Incident handler's journal

Date: 21/09/2023 9:00 a.m.	**Entry 1#**
Description	Documenting an attack to the small health care clinic.
Tool(s) used	No tools have been used
The 5 W's	• **Who**: an unknown organize group • **What**: company's files are unable to be used due to a ransomware attack • **When**: Tuesday 9:00 a.m. • **Where**: US small health care clinic • **Why**: some employees reported that they were unable to access files and that a ransomware note was displayed on their screen. This malware has been able to enter the company due to target phishing emails that were sent to different employees of the clinic. These emails contained a malicious attachment that installed the malware on the employee's PC once it has been downloaded. This ransomware encrypted all organization's files and caused major disruption in their operations. The company was forced to shutdown their computer systems and contact several organizations to report the incident and receive technical support.
Additional notes	1. It is important to teach employees on how to recognize an phishing email to avoid this incident to happen again. 2. Should the company pay the hacker group to have their activity back in business? Or they rely on the several companies they asked for help?

Date: 28/09/23 11:15 a.m.	**Entry: 2#**
Description	An employee received an attachment to an e-mail, in the end it was an malicious payload.
Tool(s) used	VirusTotal website and the file hash of the payload.
The 5 W's	● An employee downloaded the file by a phishing e-mail he/she received. ● The employee downloaded the suspicious file, and he/she executed it on his PC. ● The accident occurred on 28/09/23 at 11:15 a.m. ● Inside the organization. ● The employee received a phishing e-mail, he/she downloaded the attachment and opened it on his/her PC utilizing the password that was sent with the e-mail. Once the suspicious file .exe got opened, the victim PC started to execute a malicious payload. Once I received the alert of an suspicious file got downloaded, I retrieved the file and created an SHA256 hash, for then compare the result with the VirusTotal website. There I got the confirm that the file was a malware.
Additional notes	The employee's PC must be repaired by doing a new clean installation of the OS used or using an old backup.

Date: 20/07/2022 9:30 a.m.	**Entry: 3#**
Description	In the date indicated, a phishing alert showed up on an employee's computer. After analyzing the hash, the file has been confirmed as malicious.

Tool(s) used	Hash of the file and the organization’s playbook.
The 5 W's	● An unknown user sent a phishing email to an employee. ● The employee opened the file. ● 20/07/2022 at 9:30 a.m. ● In the organization’s office. ● The employee received an phishing email from an unknown user and thinking it was a portfolio for job recruitment, he/she executed it.
Additional notes	The alert should be escalated because the phishing e-mail has an malicious attachment