**Incident handler's journal**

**SOC Analyst: Christopher D’Angelantonio**

| **Date:**  **May 25, 2024** | **Entry:**  **CSJ001-01- Incident Documentation** | | |
| --- | --- | --- | --- |
| **Description** | a U.S-based health care organization encountered a security-related event, as a result of a supposed phishing email ploy containing a malware attachment. Once the email's ransomware attachment was unknowingly executed within their systems, it deployed a encrypted lock over their organizational data for which demanded a ransom to be met.Informatively, this attack took place at 9:00 a.m this last Tuesday and reportedly sabotaged their ongoing business operations and services. | | |
| **Tool(s) used** | * Malware * Ransomware software * Asymmetric encryption algorithms * Symmetric encryption algorithms * System shutdown & recovery * Detection and analysis * Post-incident activity * NIST incident response lifecycle * Preparation * Containment, eradication and recovery * Remediation | | |
| **The 5 W's** | * A group of **unethical hackers** caused this phishing email incident and cryptoviraogical attack (Ransomware). * Employees were victimized by a targeted phishing email that contained malware attachments for which upon unintentional system installation deployed a ransomware attack upon the organization's critical and sensitive medical data, which encrypted the data until a specified ransom amount was paid. Ultimately, this cyberattack shut down the businesses medical operations and has prevented its employees from performing their jobs, so the healthcare organization responded with system containment, reporting the incident, practices the stages of the NIST Incident Response Lifecycle and consulting professional incident response procedures. * This incident occurred at 9:00 a.m Tuesday morning. * Small healthcare company, based in the U.S. * Company was targeted by a phishing scam containing malware, which was downloaded to their IT system by unsuspecting employees. | | |
| **Additional notes** | Questionably, I contemplate the possibility that the phishing emails were made possible by a potential employee data leak and maybe even through an internal source, since the threat actor would need specific employee emails to target with the malware infested phishing scams in order to prompt the execution of this ransomware attack. Notably, I recommend that the healthcare company apply the cyclical procedures of the NIST Incident Response Life Cycle further to mitigate the situation as well as preventably remedy future occurrences. | | |

| **Date:**  May 29, 2024 | **Entry:**  **CSJ002-01-Incident Response Analysis** | | |
| --- | --- | --- | --- |
| **Description** | Data driven organizations specific employees were sent a phishing email containing unauthorized executable files, for which were opened and installed on employee computers and led to the installation of several unauthorized files within their associative systems. As a result of this IoC or threat event, the organization's IDS alerted the SOC of the installment of these unauthorized and potentially malicious files. Thus, as a security analyst assigned with forensically analyzing this security incident, I was tasked with comparing the email-relative file attatchment’s hash with that of the ratings of a crowdsourcing community of security vendors and security-relative specialist reports on TotalVirus in order to determine if the file was indeed malicious. | | |
| **Tool(s) used** | * Threat intelligence service (VirusTotal) * File hash * Forensic analytics * Incident response life cycle | | |
| **The 5 W's** | * Threat Actor or suspicious file owner who sent the spear phishing emails. * Employees opened email attachments containing unauthorized exe. files that were downloaded on their work computers. * 11:29:29 p.m last tuesday. * The incident occurred within the mailboxes of certain employees and the files were executed within their respective work computers. * The IDS detected the unauthorized file downloads from a suspected phishing attack and alerted the SOC. | | |
| **Additional notes** | Based on extensive analytics conducted on the incidents report, timeline and file hash as well as the substantial amount of malicious file indicators found within the investigation, I deemed the file as indeed malicious in nature.u\ | | |

| **Date:**  May, 30 2024 | **Entry:**  **CSJ003-01- Investigating Suspicious Hash File** | | |
| --- | --- | --- | --- |
| **Description** | Specifically, I determined an IDS generated alert ticket (A-2703) to possess valid threat indications through considering a collection of different prominent IoC indicators present within the suspected phishing email as well as through investigating the IoA or malware indications, that were present within the threat intelligence analysis, for which I conducted on the hash of its file attachment via TotalVirus. Specifically, company employees were sent suspicious emails that seemed malicious in nature and contained unauthorized execution file attachments, which were then mistakenly installed on their work computers, for which then resulted in triggering a subsequent security alert ticket. Thus, I was forced to escalate this alert ticket up the SOC chain of command in order to be investigated for further risk assessment, threat mitigation and incident response. | | |
| **Tool(s) used** | * IDS * Threat Intelligence service (VirusTotal) * Incident response life cycle (Threat alert escalation) * SOC procedures * Alert ticket investigations * Threat hunting * Hash File Investigation | | |
| **The 5 W's** | * Unsuspecting employees who received the malicious emails. * Phishing emails containing exe. malware infected files compromised their employee computers. * July 20, 2022 at 09:30:14 AM. * Within employee mailboxes and on their local machines. * Employees had inadvertently executed the malicious email attachment files on their computers or clicked an unsafe attachment link. | | |
| **Additional notes** | Upon analyzing the contents of the email for evident threat indications, I noticed that the email possessed a multitude of spelling errors and grammar mistakes, which are usually strong indicators of a non-legitimate or fraudulent message source. Additionally, the email also possessed inconsistencies like a mismatched email address and sender name as well as an unauthorized exe. file attachment, which is often a valid indicator of potential malware or unethical activity. Moreover, I have also seen that this email possessed an inorganic sender IP address along with an inauthentic web address and sender alias. After analyzing the file's hash provided within the ticket through searching for it on a crowdsourcing or community-driven threat intelligence web service called VirusTotal and referencing historical vendor reviews, I noticed an array of true positive indicators that may suggest this file is indeed malware or malicious in nature. Besides the hash file having a 61/73 community score and roughly an 85% vendor rating along with a red threat level indication, it also possessed malicious behaviors when tested in IDEs like user-input capture as well as direct cpu clock access along with data manipulations. Notably, the files hash descriptions contained keywords like Trojan, malicious and backdoor and its connection details showed that the file sent HTTP requests to a prominently malicious web address or URL (http://org.misecure.com/index.html). Therefore, I am compelled to close and escalate this security event ticket up the SOC chain of command to the SOC Tier 2 analyst for further incident response action. | | |

| **Date:**  May 31, 2024 | **Entry:**  **CSJ004-01- (NIST ILRC): Post Activity- Final Report Review** | | |
| --- | --- | --- | --- |
| **Description** | According to the post-incident report forged by the responding CSIRT of a victimized retail and e-commerce driven organization, a large-scale data breach took place that negatively impacted a million of their web users. Supposedly, this attack transpired by way of a threat actor breaching the web server of their respective web application through gaps in its security defenses to exfiltrate financial PSI of their customers. Following the breach, an employee received a disturbing email from an external source address, that originally demanded that the organization pay a hefty ransom sum in a particular cryptocurrency or else their stolen customer financials would be unethically publicized. However, the employee ignored the ransom request, since they were not aware of its validity, but the second email that was received days after had provided a provoking sample of stolen customer financials and demanded a greater ransom amount be paid or it will be exploited. As a result, the employee alerted the organizations CSIRT, who then began an ongoing investigation of the incident, to identify the 5 W’s relative to the root cause of the breach and to locate the attack vector as well as the vulnerabilities that were exploited. | | |
| **Tool(s) used** | * NIST incident response life cycle * NIST CF * Post incident activities * Lessons learned recommendations * Vulnerability assessment or analysis * Root cause analysis * Security posture improvements * Threat analysis * Response and remediation processes * Digital Forensics | | |
| **The 5 W's** | * Threat Actor seeking to steal or to tamper with customer PII. * Large scale data breach affecting a million users. * Incident between December 28, 2022, at 7:20 p.m., PT - December 31, 2022. * Within the purchase confirmation page of the organization's web application. * The incident occurred due to several gaps in the organization’s server access control list and application layer securities, that pertain to limiting unauthenticated application log access, so that unauthenticated threat actors cant have access to log data containing URLs generated by their purchase confirmation page of their web application. Ultimately, this left their customer’s PII wide open for a brute force URL guessing, unauthenticated access to data logs and customer PII exfiltration to occur, which then resulted in a ransom demand. | | |
| **Additional notes** | Essentially, it is imperative for the companies CSIRT as well as their SOC team and other relative stakeholders to correct the vulnerabilities within their web defenses and application security procedures, to remedy the possibility of any future data breaches from taking place in the future. Firstly, it's critical that their web servers' resource access control list are consistently configured to a limited range of potential URL’s at the application layer of their NIST CSF in order to make sure that threat actors cannot gain unauthenticated access to their network logs and exploit this vulnerability. This change is necessary so that their organization can ensure the long term continuity, regulatory cooperation, operational functionality and the positive PR sentiment of their business, while also preventing this type of threat from occuring in the future. Primarily, the business can reinforce a safety-first security plan organizational and a stronger security posture through implementing routine vulnerability scans and conducting regular penetration tests on their web securities in order to detect potential vulnerabilities before they are exploited. Consequently, neglecting to make the necessary changes to their CSF as well as their SPP would be dire to its financial security as well as catastrophic for its responsibility to protect the CIA of the customer’s financial records, especially when considering that the company suffered a $100,000 loss and 50,000 customer records had been compromised as a result of the incident. | | |

### 

| **Date:**  **June 2, 2024** | **Entry:**  **CSJ005-01 - Splunk Log Analysis & Querying** | | |
| --- | --- | --- | --- |
| **Description** | In this security report, I effectively utilize the data analysis software called “*Splunk>*”, via leveraging the Splunk Query Language (SPL), to compile, query and analyze event data from system logs relative to a collection of normalized login data extracted from an index of log files attached to the data flows throughout a mailing server, that are aggregated from across all facets of the e-commerce store (Buttercup Games) | | |
| **Tool(s) used** | * *Splunk>* Data Analysis Software * Data Analysis * Log Analysis * Log Management * Splunk Query Language (SPL) * Search Processing Language (SPL) | | |
| **The 5 W's** | * Uploaded organizational dataset * Queried indexed data * Analyzed search queries * Reviewed data sources related to logs of interest * Identified failed SSH login attempts | | |
| **Additional notes** | Applying smaller time modifier filters on SPL search queries produces a more accurate log search as well as improved system performance and a better overall log management result. Notably, having the ability to apply simple, but concise SPL commands within Splunk can allow for more narrowed search results to extract specific data from a wide range of log hosts and can aid in expediting the log management processes of security practitioners. | | |

| **Date:**  **June 3, 2024** | **Entry:**  **CSJ-006-001 - Chronicle Domain Analysis & Querying** | | |
| --- | --- | --- | --- |
| **Description** | As a security analyst who has been hired by a financial service company to identify, analyze and respond to security event alerts via using a SIEM tool (Chronicle) as well as (TotalVirus) threat intelligence services, I encountered an alert regarding a suspicious phishing email incident. Informationally, I was sent an alert pertaining to an email that a company worker had delivered within their inbox, for which I then started to assess potential IOCs that would raise red flags of valid security incidents. Upon reviewing the email I noticed that it possessed a shady domain name within its contents and began applying the email to the Chronicle data analysis platform. I began by running a search on the domain, so I could analyze a collection of historic logs, to aid in determining whether this domain was in fact malicious in nature and whether or not other personnel had come in contact or ventured to it as well. Notably, to make that determination, I first sifted through the event logs that had been ingested by Chronicle via leveraging applicable and relative information like hostnames, IPs, email addresses and more. Based on the maliciously favored domain information compiled, the unauthorized outbound data traffic recorded and the log events studied, I deemed this file as indeed malicious, which would make the domain a false negative when considering its vendor and community ratings, but confirms that the alert was a valid IOA. | | |
| **Tool(s) used** | * Chronicle data analysis software * VirusTotal threat intelligence service * Crowdsourcing * Data analysis * Log analysis * Log management * Queried indexed data * Analyzed search queries * Reviewed data sources related to logs of interest * Identified work emails and data requests to the domain | | |
| **The 5 W's** | * The domain owner associated with the signin.office365x24.com domain and the employees that interacted with its contents. * Employee received a phishing email to a shady domain, which triggered an IDS and SIEM alert for incident assessment. * January 31, 2023 2:40:40 p.m approx. 16 months ago * In the mail server and mailboxes of company employees. * Employees received and interacted with shady emails. | | |
| **Additional notes** | * There was no additional information about this domain during VT Lookup. * Community score of 6/93 and low vendor rating * VT Context indicated that 6 vendors tagged the domain to be malicious. * 8 POST requests & 24 GET requests indicated data packet traffic to the domain. * 9 File transmissions to the domain’s resolve IP. * The domain resolve showed that the original domain (**signin.office365x24.com**)’s IP address was connected to another domain (**signin.accounts-google.com**), but exhibited different top domains. * Overall true positive indicators of a malicious domain and a positive indication of phishing email activity. * **signin.accounts-gooqle.com - signin.office365x24.com** * **3 Assets accessed the domain:**   roger-spence-pc  emil-palmer-pc  coral-alvarez-pc   * **11 http connections to the unresolved IP address**   40.100.174.34 | | |

| **Reflections/Notes:**   * **Were there any specific activities that were challenging for you? Why or why not?**   I thought that the hashing file analysis took a little bit longer than normal for me to fully grasp compared to the other security incidents, being that I had very minimal experience with analyzing the characteristics of hashing malicious hashing files as well as with understanding the difference between the hash functions they use or how well they protect data given the security level of its algorithm. Although I found that particular exercise to be more demanding of my focus, I was able to grasp these concepts through my dedicated studies. Overall, I found it to be simple to absorb, retain and thoroughly understand the array of security practices, tools and processes that I was expected to demonstrate throughout the duration of this program.   * **Was there a specific tool or concept that you enjoyed the most? Why?**   The specific activities within this journal that I thought were particularly useful to me were the activities pertaining to the analysis and post activity stage of the incident response life cycle, since these entries required an in-depth understanding of the dynamic fundamentals behind how interconnected networks communicate with each other. Specifically, there are an overwhelming amount of data packets, system logs, and informational records being synchronized throughout an organization's IT infrastructure in order for their business to operate as it should and provide several different services to the end users. However, without a strong security posture, SPP and framework coupled with security controls and system configurations that are proactively designed to block threats and eradicate intrusions when present or prevent them before they even occur a company’s assets are at direct exposure to the harsh elements of cyberspace. Proverbially, the security of an organization is quite similar to the way a person would physically protect their own home, since a home would be doomed if it was made out of glass since it would be easy to penetrate, hard to protect and tough to manage. Similarly, cybersecurity operates in the same sense, but instead of doors, walls, windows, locks, home security systems, etc. it has a depth of various virtual and physical safety methods for protecting your digital assets, which in the ever evolving technological age of today is quintessential to our day to day lives. Essentially, cybersecurity and the infinitely transforming digital landscape for which it resides is technically complex and dynamically tough in nature, while also requiring the simplicity, flexibility and versatility needed to make that landscape safe for an organization or p2p collaborations despite having to operate with a plethora of moving parts and vulnerabilities. Thus, I believe that gaining a deep familiarity with these incident and threat response concepts will help me be a more well rounded individual in my future career as a security analyst, since it will allow me to form logically comprehensive conclusions while critical thinking, problem solving or articulating my thoughts with other team members to solve real world security issues.   * **Was there a specific tool or concept that you enjoyed the most? Why?**   The security tools that I found to be quite fascinating during this course were the IDS and IPS systems as well as the SIEM, since both the intrusion systems detect threats by applying packet and traffic behaviors, log signatures and header information to a series of tailored security configuration and access logs. These indicators help these security systems to identify what activities ought to be deemed above the baseline or potential anomalies, or IOC and alert SOC analyst via an incident ticket to initiate the incident response investigation process and acyclic life cycle stages. Mainly, it is within these vital procedures of the DAL, that an organization's security posture and incident response, threat handling and preventative procedures are improved upon, which means that without the effective execution of these steps and an organization's security posture would not grow to be able to handle the endless evolution of threat actors or attack methods and complete lack of threat intelligence for the entirety of the cyber community. Notably, I also enjoy the fact the SIEM tool allows for the total normalization and structuration of data from all endpoints of an organizational network for which it displays on a convenient all in one dashboard, since this will make my up-coming career as a security analyst to be much more seamless, being that I can focus my efforts on priority tasks instead of tedious or time consuming operations like compiling data of interest. |
| --- |