INCIDENT HANDLER’S JOURNAL

BY: ONWUATUEGWU CHIDIMMA ASSUMPTA

1.	**DATE:** May 4th, 2025	**ENTRY**: #1
2.	**Incident Summary**	A ransomware attack disrupted operations at a U.S. primary-care clinic after employees received phishing emails that led to the encryption of patient records and essential files. A ransom note demanding payment was displayed on compromised systems.
3.	**Description**	Several employees reported that they were unable to access patient records or other critical documents stored on their workstations. Simultaneously, a ransom note appeared, revealing that files had been encrypted by ransomware. Investigation revealed that attackers gained access through phishing emails containing malicious attachments. Upon execution, these attachments installed malware that facilitated the ransomware deployment. The attack halted all business operations, and the clinic contacted external incident response teams and law enforcement agencies to assist in the mitigation and recovery process.
4.	**Tools Used**	1. Splunk – to analyze logs for signs of phishing and malware execution. 2. VirusTotal – to analyze the malicious attachment. 3. Windows Event Viewer – to check login events and suspicious activity on affected machines. 4. Emsisoft or Malwarebytes – for malware/ransomware detection and cleanup. 5. Incident Response playbool
5.	**The 5W’s**	**A. Who caused the incident?** An organized cybercriminal group known to target healthcare and transportation sectors. **B. What happened?** Ransomware attack via phishing emails that encrypted company files and disrupted operations. **C. When did the incident occur?** Tuesday morning

		at approximately 9:00 AM. **D. Where did the incident happen?** Internal systems of the primary-care clinic (employee workstations, servers). **E. Why did the incident happen?** Employees unknowingly downloaded malware from a phishing email attachment, allowing attackers access to deploy ransomware.
6.	**Containment**	1. Isolated all affected endpoints from the network. 2. Disabled compromised user accounts. 3. Blocked identified malicious domains and IPs at the firewall. 4. Suspended email services temporarily to prevent further spread..
7.	**Eradication and Recovery**	1. Removed malware using antivirus 2. Applied critical patches to all systems. 3. Enforced company-wide password resets and enabled multi-factor authentication (MFA). 4. Conducted phishing awareness training for all staff.
8.	**ADDITIONAL NOTES**	1. How could the health care company prevent an incident like this from occurring again? 2. Should the company pay the ransom to retrieve the decryption key?

1.	**DATE:** May 10th, 2025	**ENTRY:** #2
2.	**Incident Summary**	Suspicious password-protected Excel file executed on an employee's computer, leading to malicious payload deployment and unauthorized executable file creation.
3.	**Description**	At approximately 1:11 p.m., an employee received an email containing a password-protected spreadsheet. The email also included the password. Upon opening the spreadsheet at 1:13 p.m., a malicious payload was executed, leading to the creation of multiple unauthorized executable files on the employee's machine. At 1:20 p.m., our IDS triggered an alert, and the SOC team was notified for further investigation.
4.	**Tools used**	1. VirusTotal (to analyze file hash) 2. Intrusion Detection System (IDS) 3. SIEM platform 4. SHA256 hashing utility
5.	**The 5W's**	**A. Who caused the incident?** An external threat actor leveraging phishing via email **B. What happened?** A malicious Excel spreadsheet was used to deploy a payload that created unauthorized executables. **C. When did the incident occur?** Initial email at 1:11 p.m.; file opened at 1:13 p.m.; alert triggered at 1:20 p.m. on July 31, 2025 **D. Where did the incident happen?** On an employee's endpoint computer within the financial services company's internal network **E. Why did the incident happen?** Social engineering via phishing email convinced the user to open a suspicious file, enabling the malware to execute.
6.	**Containment**	1. Disconnected the affected device from the network. 2. Blocked the hash 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b at the firewall
7.	**Eradication and Recovery**	1. Deleted malicious executables

		2. Ran full antivirus 3. Reimaged the device and restored essential files from backup. 4. Monitored for further signs of compromise on adjacent systems.
8.	**Additi**	1. The file hash has been reported as malicious by over 50 vendors. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor 2. User awareness training should be reinforced. 3. Recommend implementing attachment sandboxing and enhanced email filtering policies.

1.	**DATE:** May 15th, 2025	**ENTRY:** #3
2.	**Incident Summary**	A forced browsing vulnerability in the company's e-commerce web application allowed an attacker

		to access customer transaction records. The breach compromised approximately 50,000 customer records, including personally identifiable and financial information.
3.	**Description**	An attacker exploited a forced browsing vulnerability by manipulating the order numbers in a purchase confirmation page URL, which enabled unauthorized access to thousands of customer purchase confirmation pages. This led to the exfiltration of sensitive PII and financial data. Initial ransom emails were ignored, but further demands with proof triggered the investigation.
4.	**Tools used**	1. Web Application Access Logs 2. Intrusion Detection System (IDS) 3. Email Security Gateway 4. Vulnerability Scanner
5.	**The 5W's**	**A. Who caused the incident?** An unknown external threat actor exploiting web application flaw **B. What happened?** A forced browsing attack enabled data exfiltration of ~50,000 customer records. **C. When did the incident occur?** Suspicious activity was first communicated on Dec 22, 2022, and confirmed on Dec 28, 2022. **D. Where did the incident happen?** The organization's e-commerce platform/web application **E. Why did the incident happen?** Due to a lack of access control mechanisms in the web application, allowing sequential access to other users' confirmation pages.
6.	**Containment**	1. Immediate investigation by the security team. 2. Monitoring and capturing of abnormal traffic in logs. 3. Collaboration with the Public Relations department to notify customers and

		reduce reputational damage.
7.	**Eradication and Recovery**	1. The vulnerability was patched in the web application code. 2. Implemented allowlisting to restrict access to valid URLs only. 3. Conducted full penetration testing and vulnerability scanning post-recovery. 4. Offered free identity protection services to all affected customers.
8.	**Additional notes**	1. A strong reminder of the importance of employee awareness in incident escalation. 2. Emphasized the need for proactive threat modeling and access control reviews. 3. Future actions include improving SOC alert response times and web app security hardening.

Submitted by:
[ONWUATUEGWU CHIDIMMA ASSUMPTA]
Google Cybersecurity Certificate – Course 6