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: 08.04.2024 Record the date of the journal entry.	**Entry:** 4 Record the journal entry number.
Description	Provide a brief description about the journal entry. Documentation of a spear phishing incident in the organization.
Tool(s) used	List any cybersecurity tools that were used. VirusTotal (1,2), AlienVault OTX, Online Research(1,2,3,4)
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? BlackTech Group • **What** happened? A suspicious file being downloaded on an employee's computer at a financial services company. Investigated and discovered to be a malicious file attachment to an email. • **When** did the incident occur? Wednesday, July 20, 2022 09:30:14 AM • **Where** did the incident happen? At a financial services company in Japan • **Why** did the incident happen?

	BlackTech is a suspected Chinese cyber espionage group, the use malware and aim to harm, steal information and spy on organization in East Asia--particularly Taiwan, Japan, and Hong Kong--and the US. Flagpro is used in the initial stage of attacks to investigate target's environment, download a second stage malware and execute it. BlackTech uses a spear phishing e-mail, the message is adjusted to its target organization. It is disguised as an e-mail communication with target's business partner. This means the attackers probed deeper into their target before attacking. They also adjust the contents of the file to the target. Therefore, it is not easy to feel at odds with the file sent by the attacker. And so, the employee was not able to recognize the file as malicious and mistakenly clicked it. However, it was possible to notice that the attached file was and executable file and not a resume file that would most likely be a text/pdf file. It is advisable to educate the employees on spear phishing, noticing files before downloading and specifically paying attention to these kinds of attacks. It is also advisable to create and install custom signature both on network and endpoint devices in order to detect attacks using Flagpro. In the bottom line – the employee was not suspicious of malware, and the malware was possibly able to download, this is avoidable.
Additional notes	Include any additional thoughts, questions, or findings. - Known malicious file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b - Email came from: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114> Attachment: filename="bfsvc.exe"