Incident handler's journal

Instructions

Date: 23/02/2024	**Entry:** 1
Description	A small U.S. health clinic experienced a security incident on Tuesday at 9:00am. The incident, which was found to be ransomware, caused business operations to stop. Several employees reported being unable to access medical records which are critical to normal business operations. The threat actors are a notorious hacker group known to target healthcare and transportation industries. The ransom note demanded a large sum of money in exchange for the decryption key.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • The threat actors are a hacker group known to target transportation and healthcare industries. • Phishing emails containing a malicious attachment were sent to several employee computers prior to the incident. The computers were then encrypted with the ransomware. • The incident occurred on Tuesday at 9:00am. • The incident took place at a healthcare clinic

	• **Why:** The threat actors were able to access company systems through phishing attacks. The attackers motivation appears to be financial since a ransom note was left in all computers that were affected.
Additional notes	The phishing emails were sent to several employees indicating a few things: 1. The employees whose computers were affected use their work computer to receive personal emails. The personal emails have no security filters to reduce chances of phishing emails. 2. Employees have not had regular security awareness training which helps in distinguishing real emails from phishing ones. 3. There is a need for proper firewall configuration to filter traffic from unknown network sources. 4. There is no existing antivirus software, or the existing antivirus software is not effective in filtering for malicious programs in their computers.

Date: 25/02/2024	**Entry:** 2
Description	A financial services company's SOC team receives an alert of a suspicious file download. An employee receives an email with a file attachment at 1:11p.m. Upon downloading the file, the employee's computer created multiple unauthorized executable files at 1:15p.m. The alert was received at 1:20p.m.
Tool(s) used	VirusTotal was used for researching the malicious file's hash value
The 5 W's	Capture the 5 W's of an incident. • **Who**: An employee

	• **What**: The employee received an email from an unknown source with an attachment file. The employee proceeded to download the file. Once done downloading, multiple unauthorized executable files were created in the employees computer • **When** did the incident occur: The incident took place at 1:15p.m. • **Where** did the incident happen: It happened at the office of the employee • **Why** did the incident happen? The email sent may have been used to obtain access to the organization's system so that the attacker involved can pivot from the first computer. The attacker's end target may be to gain a financial advantage.
Additional notes	Analysis of the file that was downloaded has determined it to be malicious. Notable sources from VirusTotal flag the file as malicious. The files notable TTPs are defense evasion, privilege escalation, command and control, and credential access. It would be beneficial to provide security awareness training, quarterly, to all employees. Security awareness training will reduce the chances of phishing attempts becoming an incident, since many phishing attempts are easy to spot.

Date: 27/02/2024	**Entry:** 3
Description	An alert of an employee receiving a phishing email has been received. A review of the domain involved has been done to verify how many more employees, if any, received a phishing email containing the same domain as the alert. It is also to confirm how many of the employees receiving the email visited the

	domain.
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Malicious actor • **What** happened? A phishing email was sent to the PC of an employee which triggered an alert. The email contained a suspicious domain in its body. Further investigations confirmed the domain to be a drop site for logs and stolen credentials. • **When** did the incident occur? February 27th 2024 • **Where** did the incident happen? The employee's workstation • **Why** did the incident happen? It is likely that the bad actor was trying was targeting to steal login credentials
Additional notes	Upon doing further investigation it turns out that the domain has been visited by 2 of our assets in the past year. All said assets have had their login credentials stolen. All 2 assets involved will be required to have their passwords changed. It would be beneficial to have a security awareness training program for all employees to reduce the chances of future incidents.

Date: 25/02/2024	**Entry:** 4
Description	Monitoring network traffic and using Suricata to configure it to trigger alerts.
Tool(s) used	Suricata

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Junior Security Analyst • **What** happened? I set up custom rules in Suricata. I then ran Suricata with the custom logs in order to trigger it and then examine the output logs in the fast.log file. I have also examined the eve.json file to observe the additional information that is not present in the fast.log file • **When** did the incident occur? 25th February 2024 • **Where** did the incident happen? On my PC • **Why** did the incident happen? To examine how Suricata works
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?

Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Reflections/Notes: Record additional notes.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Date: Record the date of the journal entry.	**Entry:** Record the journal entry number.
Description	Provide a brief description about the journal entry.
Tool(s) used	List any cybersecurity tools that were used.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? • **What** happened? • **When** did the incident occur? • **Where** did the incident happen? • **Why** did the incident happen?
Additional notes	Include any additional thoughts, questions, or findings.

Reflections/Notes: Record additional notes.