# Incident handler's journal

| | |
|---|---|
| **Date:** 07/05/2023 | **Entry:** 1 |
| Description | A small US health care clinic experienced a security event. This entry falls under NIST's Incident Response Lifecycle of Detection and Analysis. The attack has happened and is ongoing, so I am reviewing the 5 W's of the incident to gather more intelligence. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who**: An organized group of unethical hackers<br>● **What**: A ransomware attack, originating from phishing emails. Several employees reported that they were unable to use their computers to access files like medical records. Business operations shut down because employees were unable to access the files and software needed to do their job.<br>● **When**: Tuesday morning, at approximately 9:00 a.m.<br>● **Where**: Occurred in the health care clinic.<br>● **Why**: The attackers were able to gain access into the company's network by using targeted phishing emails, which were sent to several employees of the company. The phishing emails contained a malicious attachment that installed malware on the employee's computer once it was downloaded. Once the attackers gained access, they deployed their ransomware, which encrypted critical files. Their motive most likely was money, as they demanded money in exchange for the decryption key. |
| Additional notes | If the company acquiesces to the ransom note, will the attackers demand more |

| | |
|---|---|
| | money and/or not provide the decryption key? |

---

| | |
|---|---|
| **Date:** 7/11/2023 | **Entry:** 2 |
| Description | A security event researching IoCs. This falls under the category of Detection and Analysis in the NIST Incident Response Lifecycle. I am alerted to a suspicious file download, and analyze whether the SHA256 file hash is malicious or not. |
| Tool(s) used | VirusTotal. The tool is used to determine whether files, hashes, etc are deemed malicious. They have a score determining how dangerous a file could be. |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who**: A malicious actor by the name of "Clyde West". Email says it is from "Def Communications".<br>● **What**: A suspicious file was downloaded on an employee's computer.<br>● **When**: Files downloaded and execution occurred approx at 1:15 PM. Email from attacker sent at 09:30:14 AM.<br>● **Where**: Occurred within the company's physical location.<br>● **Why**: The affected employee received an email containing an attachment that was a password-protected spreadsheet file, with the password to the file in the email. The employee downloaded the file, then entered the password to open it. Once the file was opened, a malicious payload was then executed on the employee's computer. |
| Additional notes | This file was determined to be malicious by looking at SHA256 file hash 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b through VirusTotal. Threat label flagpro and category trojan. |

| | |
|---|---|
| | Indicators of Compromise found:<br>- One IP address: 108.177.119.113<br>- Multiple domain names such as:<br>  - windowsupdatebg.s.llnwi.net<br>  - org.misecure.com<br>  - misecure.com<br>- One URL: http://org.misecure.com/favicon.ico<br>Under behavior, there is mention of creating files in the user directory (masquerading). Also mentions input capturing. |

---

| | |
|---|---|
| **Date:** 7/12/2023 | **Entry:** 3 |
| Description | Reviewing aftermath of a data theft security incident from a final report. This is the NIST's Incident Response Lifecycle Post-incident Activity part. Reviewing and examining areas to improve are part of the post-incident activity. |
| Tool(s) used | None. |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who**: An attacker with an external email address.<br>● **What**: The external attacker gained unauthorized access to customer personal identifiable information (PII) and financial information. Approximately 50,000 customer records were affected.<br>○ On Dec 22nd, an employee received an email from an external email address. The sender claimed they stole customer data. In exchange for not releasing the data to the public, the sender demanded a $25,000 cryptocurrency payment. The employee assumed the email was spam and deleted it. Six days later on the |

| | |
|---|---|
| | 28th, the same employee received another email from the same sender; It included a sample of the stolen customer data and an increased payment demand of $50,000.<br>● **When**: Approximately 3:13 PM, PT, on December 22, 2022.<br>● **Where**: The employee that received the email was onsite at one of the company's physical locations.<br>● **Why**: The cause of the incident was due to a vulnerability in the e-commerce web application. It 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. |
| Additional notes | The final report included this for future prevention:<br>● Perform routine vulnerability scans and penetration testing.<br>● Implement the following access control mechanisms:<br>○ Implement allowlisting to allow access to a specified set of URLs and automatically block all requests outside of this URL range.<br>○ Ensure that only authenticated users are authorized access to content. |

| **Date:** 07/18/2023 | **Entry:** 4 |
|---|---|
| Description | Querying a suspicious domain signin.office365x24.com. This is the NIST's Incident Response Lifecycle portion of Detection and Analysis. I am reviewing information in Google's Chronicle to gather the 5 W's of the security incident to determine next steps. |
| Tool(s) used | Google's Chronicle. It is used for querying and it collects, aggregates, and |

| | |
|---|---|
| | normalizes logs for users to review in a centralized area. |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who**: Based on Chronicle's VirusTotal WHOIS lookup, by a user with the email address of 9a6229aeb54b0cc2s@kamtrononline.com in Indiana.<br>● **What**: An employee received a phishing email in their inbox. An alert was sent and identified a suspicious domain name contained in the email's body: signin.office365x24.com. Other employees may have been sent emails from this domain and visited the domain.<br>● **When**: First occurrence based on the timeline for a POST request is Jan 31st 2023 at 14:40:45.<br>● **Where**: Incident occurred on company's premises.<br>● **Why**: There was a gap in security to block external emails to prevent phishing emails being sent to employees. |
| Additional notes | **In Chronicle, includes ET INTELLIGENCE REP LIST information below:**<br>Category: Drop site for logs or stolen credentials<br>Confidence (Min: 20, Max: 127): 22<br>Severity: Medium<br><br>Multiple assets (6) have accessed the domain.<br><br>**Under RESOLVED IP ADDRESS, reviewed 40.100.174.34:**<br>TIMELINE: New POST request on Jan 31st 14:51:45.<br>ASSETS: Additional affected asset titled warren-morris-pc.<br>DOMAINS: signin.office365x24.com and signin.accounts-gooqle.com were the domains for this IP address. |

| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>Record the journal entry number. |
| Description | Provide a brief description about the journal entry. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who** caused the incident?<br>● **What** happened?<br>● **When** did the incident occur?<br>● **Where** did the incident happen?<br>● **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

## Need another journal entry template?

If you want to add more journal entries, please copy one of the tables above and paste it into the template to use for future entries.

Reflections/Notes:

1. Were there any specific activities that were challenging for you? Why or why not?
   Activities that did not use any tool were more challenging. Reviewing information without a tool can be challenging, because I will have to rely on human words that may be unable to describe the full scope of the situation.
2. Has your understanding of incident detection and response changed since taking this course?
   My understanding has drastically changed. There are many aspects that constantly repeat, and some overlap. Detection and Analysis can go into Post-Incident Analysis. You can do Detection and Analysis as you Contain, Eradicate and Recover. This cycle requires a lot of careful thinking and reviewing

to make sure you have as much as the full picture as possible when handling incidents.

3. Was there a specific tool or concept that you enjoyed the most? Why?

    I enjoyed Chronicle the most, because it included a grading from VirusTotal. I appreciate that it aggregates information in one centralized area for me to review. There are different ways to look at information as well, and I like having options when researching.