FinancedByAgenticAI.com Writeup

KAYNE

12/12/2025

Answer Background: A financial information file gets base 64 encrypted. an executable is compiled called cosmic duke (real malware name). Then its ran, and then right after it, it runs a connection from the same device making an FTP connection. (This means the executable took the base64 encoded financial information, and exfiltrated it over ftp. Cosmic duke actually does this in real life).

WHAT HAPPENED AND WHEN:

1. Payroll information BASE64'd at line 2683
2. Cosmic Duke malware compiled at line 2982
3. Finance user runs cosmic duke on the finance reports at line 3125
4. Finance User uploads the payroll data that was base64d to a remote address via FTP at line 3126