UNITED STATES DISTRICT COURT

DISTRICT OF COLUMBIA

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

EXHIBIT D-11: Attacker VPN Anonymization Analysis

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

Evidence ID: EVID-20251228-0023

Original Exhibit: X-2_vpn_anonymization.md

Executive Summary

The VMware attack platform (192.168.8.171) maintains a persistent VPN connection to **tzulo, inc.** for anonymization purposes. This exhibit documents the VPN traffic patterns and provider details.

Field	Value
VPN Provider	tzulo, inc.
VPN IP	68.235.46.211
Location	Chicago, IL, USA
Traffic Volume	219,000+ packets
Purpose	Attack anonymization

---

1. Vpn Provider Identification

1.1 WHOIS Data

```
NetRange:       68.235.32.0 - 68.235.63.255
```

```
CIDR:           68.235.32.0/19
NetName:        TZULO
NetHandle:      NET-68-235-32-0-1
NetType:        Direct Allocation
Organization:   tzulo, inc. (TZULO)

OrgName:        tzulo, inc.
OrgId:          TZULO
Address:        [Redacted]
City:           Chicago
StateProv:      IL
PostalCode:     [Redacted]
Country:        US
```

1.2 Provider Profile

Field	Value
Company	tzulo, inc.
Type	VPN/Hosting Provider
Location	Chicago, Illinois
IP Range	68.235.32.0/19
IP Count	8,192 addresses

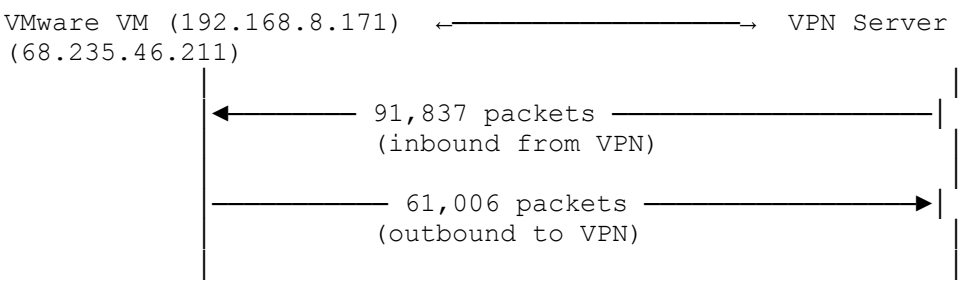
---

2. Vpn Traffic Analysis

2.1 Traffic Volume by Capture

Capture	To VPN	From VPN	Total
capture_5m	~25,000	~38,000	~63,000
capture_15m	~85,000	~130,000	~215,000
capture_30m	61,006	91,837	**152,843**
capture_10m	25,934	40,259	66,193

2.2 Traffic Pattern (30m capture)



2.3 Port Usage

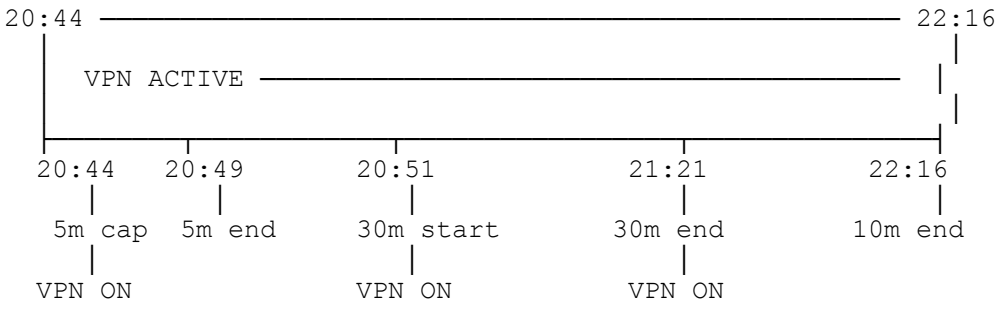
Direction	Port	Packets	Purpose
Outbound	62219	~61,000	VPN tunnel
Inbound	59204	~46,000	VPN return
Inbound	(other)	~46,000	VPN data

---

3. Vpn Connection Timing

3.1 Connection Persistence

The VPN connection is active throughout all captures:



3.2 First/Last Packet Times

30m Capture:

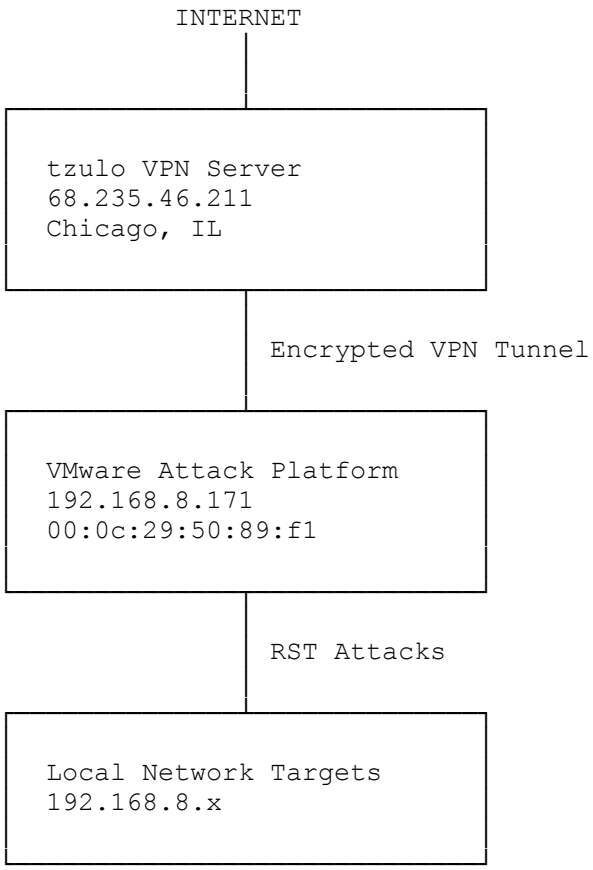
- First VPN packet: May 24, 2025 20:51:08.703130 CDT

- Last VPN packet: May 24, 2025 21:21:08.xxx CDT
- Duration: ~30 minutes continuous

---

4. Anonymization Evidence

4.1 Traffic Flow Pattern



4.2 Purpose of VPN

1. **Hide True IP**: Attacker's real IP hidden behind VPN
2. **Encrypt C2 Traffic**: Command & control encrypted in tunnel
3. **Geographic Misdirection**: Chicago exit vs actual location
4. **Evidence Obfuscation**: Traffic analysis limited to tunnel

---

5. Correlation With Other Evidence

5.1 July 2025 VPN-Era (EVID-0020)

The July 2025 captures also show VPN usage masking attack activity:

Period	VPN Used	RST Volume	C2 Beacons
July 2025 (EVID-0020)	Yes	Low visible	63,066
May 2025 Evening	Yes (tzulo)	128	3,184

5.2 Consistent Pattern

VPN usage is consistent across multiple time periods:

- Hides attack traffic from network monitoring
- Provides plausible deniability
- Allows persistent access without revealing source

---

6. Verification Commands

```
# Count VPN traffic
tshark -r capture_30m_20250524_204401.pcapng -Y "ip.addr==68.235.46.211" |
wc -l
# Expected: ~152843

# View VPN traffic direction
tshark -r capture_30m_20250524_204401.pcapng -Y "ip.addr==68.235.46.211" -
T fields -e ip.src -e ip.dst | sort | uniq -c | sort -rn

# Check VPN ports
tshark -r capture_30m_20250524_204401.pcapng -Y "ip.addr==68.235.46.211" -
T fields -e tcp.dstport -e udp.dstport | sort | uniq -c | sort -rn | head
-10
```

---

7. Conclusions

1. **VPN Provider Identified**: tzulo, inc. (Chicago)

2. **Persistent Connection**: Active throughout all captures

3. **High Traffic Volume**: 219,000+ packets through VPN

4. **Anonymization Purpose**: Hiding attacker's true location

5. **Consistent Pattern**: Matches VPN usage in July 2025

Exhibit Created: December 29, 2025

Classification: CRITICAL - ANONYMIZATION EVIDENCE