like VirusTotal to

enhance detection rules.

5. **Incident Response Playbooks**

Develop and test response procedures tailored to phishing and malware events.
