Incident handler's journal

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this journal as a way to log the key takeaways about the different cybersecurity tools or concepts you encounter in this course.

Date: 2024/04/18	**Entry:** 1
Description	This entry is about a ransomware attack that occurred to a small U.S. health care clinic. The business operations were down because employees were unable to access the files and software needed to do their job.
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. • **Who:** Organised group of unethical hackers • **What:** Ransomware attack • **When:** Approximately 9:00 a.m. • **Where:** A U.S. health care clinic • **Why:** The attackers sent several phishing emails to the company's employees. The phishing emails contained a malicious attachment that installed malware on the employee's computer once downloaded. Once the attacker gained access, they deployed their ransomware, encrypting critical files. The motive is likely financial due to them asking for a large sum of money to decrypt the files.
Additional notes	• What security controls are in place to deal with phishing emails?

	• What security training have the employees been trained on?

Date: 2024/04/22	**Entry:** 2
Description	This entry is about a trojan horse attack that occurred on an employee's computer of a financial services company. The employee received a job application email with an attachment. I am to investigate a suspicious file hash from the email.
Tool(s) used	For this activity, I used VirusTotal. The tool can be used to check if there are any IoCs reported for a website or a file. I used VirusToal to analyse the hash file that was reported.
The 5 W's	Capture the 5 W's of an incident. • **Who**: Threat actor BlackTech • **What**: Phishing email with trojan attached • **When**: 1:20 p.m. • **Where**: A financial services company • **Why**: The attacker sent an employee of the company a job application email containing a password protected resume and the password. The employee downloaded the file, then entered the password to open the file. A malicious payload was then executed on their computer. Due to the malware having input capture, it is likely it is designed to obtain credentials.
Additional notes	• The malware is a trojan under the name Flagpro commonly used by threat actor BlackTech

	• What is the best way to prevent similar attack in the future

---

Date: 2024/04/23	**Entry:** 3
Description	An individual gained unauthorised access to customer PII and financial information. Approximately 50,000 customer records were affected. The financial impact of the incident is estimated to be $100,000 in direct costs and potential loss of revenue.
Tool(s) used	NA
The 5 W's	Capture the 5 W's of an incident. • **Who**: Unknown threat actor • **What**: A major data breach • **When**: 7:20 p.m. December 28, 2022 • **Where**: A retail company • **Why**: The attacker took advantage of a vulnerability in the e-commerce web application. They performed a forced browsing attack and accessed customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. The attacker was able to access customer purchase confirmation pages, which they then collected and exfiltrated. The motivation seems to be monetary as they demanded payment in exchange for not releasing the data.
Additional notes	• How much has the incident affected the company's public standing? • What other controls should be in place to keep customers' data safe

Date: 2024/04/26	**Entry:** 4
Description	This entry is about identifying whether there are any security issues with the mail server.
Tool(s) used	For this activity, I used Splunk. The tool can be used to check logs and determine the events of interest. I used plunk to check the logs coming to the company's mail server.
The 5 W's	Capture the 5 W's of an incident. • **Who**: Unknown threat actor • **What**: Multiple login attempts • **When:** 1:39 a.m. February 27, 2023 • **Where**: Mail server of an e-commerce store Buttercup Games • **Why**: Threat actor attempting to brute force root account login into the company's mail server. Possible motive is to gain user credentials and PII from the emails.
Additional notes	• How do we protect users' data contained in the emails? • Should there be more security controls in place to prevent threat actors from being able to brute force the root account?

Date: 2024/04/26	**Entry:** 5
Description	An employee received a phishing email in their inbox. I need to determine whether any other employees have received phishing emails containing the same domain and whether they have visited the domain.
Tool(s) used	For this activity I used Google Chronicle, and VirusTotal. Google Chronicle was used to view logs of the assets visiting the suspicious domain and determine how many POST requests were made. Also to find out if there were any other related domains, and IP addresses. VirusTotal was used to determine if the domains were suspicious.
The 5 W's	Capture the 5 W's of an incident. • **Who:** Unknown threat actor • **What**: A phishing attack • **When:** 5:02 a.m. July 8th, 2023 • **Where**: A financial services company • **Why:** Company's employees accessed a website that was determined to be malicious by TotalVirus after receiving a phishing email from a threat actor. The domain has been involved in phishing campaigns as there are reused infrastructures. The threat actor was able to get login credentials of multiple employees as there are multiple POST requests to login.php. There are more domains related to the suspicious domain after examining the resolved IP address.
Additional notes	• What security controls should be implemented to help the employees more aware of social engineering attacks? • What other security controls should be implemented to keep the accounts safe even if the threat actor obtains the user credentials? • Should any specific web requests be blocked?

Reflections/Notes:

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

   First time using VIrusTotal, it was hard to determine who was the threat actor as I was not familiar with the website and it took a while for me to navigate.

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

   After taking this course, I believe that my understanding of incident detection and response has improved drastically. I have learned many tools that are used for incident detection and response and the process that goes into it.

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

   As I am quite a technical person, I really enjoyed learning different tools and gaining real experience using them. It was really enjoyable to learn about VirusTotal, Suricata, Splunk, and Chronicle.

Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.