Incident handler's journal

Date: 2024/05/07	**Entry:** A1
Description	A small U.S. health care clinic experienced a security incident at 9:00 a.m. Employees were unable to use their computers to access medical records, and business operations were shut down. Employees received a ransom note stating all the company's files were encrypted, and demanded money in exchange for the decryption key. The attackers gained entry via phishing emails using malicious attachments.
Tool(s) used	None

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ *Organized group of unethical hackers who are known to target organizations in healthcare and transportation*
	• **What** happened?
	  ○ *A small U.S. health care clinic had its organizations files encrypted and ransomed for money*
	• **When** did the incident occur?
	  ○ *Tuesday morning at 9:00 a.m*
	• **Where** did the incident happen?
	  ○ *At a small U.S. health care clinic, through the company's emailing system*
	• **Why** did the incident happen?
	  ○ *An employee clicked on a malicious attachment*

Additional notes	How can we prevent an incident from occurring again in the future?

Date: 2024/06/10	**Entry:** A2
Description	You have received an alert about a suspicious file being downloaded on an employee's computer. You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer. You retrieve the malicious file and create a SHA256 hash of the file.
Tool(s) used	VirusTotal

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ An anonymous threat actor
	• **What** happened?
	  ○ A malware that was downloaded via an email attachment triggered a phishing alert
	• **When** did the incident occur?
	  ○ 2024/06/10 @1:11 p.m.
	• **Where** did the incident happen?
	  ○ On an employees computer, at a financial services company
	• **Why** did the incident happen?
	  ○ An employee opened a suspicious email and downloaded a malicious file

Additional notes	MD5 hash of the malicious file: 287d612e29b71c90aa54947313810a25

	Malware contacted an IP address of 207.148.109.242 Malware contacted a domain of http://org.misecure.com/index.html Malware made HTTP requests to http://org.misecure.com/favicon.ico Malware used Input capture Malware attempted to evade detection by having delayed execution, also encoding to obfuscate itself

Date: 2024/06/10	**Entry:** A2-1
Description	Previously, you received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified to be malicious. Now that you have this information, you must follow your organization's process to complete your investigation and resolve the alert. Your organization's security policies and procedures describe how to respond to specific alerts, including what to do when you receive a phishing alert. In the playbook, there is a flowchart and written instructions to help you complete your investigation and resolve the alert. At the end of your investigation, you will update the alert ticket with your findings about the incident.
Tool(s) used	Phishing incident response playbook, Ticketing system

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ A malicious actor with the email and IP address <76tguyhh6tgftrt7tg.su> <114.114.114.114>
	• **What** happened?
	  ○ A malware that was downloaded via an email attachment triggered a phishing alert
	• **When** did the incident occur?
	  ○ Wednesday, July 20th, 2022 @ 9:30:14 a.m.
	• **Where** did the incident happen?
	  ○ An employee's computer, via email
	• **Why** did the incident happen?
	  ○ An employee opened a suspicious email and downloaded a malicious file

Additional notes	Sender's email is suspicious: ‘76tguyhh6tgftrt7tg.s’ Subject line has the incorrect spelling of ‘Engineer’ Multiple grammar and spelling mistakes in the body of the email Resume file listed is an executable file File name is suspicious ‘bfsvc’ File hash was confirmed as malware via VirusTotal Ticket is being escalated to a level 2 SOC analyst due to the file hash containing malware, and the file itself already has been executed on the employees computer.

Date: 2024/06/11	**Entry:** A3
Description	You recently joined the security team as a level-one security operation center (SOC) analyst at a mid-sized retail company. Along with its physical store locations, your company also conducts operations in e-commerce, which account for 80% of its sales. You are spending your first week of training becoming familiar with the company's security processes and procedures. Recently, the company experienced a major security incident involving a data breach of over one million users. Because this was a recent and major security incident, your team is working to prevent incidents like this from happening again. This breach happened before you began working at the company. You have been asked to review the final report.
Tool(s) used	Incident final report

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ An anonymous threat actor
	• **What** happened?
	  ○ An individual was able to gain unauthorized access to PII and financial information
	• **When** did the incident occur?
	  ○ December 28th, 2022, @7:20 p.m., PT
	• **Where** did the incident happen?
	  ○ The organizations web application
	• **Why** did the incident happen?
	  ○ A web application vulnerability was discovered, which allowed the attacker to access customer purchase confirmation pages, exposing customer data

Additional notes	The employee could have elevated the first email to the security team, minimizing

	the potential for the attack to get worse. This incident handler journal entry is using the last phase of the NIST incident response lifecycle: Post-incident activity, by reviewing a final report of an incident that took place.

Date: 2024/06/18	**Entry:** A4
Description	Reviewing a suspicious domain through Chronicle
Tool(s) used	Chronicle
The 5 W's	Capture the 5 W's of an incident. ● **Who** caused the incident? ○ ashton-davidson, bruce-monroe, coral-alvarez, emil-palmer, jude-reyes, roger-spence, amir-david, warren-morris ● **What** happened? ○ A total of 8 different computers accessed the domain '104.215.148.63' on July 9th, then again with a different domain IP '40.100.174.34' ● **When** did the incident occur? ○ Beginning July 8th, 2023 from 2:40:45 p.m. to July 9th, 2023 to 5:04:44 a.m., and again on February 1st, 2023 from 2:40:40 p.m. to 2:51:45 p.m. ● **Where** did the incident happen? ○ signin.office365x24.com ● **Why** did the incident happen? ○ Possible phishing attempt
Additional notes	Started with 6 distinct assets on July 9th, then 2 more distinct assets accessed the domain on February 1st Each user had 3 different POST attempts, possible phishing attack Both IP's linked to a domain with the name of 'signin.accounts-gooqle.com', notice the q in google