**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:** July 23, 2023 | **Entry:** #1 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None. |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: A ransomware security incident * **Where**: At a health care company * **When**: Tuesday 9:00 a.m. * **Why**: The incident happened because unethical hackers were able to access the company's systems using a phishing attack. After gaining access, the attackers launched their ransomware on the company's systems, encrypting critical files. The attackers' motivation appears to be financial because the ransom note they left demanded a large sum of money in exchange for the decryption key. |
| Additional notes |  |

|  |  |
| --- | --- |
| **Date:** Jan 2, 2024 | **Entry:** #2 |
| Description | Investigate a suspicious file hash |
| Tool(s) used | For this activity, I used VirusTotal, which is an investigative tool that analyzes  files and URLs for malicious content such as viruses, worms, trojans, and more.  It's a very helpful tool to use if you want to quickly check if an indicator of  compromise like a website or file has been reported as malicious by others in  the cybersecurity community. For this activity, I used VirusTotal to analyze a file  hash, which was reported as malicious.  This incident occurred in the Detection and Analysis phase. The scenario put  me in the place of a security analyst at a SOC investigating a suspicious file  hash. After the suspicious file was detected by the security systems in place, I  had to perform deeper analysis and investigation to determine if the alert  signified a real threat. |
| The 5 W's | * **Who**: An unknown malicious actor * **What**: An email sent to an employee contained a malicious file   attachment with the SHA-256 file hash of  54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab5  27f6b   * **Where**: An employee's computer at a financial services company * **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the   intrusion detection system detected the file   * **Why**: An employee was able to download and execute a malicious file   attachment via e-mail. |
| Additional notes | 1. The file hash has been reported as malicious by over 50 vendors. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech. |

|  |  |
| --- | --- |
| **Date:** Jan 3, 2024 | **Entry:** #3 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None. |
| The 5 W's | * **Who**: An employee * **What**: a malicious file from a phishing email * **Where**: At financial services company * **When**: Wednesday 9:38 a.m. * **Why**: The incident happened because an employee downloaded and opened a malicious file from a phishing email. There is an inconsistency between the sender’s email address “76tguy6hh6tgftrt7tg.su’” the name used in the email body “Clyde West,” and the sender’s name, “Def Communications.” The email body and subject line contained grammatical errors. The email’s body also contained a password-protected attachment, “bfsvc.exe,” which was downloaded and opened on the affected machine. Having previously investigated the file hash, it is confirmed to be a known malicious file. Furthermore, the alert severity is reported as medium. With these findings, I chose to escalate this ticket to a level-two SOC analyst to take further action. |
| Additional notes | Known malicious file hash:  54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b  Email:  From: Def Communications <76tguyhh6tgftrt7tg.su> <114.114.114.114>  Sent: Wednesday, July 20, 2022 09:30:14 AM  To: <hr@inergy.com> <176.157.125.93>  Subject: Re: Infrastructure Egnieer role  Dear HR at Ingergy,  I am writing for to express my interest in the engineer role posted from the website.  There is attached my resume and cover letter. For privacy, the file is password protected. Use  the password paradise10789 to open.  Thank you,  Clyde West  Attachment: filename="bfsvc.exe" |

|  |  |
| --- | --- |
| **Date:** Dec 28, 2022 | **Entry:** #4 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | None. |
| The 5 W's | * **Who**: An individual unethical hackers * **What**: a vulnerability in the e-commerce web application. * **Where**: At a retail company * **When**: Thursday 3:13 p.m * **Why**: The incident happened because a vulnerability in the e-commerce web application. 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. This vulnerability allowed the attacker to access customer purchase confirmation pages, exposing customer data, which the attacker then collected and exfiltrated. After confirming the web application vulnerability, the security team analyzed the web application access logs. The logs indicated that the attacker accessed the information of thousands of purchase confirmation pages. |

|  |  |
| --- | --- |
| **Date:** Jan 6, 2024 | **Entry:** #5 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | Splunk. |
| The 5 W's | * **Who**: An individual unethical hackers * **What**: a vulnerability in the company’s main server. * **Where**: At a e-commerce company * **When**: Saturday 11:22 AM * **Why**: The incident happened because a vulnerability in the company’s main server. This vulnerability allowed the attacker to perform a brute force attack and access the server by using. This vulnerability allowed the attacker to access to all of the company’s data that are stored on the main server, which the attacker then collected and exfiltrated. After confirming the vulnerability, the security team analyzed the server access logs. The logs indicated that the attacker accessed the information of thousands of employees information pages. |

|  |  |
| --- | --- |
| **Date:** Jan 7, 2024 | **Entry:** #6 |
| Description | Documenting a cybersecurity incident |
| Tool(s) used | Chronicle. |
| The 5 W's | * **Who**: 6 employees accessed the site * **What**: a stolen credntials * **Where**: at financial services company * **When**: Sunday 2:33 PM * **Why**: The incident happened because a vulnerability in the company’s main server. This vulnerability allowed the attacker to perform a brute force attack and access the server by using. This vulnerability allowed the attacker to access to all of the company’s data that are stored on the main server, which the attacker then collected and exfiltrated. After confirming the vulnerability, the security team analyzed the server access logs. The logs indicated that the attacker accessed the information of thousands of employees information pages. |

|  |  |
| --- | --- |
| **Date:** July 25 2024 | **Entry:** #7 |
| Description | Analyzing a packet capture file |
| Tool(s) used | For this activity, I used Wireshark to analyze a packet capture file. Wireshark is a  network protocol analyzer that uses a graphical user interface. The value of  Wireshark in cybersecurity is that it allows security analysts to capture and  analyze network traffic. This can help in detecting and investigating malicious  activity. |
| The 5 W's | * **● Who: N/A** * **● What: N/A** * **● Where: N/A** * **● When: N/A** * **● Why: N/A** |
| Additional notes | I've never used Wireshark before, so I was excited to begin this exercise and  analyze a packet capture file. At first glance, the interface was very  overwhelming. I can see why it's such a powerful tool for understanding  network traffic. |

|  |  |
| --- | --- |
| **Date:** July 25 2024 | **Entry:** #8 |
| Description | Capturing my first packet |
| Tool(s) used | For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the  command-line interface. Similar to Wireshark, the value of tcpdump in  cybersecurity is that it allows security analysts to capture, filter, and analyze  network traffic. |
| The 5 W's | * **● Who: N/A** * **● What: N/A** * **● Where: N/A** * **● When: N/A** * **● Why: N/A** |
| Additional notes | I'm still new to using the command-line interface, so using it to capture and  filter network traffic was a challenge. I got stuck a couple of times because I  used the wrong commands. But after carefully following the instructions and  redoing some steps, I was able to get through this activity and capture network  traffic. |

|  |  |
| --- | --- |
| **Date:** July 27 2024 | **Entry:** #9 |
| Description | Capturing my first packet |
| Tool(s) used | For this activity, I used tcpdump to capture and analyze network traffic. Tcpdump is a network protocol analyzer that's accessed using the  command-line interface. Similar to Wireshark, the value of tcpdump in  cybersecurity is that it allows security analysts to capture, filter, and analyze  network traffic. |
| The 5 W's | * **● Who: N/A** * **● What: N/A** * **● Where: N/A** * **● When: N/A** * **● Why: N/A** |
| Additional notes | I'm still new to using the command-line interface, so using it to capture and  filter network traffic was a challenge. I got stuck a couple of times because I  used the wrong commands. But after carefully following the instructions and  redoing some steps, I was able to get through this activity and capture network  traffic. |