| | |
|---|---|
| **Date:**<br>Record the date of the journal entry. | **Entry:**<br>04.04.24 |
| Description | A description of the AKIRA apt cyber attack on south-africa state owned bank. |
| Tool(s) used | Alien vault, Google search |
| The 5 W's | Capture the 5 W's of an incident.<br>● **Who** - An untrained employee, AKIRA ransomware group.<br>● **What** - Phishing led to ransomware<br>● **When** - 13.3.23<br>● **Where** - Pretoria, South-Africa<br>● **Why** - On the 13.3.23, 14:00, an employee from the banks pressed a link that led to a download of a malicious file to the bank's computer. Consequently, the malware infected more computers in the bank. All the computer got locked, and a ransomware message appeared on the screens. |
| Additional notes | The employee didn't go through cyber training routinely.<br>What is AKIRA.EXE:<br>https://www.sentinelone.com/blog/inside-the-mind-of-a-cyber-attacker-tactics-techniques-and-procedures-ttps-every-security-practitioner-should-know/ |