Incident handler's journal

Date: 07/03/2025	**Entry:** 01
Description	A security incident occurred against a U.S. health care clinic on Tuesday, at 9:00 a.m. It was a ransomware attack organized by a group of unethical hackers that targets healthcare and transportations industries. They encrypted all files that stored patients data, forcing a shut down of the system and business operations. In order to restore the files, a demand of a large amount of money was made by the attackers. The incident emerged from a phishing attack containing malware, whose goal was to gain access to internal information.
Tool(s) used	N/A
The 5 W's	● Who - a group of unethical hackers; ● What - A ransomware attack against a small U.S. healthcare clinic; ● When - It happened on Tuesday, at 9 a.m; ● Where - On a U.S. healthcare clinic; ● Why - a phishing method was made by the hackers to steal money from the company.
Additional notes	The incident could be easily prevented by an early training with the workers about phishing methods and how to avoid them. Also, technical operations like configuring email filtering and an antivirus software would decrease the company's attack vectors.

Date: Not informed	**Entry:** 02
Description	A phishing attack occurred against an employee at a financial services company. The security incident was alerted for the SOC team, that eventually discovered a file containing malicious code, which was activated by a password sent on the email and then used by the employee to open the file.
Tool(s) used	N\A
The 5 W's	● Who - malicious actor; ● What - a phishing attack which involved a trojan on the email; ● When - Around 1:20 p.m.; ● Where - at a financial services company; ● Why - The malware was spread to infect the company's network and gain access to their data.
Additional notes	A further investigation was made to discover more about the malicious file. VirusTotal indicated some trojan files included, which was related to some domains and URLs investigated by other analysts before. This attack could be prevented if the employee contacted the security team to verify the file integrity.

Date: December 28, 2022, at 7:20 p.m..	**Entry:** 03
Description	A Broken Access Control was exploited by a malicious actor at a mid-sized retail company, which gained information about many customers PII and SPII that use the e-commerce company's website. This vulnerability allowed the attacker to perform a forced browsing attack and access customer transaction data by modifying the order number included in the URL string of a purchase confirmation page. An amount of money was requested for an employee in order to retrieve the data stolen, through external emails sent to the worker. It was sent two times. The email sender claimed that they had successfully stolen customer data. In exchange for not releasing the data to public forums, the sender requested a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it. The same employee received another email from the same sender. This email included a sample of the stolen customer data and an increased payment demand of $50,000. The worker contacted the security team right after, and then an investigation began.
Tool(s) used	N\A
The 5 W's	● Who - Malicious actor; ● What - data theft by a Broken Access Control exploitation, besides a payment request in order to retrieve data stolen; ● When - At December 28, 2022, at 7:20 p.m.; ● Where - a mid-sized retail company; ● Why - The exploit discovered by the hacker was used to request money in order to recover the data stolen.
Additional notes	Approximately 50,000 customer records were affected, and the financial

	impact estimated is around $100,000,000. The recommendations made by the security team were to perform a routine vulnerability scan, improve the role-based access and least privilege principles and do penetration tests frequently.