Incident handler's journal

Date: 02/06/2024	**Entry: 1**
Description	U.S. healthcare ransom incident
Tool(s) used	**None**
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A group of unethical hackers • **What** happened? Targeted phishing emails were used to install malicious software on computer that granted access and allowed encryption of critical files on the system. • **When** did the incident occur? 9:00 am • **Where** did the incident happen? At the U.S. healthcare clinic • **Why** did the incident happen? Lack of education of various social engineering techniques. No up to date anti-malware software installed on systems.
Additional notes	Employee education is necessary to mitigate future social engineering attacks. If employees do not know what to look out for they will be unable to discern legitimate business operations from malicious attacks.

Date: 02/07/2024	**Entry:** 2
Description	A suspicious file download was detected on an employee's computer. It was determined through a VirusTotal check to be a malicious password-protected spreadsheet file received by email. After the file is executed it delivers a trojan virus that attempts to collect SPII and take control of the host computer.
Tool(s) used	SHA256 decryption; VirusTotal. The decryption was used to compare similar fil hashes using the VirusTotal website. VirusTotal is a trusted website that aggregates malicious file/url data for comparison and detection.
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? An employee at the financial services company • **What** happened? A malicious file was downloaded by email to an employee computer. • **When** did the incident occur? NA • **Where** did the incident happen? At the financial services company grounds • **Why** did the incident happen? Lack of employee knowledge of malicious email best practices.
Additional notes	Classic lack of information at a critical moment. Employee education would prevent suspicious downloads/links. Add to that a HIDS would detect and quarantine a trojan like this with ease. I knew about VirusTotal but never thought to visit the site and get a complete picture of what it does.

Date: 02/07/2024	**Entry:** 3
Description	On 12/22/2022 at 3:13, PT a malicious actor sent a ransom email to an employee demanding $25,000 in cryptocurrency. Then on 12/28/2022 the same employee receives another email containing sample ransom data and a demand for $50,000. Approximately 50,000 customer records were affected with a an estimated financial impact of $100,000 in direct costs and potential revenue loss.
Tool(s) used	SIEM web server log analysis
The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? A malicious actor • **What** happened? A forced browsing attack accessed customer transaction data by modifying the order number included in the URL of the transaction confirmation page allowing access to customer data • **When** did the incident occur? 12/22/2022 - 12/28/2022 • **Where** did the incident happen? On site • **Why** did the incident happen? Lack of routine vulnerability scans and pen testing. No access control mechanisms in place blocking requests outside of specific ranges. No authentication required for user access to sensitive customer data.
Additional notes	Unfortunate side effect of no defense in depth handling to prevent an incident of this scale from happening. This was a very fun example of a very scary and possible real life scenario playing out.