UNITED STATES DISTRICT COURT

DISTRICT OF COLUMBIA

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

EXHIBIT D-9: Anthropic API Direct Targeting

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

Evidence ID: EVID-20260112-0002

Original Exhibit: X-1_jan12_anthropic_targeting.txt

Attack Summary

Metric	Value
Total RSTs	14,113
Segments	90
Anthropic RSTs	47
Spoofed DNS RSTs	183

Rst Source Distribution

Source IP	Count	Identity	Status
10.157.12.231	200	Internal	Relay
9.9.9.9	110	Quad9 DNS	**SPOOFED**
136.143.189.20	82	Zoho Mail	INBOUND
149.112.112.112	73	Quad9 DNS	**SPOOFED**
160.79.104.10	**47**	**Anthropic API**	**TARGETED**

Anthropic Api Targeting

IP Address: 160.79.104.10

Service: Anthropic Claude API

RST Count: 47 packets

This proves:

1. Attacker KNOWS plaintiff uses Anthropic services
2. Attacker TARGETS Anthropic API specifically
3. Attack correlates with Claude Code usage disruption

Spoofed Dns Evidence

DNS Server	IP	RST Count	Status
Quad9 Primary	9.9.9.9	110	IMPOSSIBLE
Quad9 Secondary	149.112.112.112	73	IMPOSSIBLE
Total		**183**	**INJECTION PROOF**

DNS servers provide UDP responses, NOT TCP RST packets.

Their presence as RST sources is forensic proof of packet injection.

Verification Commands

Count Anthropic-targeted RSTs:

```
tshark -r seg_20260112_.pcapng \
-Y "tcp.flags.reset==1 and ip.addr==160.79.104.10" | wc -l
```

Expected: 47

Count spoofed DNS RSTs:

```
tshark -r seg_20260112_.pcapng \
-Y "tcp.flags.reset==1 and (ip.src==9.9.9.9 or ip.src==149.112.112.112)" | wc -l
```

Expected: 183