Incident handler's journal - U.S. health care

Date: 06/26/2023	**Entry:** 1
Description	A small U.S. health care clinic experienced a security incident that has severely disrupted their business operations. This appears to be a ransomware attack from an experienced group of unethical hackers as several employees have reported their files to be encrypted and new ransom notes appearing on their devices.
Tool(s) used	• Email filters • Firewall filters and network port filtering • File recovery and backup tools • SEIM tools • Network protocol analyzers

The 5 W's	Capture the 5 W's of an incident.
	• **Who** caused the incident?
	  ○ An organized group of unethical hackers who are known to target healthcare and transportation companies
	• **What** happened?
	  ○ The attackers sent several targeted phishing emails which contained a malicious file attachment that installed malware on the employee's device when downloaded. This led to employees reporting that they were unable to use their computers to access files like medical records. Business operations were then shut down because employees were not able to access files or software needed to complete their jobs. There were reports of ransom notes being displayed on employee's computers demanding payment in exchange for decryption keys.

	• **When** did the incident occur?
	  ◦ Tuesday, approximately 9:00 a.m.
	• **Where** did the incident happen?
	  ◦ A small U.S. health care clinic specializing in delivering primary-care services
	• **Why** did the incident happen?
	  ◦ The attackers were able to bypass the current security controls in place to filter emails and validate attachments being sent through email

Additional notes	Include any additional thoughts, questions, or findings.
	The phishing attacks were reported to be targeted, meaning that they were personalized for the intended receiver. The organization may need to review and update its policies on employee social media usage related to business operations.

Date: 6/28/2023	**Entry:** 2
Description	Suspicious file downloaded onto an employee's computer.
Tool(s) used	• SHA256 hash • VirusTotal
The 5 W's	Capture the 5 W's of an incident. • **Who** – Unknown email sender • **What** – Employee opened email with attached password-protected spreadsheet file. When the employee opened the file, a malicious payload was executed on their device. • **When** – 1:11 p.m.

	• **Where** – On a single employee's device. • **Why** – The organization's email filter did not detect/block the malicious file, which could have been done through the file's SHA256 hash.
Additional notes	The behavior reported by the employee also aligns with the behavior reported on VirusTotal. This behavior consists of creating new processes, editing files, setting registry keys, and many other malicious actions.

Date: 06/29/2023	**Entry:** 3
Description	Incident response playbook for email phishing and malware attack.
Tool(s) used	• Phishing playbook
The 5 W's	Capture the 5 W's of an incident. • **Who** – Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> • **What** – An employee was sent a phishing email that held a password-protected malicious file. • **When** – July 20, 2022 09:20:14 AM • **Where** - Inergy • **Why** - The organization's email filter did not detect/block the malicious file, which could have been done through the file's SHA256 hash.
Additional notes	

Date: 06/29/2023	**Entry:** 4
Description	Final report review for data breach
Tool(s) used	
The 5 W's	Capture the 5 W's of an incident. • **Who** - Unknown • **What** – An employee received a ransom email stating the attacker had stolen consumer data and was requesting $25,000 in cryptocurrency payment. The employee was then sent another email sending proof of stolen information and with an increased payment request of $50,000. • **When** – December 28, 2022 7:20 p.m. PT • **Where** – The organization’s ecommerce site, on the purchase confirmation page • **Why** - The attacker exploited a vulnerability in the organization’s website using a forced browsing attack which allowed them to steal customer purchase confirmation pages and customer data.
Additional notes	Certain pages within the organization’s website did not have adequate access controls and the security team has now implemented allow listings to ensure only authorized employees can visit those pages.

Date: 07/02/2023	**Entry:** 5
Description	Searching for security issues with mail server
Tool(s) used	• Splunk

The 5 W's	Capture the 5 W's of an incident. • **Who** – root account • **What** – There were many failed SSH login attempts on the mail server using the root account • **When** - Thu Mar 06 2023 01:39:51 • **Where** – Multiple different IPs: 194.8.74.23 port 3768, 89.106.20.218 port 1392, 193.33.170.23 port 1151 • **Why** – It appears to be an attacker trying multiple different IP addresses to login to the account.
Additional notes	The login attempts all happen at almost the exact same time, and there are multiple attempts each date that the attacker has tried. This could suggest the attacker is using some sort of brute-force method to attempt to guess the account's password.

Date: 07/02/2023	**Entry:** 6
Description	Phishing email from suspicious/spoofed email
Tool(s) used	• Chronicle
The 5 W's	Capture the 5 W's of an incident. • **Who** - warren-morris-pc, ashton-davidson-pc, emil-palmer-pc • **What** – An employee reported a suspicious email that was believed to be a phishing attempt with the domain signin.office365x24.com in the body of the email. • **When** - 2023-01-31 14:51:45 • **Where** - 40.100.174.34

	• **Why** – The organization's email filter did not detect this domain as suspicious, likely because there is not overwhelming evidence that it is malicious. There are only a few VirusTotal reports on this and its connected domains, but it has been categorized as a dump site for stolen credentials.
Additional notes	The reported domain signin.office365x24.com has a resolved IP of 40.100.174.34 and a top private domain of office365x24.com. Chronicle categorizes these domains/IPs as "Drop site for logs or stolen credentials" The reported domain signin.office365x24.com has 2 POST requests listed to http://signin.office365x24.com/login.php but the resolved IP of 40.100.174.34 has an additional POST request to http://signin.accounts-gooqle.com/login.php which may suggest that credentials were stolen and used to login to another account.

Reflections/Notes:

1. Were there any specific activities that were challenging for you? Why or why not?
    - I think the Suricata activity took the longest because it is a CLI and generally harder to take in all the information being output.
2. Has your understanding of incident detection and response changed since taking this course?
    - Absolutely, I gained a lot more information about the lifecycle of incident response and the different tiers of security team members that have different responsibilities in the lifecycle.
3. Was there a specific tool or concept that you enjoyed the most? Why?
    - Chronicle was very interesting because of the VirusTotal integration and the tools that it gives you to dive deeper on related domains or IP addresses.