Incident handler's journal

Date: 07/23/2023	**Entry:** #1
Description	• A small U.S. health care clinic experienced a security incident on Tuesday at 9:00 a.m. which severely disrupted their business operations. • The cause of the security incident was a phishing email that contained a malicious attachment. Once it was downloaded, ransomware was deployed encrypting the organization's computer files. • An organized group of unethical hackers left a ransom note stating that the company's files were encrypted and demanded money in exchange for the decryption key
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers. • **What** happened? Employees were unable to use their computers and access their files, due to a ransomware attack that had infected several systems. • **When** did the incident occur? The incident happened at 9:00am. • **Where** did the incident happen? A small U.S. health care clinic specializing in delivering primary-care services. • **Why** did the incident happen? An employee was the target of a phishing email. This could be due to a lack of awareness around phishing attack techniques.
Additional notes	The organization should implement a cybersecurity training and awareness

	program for its employees so that they are better prepared for this in the future and can hopefully prevent it from happening again.

Date: 07/29/2023	**Entry:** #2
Description	• **1:11 p.m.:** An employee receives an email containing a file attachment. • **1:13 p.m.:** The employee successfully downloads and opens the file. • **1:15 p.m.:** Multiple unauthorized executable files are created on the employee's computer. • **1:20 p.m.:** An intrusion detection system detects the executable files and sends out an alert to the SOC.
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • The employee who received the email and opened the file attachment. • The employee received an email containing a file attachment, which they successfully downloaded and opened. • The incident occurred at 1:11 p.m., 1:13 p.m., 1:15 p.m., and 1:20 p.m • The incident occurred on the employee's computer. • The employee was tricked into opening the malicious file attachment, which allowed the malware to be installed on their computer.
Additional notes	The SOC should investigate the incident and take steps to prevent it from happening again. This may include educating employees about phishing scams, updating the organization's security software, and implementing a

	more secure email filtering system.

Date: 07/30/2023	**Entry:** #3
Description	SERVER-MAIL Phishing attempt possible download of malware
Tool(s) used	VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An employee • **What** happened? Received a phishing alert about a suspicious file being downloaded on an employee's computer. • **When** did the incident occur? The alert was received on 2023-07-30 at 10:16am • **Where** did the incident happen?The alert was received from the employee's computer. • **Why** did the incident happen? The alert was received because the email attachment file's hash has already been verified malicious.
Additional notes	The user may have opened a malicious email and opened attachments or clicked links. **Additional information** **Known malicious file hash**: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b **Email**: From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> Sent: Wednesday, July 20, 2022 09:30:14 AM

	To: <hr@inergy.com> <176.157.125.93> Subject: Re: Infrastructure Egnieer role Dear HR at Ingergy, I am writing for to express my interest in the engineer role posted from the website. There is attached my resume and cover letter. For privacy, the file is password protected. Use the password paradise10789 to open. Thank you, Clyde West Attachment: filename="bfsvc.exe"

Date: 7/31/2023	**Entry:** #4
Description	The organization experienced a security incident on December 28, 2022, at 7:20 p.m., PT, during which an individual was able to gain unauthorized access to customer personal identifiable information (PII) and financial information.
Tool(s) used	The vulnerability scanner was used to identify the vulnerability in the e-commerce web application that was exploited by the attacker. The security team also used an incident response plan to guide their response to this incident. The plan included steps for containing the incident, investigating the incident, and remediating the vulnerability.

The 5 W's	Capture the 5 W's of an incident. ● The incident was caused by an individual who exploited a vulnerability in the organization's e-commerce web application. ● The attacker was able to gain unauthorized access to the organization's e-commerce web application and access customer purchase confirmation pages. The attacker then collected and exfiltrated customer data, including personal identifiable information (PII) and financial information. ● The incident occurred on December 28, 2022. ● The incident occurred on the organization's e-commerce web application. ● The incident happened because of a vulnerability in the organization's e-commerce web application. The vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page.
Additional notes	● The incident was first discovered on December 28, 2022, when an employee received an email from an external email address claiming that they had stolen customer data. ● The security team investigated the incident and determined that the attacker had gained unauthorized access to the organization's e-commerce web application by exploiting a vulnerability in the application. ● The attacker was able to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. ● The organization has taken steps to prevent future recurrences of this incident, including performing routine vulnerability scans and penetration testing, and implementing access control mechanisms.

Reflections/Notes:

1. Were there any specific activities that were challenging for you? Why or why not?

   The difficulties that I experienced during these activities were in the usage of VirusTotal. VirusTotal has many features that I have never seen before and because of this, the analysis part of the activities were more challenging.

2. Has your understanding of incident detection and response changed since taking this course?

   Yes, my knowledge and understanding of incident response has grown since taking this course. Before taking this course I was not aware of the 5 W's and how this helps security analysts perform incident response. Although it is not necessary, it is still a good starting point. By asking these questions, a security analyst can gather the information they need to effectively respond to an incident.

3. Was there a specific tool or concept that you enjoyed the most? Why?

   I enjoyed using the Chronicle SIEM tool created by Google. It was my first time utilizing this tool to perform search queries and it was rather robust with it's many features.