Incident handler's journal

Date: 12/09/2024	**Entry: #1**
Description	On Tuesday morning at 9:00am, employees reported not being able to access their files and seeing a ransom note on their desktop. The threat actors gained access to the network through a phishing email sent to several employees that contained an attachment that downloaded the ransomware once opened.
Tool(s) used	None.
The 5 W's	• **Who**: A group of notorious unethical hackers • **What:** They encrypted all files and demanded a ransom for the decryption key • **When**: Tuesday at 9:00am • **Where**: Healthcare clinic • **Why**: An employee fell for the phishing email and opened an attachment that downloaded the ransomware. The hackers are demanding money, so their motivation is financial
Additional notes	• How can this be prevented in the future? • Should the company pay the ransom?

Date: 12/11/2023	**Entry: #2**
Description	An employee downloaded a file from an email containing a Trojan that started creating multiple executable files.
Tool(s) used	VirusTotal
The 5 W's	• **Who:** Internal (employee) • **What:** Phishing – Attachment-based malware (Trojan) • **When:** 1:13pm • **Where:** employee's computer • **Why:** employee downloaded the malware disguised as an attachment in an email they received.
Additional notes	• Additional security training needs to be provided to the employees in regards to opening and downloading files from untrusted or unknown sources • Malware needs to be contained and recovery needs to be initiated • Escalates to Tier-2 team

---

Date: 12/16/2024	**Entry: #3**
Description	An unauthorized actor gained access to an estimated 50,000 customers' PII and financial information, causing an estimated loss of $100,000 in direct costs and loss of revenue.
Tool(s) used	None.
The 5 W's	Capture the 5 W's of an incident. • **Who**: outside threat actor • **What**: forced browsing attack by modifying the order number on the URL string. • **When**: December 28th, 2022 at 7:20pm PT • **Where**: online web application • **Why**: There was no access control list for different URLs that allowed unauthorized users to access information they were not supposed to.
Additional notes	• Implemented allowlisting to a range of URLs to only allow specific requests and automatically blocks all other ones. • Implemented more frequent routine vulnerability assessments

---

Date: 12/18/2024	**Entry: #4**
Description	There were over 100 failed login attempts for root access simultaneously from different unidentified IP addresses.
Tool(s) used	Splunk
The 5 W's	Capture the 5 W's of an incident. • **Who**: outside threat actor • **What**: failed root login attempts • **When:** March 6th, 2023 at 01:39:51 am • **Where:** mailsv/secure.log • **Why:** Unclear. Since there was no successful attempt, the threat actor could not follow through. Since they were trying to gain root access, it's possible they were trying to exfiltrate information, encrypt critical information for ransomware, or gain access to customer financial information, among others.
Additional notes	N/A

Date: 12/19/2024	**Entry: #5**
Description	Employees Ashton Davids and Emil Palmer got their credentials stolen after falling for a phishing email and accessing the fake sign-in domain signin365x24.com
Tool(s) used	Google Chronicle
The 5 W's	Capture the 5 W's of an incident. • **Who:** outside threat actor • **What:** phishing email • **When** January 1st, 2023 at 2:40:40 pm • **Where**: domain signin365x24.com • **Why**: employees received an email that contained a link that redirected them to a login page claiming to be the company's new login portal. After failing to recognize the email as phishing, two employees input their credentials, which the threat actors then used to gain access to their accounts.
Additional notes	• The affected accounts need to be isolated, recovered and restored. • Phishing email identification training needs to be provided to the company to avoid future incidents

---