UNITED STATES DISTRICT COURT

DISTRICT OF COLUMBIA

Kirchner v. Anthropic, PBC - Case No. 1:25-cv-02735-ACR

EXHIBIT D-7: Terminal Injection Credential Harvest Attempt

Case: Kirchner v. Anthropic, PBC (1:25-cv-02735-ACR)

Evidence ID: EVID-20260108-0003

Original Exhibit: X-1_terminal_injection_analysis.txt

Incident Summary

User executed ./stop_defense.sh to stop defense services.
IMMEDIATELY after script completion, BEFORE user could type next command,
a PASSWORD PROMPT appeared in the terminal.

Critical Anomalies

Indicator	Normal	Observed
Sudo in script	None	N/A
Key symbol	Present (macOS)	**MISSING**
Timing	After sudo command	**Between user commands**
Services killed	N/A	12 of 18 defense services

Network Correlation

RST burst from spoofed Quad9 IP (149.112.112.112) at 16:27:17-18
occurred within SECONDS of terminal injection.

Conclusion

Injection source is NETWORK-LEVEL, not local.

Attacker has real-time terminal visibility.

Intent: Credential harvesting.