**Incident handler's journal**

|  |  |
| --- | --- |
| **2024-05-06** | **Entry:**  1 |
| Description | The first case concerned a small US Health Care clinic, which was targeted with a ransomware attack. It was a twostep attack, starting with targeted phishing emails at several employees, who upon opening said emails downloaded an attachment with malicious code. This downloaded the ransomware, along with a note that notified the employees trying to access their computer on Tuesday morning about what has happened.  It severely interrupted the business operations. |
| Tool(s) used | None. |
| The 5 W's | * **Who** caused the incident? An organized group of black-hat hackers * **What** happened? A ransomware attack enabled by previous spear phishing attacks. * **When** did the incident occur? It was discovered on Tuesday morning at 9.00 AM. * **Where** did the incident happen? At the clinic’s premises * **Why** did the incident happen? The clinic was an attractive target for a ransomware attack, and the employees lack sufficient security awareness to avoid the phishing attack being successful. |
| Additional notes | Should the company pay the ransom to get an encryption key? The circumstances need to be clearer.  There should have been security training for the employees beforehand about how to recognize a phishing email and what to do about it. There should have been a backup of available data accessible. |

|  |  |
| --- | --- |
| **Date:**  2024-05-09 | **Entry:**  2 |
| Description | A financial services company. An employee had received a suspicious email with an attachment inside in the form of password protected Excel file. He downloaded it and opened it, and malicious content were downloaded onto his computer which had to be put in quarantine.  I retrieved the file and put a SHA256 hash on it to investigate its nature using crowdfunding sources. |
| Tool(s) used | VirusTotal website |
| The 5 W's | * Who? An employee at the financial services company**.** * What? The employee downloaded an unknown exe file from an email. * When? 1.13 – 1.15 pm. * Where? At the employee’s workstation. * Why? Lack of safety awareness. |
| Additional notes | The employees need to receive training and procedures set on how handle filesharing. The firewall needs to be reconfigured since the malicious payload made several http attempts. There is possibility that the network has not been set up properly from a security point of view, because an employee should not receive an executable file. |

|  |  |
| --- | --- |
| **Date:**  2024-05-11 | **Entry:**  3 |
| Description | Situation: A mid-size retail company that makes 80% of their revenues online. A vulnerability in e-commerce web application enabled a forced browsing attack, that by modifying the order number included in the URL string of a purchase confirmation page, gave an attacker access to customer data. Approximately 50 000 customer records were affected.  The attacker then contacted an employee via email and demanded ransom for not releasing this PII to the public. |
| Tool(s) used | None |
| The 5 W's | * **Who** caused the incident? A black hat attacker that detected a vulnerability in * **What** happened? A forced browsing attack enabled unauthorized access to customers PII and financial information. * **When** did the incident occur? The employee was contacted at 3.13 am on December 22, 2022. But the actual attack happened some time before that as evidenced by the associated web server logs. * **Where** did the incident happen? On the web server. * **Why** did the incident happen? A vulnerability in the e-commerce web application made it a tempting target |
| Additional notes | We recommended routine vulnerability scans and penetration testing, as well as enhanced access controls: only authorized access to authenticated users, and only to a specified set of URL: s. |

|  |  |
| --- | --- |
| **Date:**  2024-05-13 | **Entry:**  4 |
| Description | A financial services company. An employee has received a phishing email in their inbox. This suspicious domain was hidden within the email body; signin.office365x24.com. Upon investigation of that domain, it became clear that it is malicious, and links to other sites. |
| Tool(s) used | Google Chronicle |
| The 5 W's | * **Who** caused the incident? These assets were used: ashton-davidson-pc, emil-palmer-pc, warren-morris-pc * **What** happened? In total 8 assets accessed the domain listed, and of those 3 posted to that domain making it a successful phishing attempt. * **When** did the incident occur? On January 31, 2023, and then again on July 09, 2023 * **Where** did the incident happen? At the office in GB * **Why** did the incident happen? The link had a similar name to a popular service from a popular vendor. |
| Additional notes | My thoughts are that a big vendor does not usually send clickable emails to potential customers, and there is some security training needed to be done. |