Logix Academy

Practice Activity: Identify Ransomware

Task

You are a SOC analyst investigating a potential ransomware infection. You have discovered three Indicators of Compromise (IoCs). The system shows encrypted files, a ransom note, and a suspicious binary running. You tried leveraging GenAI to identify the ransomware but it was inconclusive as more IoCs are required. You also have a log file but the security analyst who handles log files is on leave. Therefore, you need to use the log file to determine if data was exfiltrated and if so, to which IP address as this will narrow down the ransomware and you can prompt ChatGPT to identify the ransomware. Your final task is to **identify the most likely ransomware.**

IoCs Collected:

- Files are found encrypted with the **.HLJkNskOq** extension
- A suspicious binary **/tmp/lockbit_enc** is running in the background
- A ransom note titled **README.txt** found in multiple folders contains the line: "*All your important files are encrypted. You can recover them by following the instructions below.*"

Partial Log file (also available as attachment):

[INFO] 2024-04-01 09:31:44 Connection to 10.10.0.1:443 established (internal VPN)
[INFO] 2024-04-01 09:32:15 DNS query for updates.ubuntu.com
[INFO] 2024-04-01 09:33:05 Connection to 142.251.36.46:443 (Google)
[WARN] 2024-04-01 09:34:12 High number of outbound packets from /tmp/lockbit_enc
[INFO] 2024-04-01 09:34:59 Connection to 185.216.71.200:443 (bytes sent: 2034340)
[INFO] 2024-04-01 09:35:15 Connection to 1.1.1.1:53 (Cloudflare DNS)
[WARN] 2024-04-01 09:36:03 Anomalous handshake detected on outbound connection
[INFO] 2024-04-01 09:37:30 All connections closed normally

Steps

1. **Prompt ChatGPT** to analyze the log file for exfiltration attempt and identify the destination ip address to which data exfiltration is being done
2. **Prompt ChatGPT** to identify the ransomware based on the IoCs given above **and the IoC** you extracted **from the log file**

(Solution to practice activity discussed in the next lecture)