

An employee within your organization in the USA banking industry received an email with a seemingly innocent attachment from an unknown source. the file was called " AKIRA.EXE" Curious, the employee opened the attachment, which contained a malicious payload. This malware spread through the employee's computer and subsequently infected several other machines within your organization's network. What will your response be?

Date: Record the date of the journal entry.	Entry: 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. <ul style="list-style-type: none"> • Who - An untrained employee, AKIRA ransomware group. • What - Phishing led to ransomware • When - 13.3.23 • Where - Pretoria, South-Africa • 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. What is AKIRA.EXE: https://www.sentinelone.com/blog/inside-the-mind-of-a-cyber-attacker-tactics-techniques-and-procedures-tips-every-security-practitioner-should-know/