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: Record the date of the journal entry.	**Entry:** Record the journal entry number. 2
Description	Provide a brief description about the journal entry. Documentation of Cobalt Strike activity across my industry sector.
Tool(s) used	List any cybersecurity tools that were used. AlienVault, VirusTotal, Whois, Canadian Centre for Cyber Security Website (1, 2)
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? ALPHV Ransomware Group (BlackCat Ransomware Group) • **What** happened? The Canadian Cyber Centre assesses that ALPHV is almost certainly a financially motivated, Russian-speaking, RaaS cybercrime group that is very likely based in a CIS country. ALPHV/BlackCat is the first known ransomware written in the “Rust” programming language and can infect both Windows and Linux-based systems. ALPHV/BlackCat campaigns often involve triple-extortion, making ransom demands and using social engineering and MFA fatigue to gain foothold with the BlackCat ransomware.

	• **When** did the incident occur? 25th and 28th of March 2023 • **Where** did the incident happen? Toronto, Canada • **Why** did the incident happen? The Canadian Cyber Centre assesses that ALPHV/BlackCat are almost certainly financially motivated and have shown no pattern to victimization that suggests deliberate targeting. The assessment is that ALPHV/BlackCat and its affiliates very likely select their victims based on opportunity.
Additional notes	Include any additional thoughts, questions, or findings. Why was the malware undetected? How can we better prepare individuals for social engineering attacks such as theses? What are the specific differences that gave BlackCat an edge? could using Rust for example and looking for easy opportunities gave them an advantage?