Incident Handler's Journal

Tyler Ebra
CSEC 3003

Date: 2/6/2025	**Entry:** #1
Description	A U.S. health care clinic had a security breach on Tuesday at 9:00 am which disrupted business. The attack was through a phishing email that had a malicious file attached to it that downloaded ransomware that encrypted the company's files. The attackers left a note requesting money in exchange for the decryption key.
Tool(s) used	The malicious actors used ransomware and phishing emails to infiltrate the company's system.
The 5 W's	• **Who**: a group of Unethical hackers. • **What**: A phishing email installed ransomware encrypting company files. • **When**: at 9:00 AM impeding business hours. • **Where**: A U.S. health care clinic. • **Why**: The attackers wanted financial gain which led them to compromising the company's system so that they could sell the company a decryption key.
Additional notes	1. This company should hold training to ensure employees are educated on the dangers of malicious links and phishing emails. 2. Limiting emails from unknown sources can also help the company's security posture.

Date: 2/19/2025	**Entry:** #2
Description	An employee received an email that had a malicious file attachment that had a password. The password was provided in the email and once put into the downloaded file it executed the malicious file on the device.
Tool(s) used	VirusTotal was used to examine file hash in order to determine whether it was malicious or not.
The 5 W's	Capture the 5 W's of an incident. • **Who:** Unidentified group of malicious attackers. • **What**: A malicious executable file. • **When**: 1:11pm the email attachment was received. 1:13pm the file was downloaded and opened. 1:15pm executable files are created on the device. 1:20pm The IDS sent an alert to the SOC as the executable files were detected. • **Where**: The incident happened on an employee's device through an email at a financial institution. • **Why:** The incident happened because the employee downloaded and opened the executable file. This was done so that the bad actors could exfiltrate the employee's data.
Additional notes	This is the file hash of the executable file: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b This is a malicious executable file that collects user data.

Date: 2/26/2025	**Entry:** #3
Description	An employee received a phishing email that contained a suspicious domain name. Unsure if other employees received the same email or if they have gone to the domain.
Tool(s) used	Chronicle was utilized in this investigation to analyze the suspicious domain and which employee visited the domain.
The 5 W's	Capture the 5 W's of an incident. • **Who:** Unknown attacker. • **What:** Employee received email with a suspicious domain attached to it. • **When:** 8:30 am. • **Where:** On an employee's email at a financial services company. • **Why:** Employees received a suspicious email containing the link to a domain. The domain appears to install malware once visited thus compromising the employee's device.
Additional notes	Investigating the domain (`signin.office365x24.com)` has shown that it appears likely to be malicious. Upon observing the domain 6 employee assets appear to have visited it which are Ashton Davidson, Bruce Monroe, Coral Alvarez, Emil Palmer, Jude Reyes, and Roger Spence. The phishing attack appears to be successful on the devices of Ashton and Emil. After analyzing the IP address of the domain it appears that another employee Warren Morris has also visited this malicious domain.

Date:	**Entry:**

2/27/2025	#4
Description	A U.S. financial services firm experienced a ransomware attack that encrypted important customer information. The attackers asked for a ransom payment in bitcoin to decrypt the data. This was done through a zero-day exploit and compromised employee credentials. This caused the firm to stop its normal operations.
Tool(s) used	None
The 5 W's	Capture the 5 W's of an incident. • **Who:** A group of unauthorized attackers. • **What:** A ransomware attack through a zero-day exploit in the firm's web app firewall as well as through compromised employee credentials from an employee who recently stopped working at the firm. • **When:** Wednesday at 10:30 am. • **Where:** It happened on the server of a U.S. financial service firm. • **Why:** This incident happened because of poor patch management and improper employee termination.
Additional notes	1. This incident could have been avoided if the firm properly deactivated the former employees credentials as soon as they left the firm. 2. If the firm had more rigorous patch testing they may have been able to avoid putting out a vulnerable patch. 3. The firm did great by isolating the affected systems but to mitigate the damage and improve the speed of the recovery the firm could have used a back of their servers to start up operations much sooner.