**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  10/04/2024 | **Entry:**  #1 |
| Description | * A small U.S. health care clinic experienced a security incident which severely disrupted their business operations*.* |
| Tool(s) used | none. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who**: Small group of unethical hackers who are known to target organisations in healthcare and transportation industries. * **What**: 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. * **When**: Tuesday 9:00am * **Where**: At a healthcare company * .**Why**: Because the attackers wanted a large sum of money in return for giving back access to the encrypted files. Which have caused disruption to ongoing business activities. |
| Additional notes | How can this be prevented in the future?  Is there enough employee training and awareness on phishing attacks?  How are they going to recover? |

|  |  |
| --- | --- |
| **Date:**  15/04/2024 | **Entry:**  #2 |
| Description | employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer. |
| Tool(s) used |  |
| The 5 W's | * **Domain names**: org.misecure.com is reported as a malicious contacted domain under the Relations tab in the VirusTotal report. * **IP address**: 207.148.109.242 is listed as one of many IP addresses under the Relations tab in the VirusTotal report. This IP address is also associated with the org.misecure.com domain as listed in the DNS Resolutions section under the Behavior tab from the Zenbox sandbox report. * **Hash value:** 287d612e29b71c90aa54947313810a25 is a MD5 hash listed under the Details tab in the VirusTotal report. * **Network/host artifacts**: Network-related artifacts that have been observed in this malware are HTTP requests made to the org.misecure.com domain. This is listed in the Network Communications section under the Behavior tab from the Venus Eye Sandbox and Rising MOVES sandbox reports. * **Tools**: Input capture is listed in the Collection section under the Behavior tab from the Zenbox sandbox report. Malicious actors use input capture to steal user input such as passwords, credit card numbers, and other sensitive information. * **TTPs**: Command and control is listed as a tactic under the Behavior tab from the Zenbox sandbox report. Malicious actors use command and control to establish communication channels between an infected system and their own system. |
| Additional notes | 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:**  16/04/2024. | **Entry:**  #3 |
| Description | you received a phishing alert about a suspicious file being downloaded on an employee's computer. After investigating the email attachment file's hash, the attachment has already been verified malicious. |
| Tool(s) used | none |
| The 5 W's | * **Who**: an email received from an account named “def communications” * **What**: an alert was triggered as a SERVER-MAIL phishing attempt, possible download of malware. * **When**: Wednesday, July 20, 2022 09:30:14 AM * **Where**: sent to company email * **Why**: happened because a threat actor wanted to access to the organisations files through malware contained in the downloadable attachment. |
| Additional notes | A known malicious file hash used: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b  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. |

|  |  |
| --- | --- |
| **Date:**  21/04/2024 | **Entry:**  #4 |
| Description | Phishing attack on company employees. |
| Tool(s) used | Threat actors may have utilized email spoofing tools to forge the sender's email address, making it appear as if the phishing emails were sent from a legitimate source within the company, such as the IT department. |
| The 5 W's | * **Who**: The incident was caused by unidentified threat actors who sent phishing emails to employees within the company, impersonating the IT department. This could be an external threat actor, an insider within the organization. * **What:** A suspicious email was sent out to employees from the IT department requesting urgent password resets due to a system upgrade. The emails contain a link to a login page that closely resembles the company's internal portal. Some employees clicked the link and entered their credentials before realizing the request seemed suspicious. * **When**: 9:00am * **Where**: The incident occurred within the company's email system, as employees received the phishing emails in their company email accounts. * **Why**: The incident happened because threat actors sought to gain unauthorized access to company systems and data by exploiting the trust of employees. The phishing emails were designed to deceive employees into providing their login credentials, likely with the intent of accessing sensitive information or perpetrating further attacks, such as data theft or financial fraud. |
| Additional notes | Employees should be more aware of phishing emails. Training is needed.  How where the attackers aware of the companies internal portal? |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  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.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  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.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |