Incident handler's journal

Instructions

Date: 6/5/2024	**Entry:** #1
Description	Small U.S. health care clinic encountered ransomware
Tool(s) used	Social Engineering, Phishing, Encryption, Ransomware
The 5 W's	Capture the 5 W's of an incident. • **Who** = An organized group of Unethical Hackers that are know to target healthcare companies • **What** happened = Employees logged into their computers to find they were unable to access files but instead saw a ransom note displayed • **When** did the incident occur? Tuesday at 9 am • **Where** did the incident happen? The office of a small US health care clinic • **Why** did the incident happen? The hackers used phishing emails to gain access to the company network. The emails contained an attachment that installed malware on the computer once it was downloaded.
Additional notes	The hacker group frequently targets health care and transportation organizations because they are likely to have SPII.

Date: 6/18/2024	**Entry:** 2
Description	**SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b** Here is a timeline of the events leading up to this alert: ● 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. ● **Who** = A hacking group known as “BlackTech” ● **What** = Employee opened an email with a file attachment. Upon opening the attachment, multiple malicious files were created ● **When** = 1:11 pm - 1:20 pm ● **Where** = The incident happened in the office at an employee’s computer ● **Why** = Unauthorized executable files were downloaded to the employee computer to try and spread a malicious hash file.
Additional notes	VirusTotal flagged the hash file as malicious and the community noted that the hash has been used by BlackTech before

Date: 6/20/2024	**Entry: 3**
Description	An employee received a potential phishing email and may have clicked links or opened the attachments within the email that are malicious.
Tool(s) used	Hash File, Virus Total
The 5 W's	Capture the 5 W's of an incident. • **Who** = An employee within HR opened a phishing email. • **What** = The phishing email contained malicious links or attachments that the employee opened. • **When** = The incident occurred on Wednesday, July 20, 2022 at 9:30:14 AM • **Where** = The incident happened in the office at the employee's computer. • **Why** = The links contained malicious links that may have been downloaded to the employee computer.
Additional notes	Upon researching the hash file that was opened by the employee on VirusTotal, I discovered that 62/74 vendors labeled it as malicious and 3 sandboxes did as well. The hash file also had a communit score of -153. According to community members, this hash is also from the hacking group know as "blacktech" and it is used to create a backdoor within an organization's system.

Date: 6/24/2024	**Entry:** 4
Description	An employee on the security team received an external email claiming they had stolen customer PII & SPII and requested a payment of $25K in crypto in exchange for not releasing the data to public forums. The employee assuming it was spam deleted it. About a week later, they received the same email but this time, they had a sample of the data stolen and requested $50K.
Tool(s) used	Forced Browsing Attack
The 5 W's	Capture the 5 W's of an incident. • **Who** = External Email Sender claimed they stole customer PII & SPII • **What** = A hacker found a vulnerability in the e-com web application where they were able to perform a forced browsing attack by modifying the order number included in the URL string of the purchase confirmation page to access customer data. • **When** = Approximately 3:13 pm, PT, on December 22, 2022 • **Where** = On the e-com web application • **Why** = The web application had a vulnerability that allowed an attacker to modify the order number included in the URL of the confirmation page in order to gain access to customer data.
Additional notes	The security team has decided to implement allowlisting to only allow access to a specified set of URLs and automatically block all others. They will also only allow authorized users to access this content.

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: 7/3/2024	**Entry:** 6
Description	I received an alert that an employee received a phishing email in their inbox. As an analyst at a financial services company, I am tasked with investigating the alert and identifying a suspicious domain name contained in the email's body: signin.office365x24.com. I need to determine whether any other employees have received phishing emails containing this domain and whether they have visited the domain.
Tool(s) used	Chronicle, VirusTotal, WHOIS

The 5 W's	Capture the 5 W's of an incident. • **Who** - An Employee recieved a phishing email with a suspicious domain name in their inbox. Using Chronicle, I can determine that 6 assets have accessed the domain name. They are: ashton-davidson-pc, bruce-monroe-pc, coral-alvarez-pc, emil-pallmer-pc, jude-reyes-pc, and roger-spence-pc • **What** - Multiple assets may have been impacted. Logs showed the login information was submitted to the suspicious domain via POST requests. • **When** - 7/3/2024 • **Where** - The incident happened on employee emails • **Why** - Multiple employee received phishing emails with a fake sign in domain name. They entered their own login information to the fake domain.
Additional notes	While examining resolved IPs, I found that this domain has also been using two additional domains. Logs indicate that the additional domains received login information from more assets via POST requests.

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.

Reflections/Notes: Record additional notes.