UNITED STATES DISTRICT COURT

DISTRICT OF COLUMBIA

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

EXHIBIT D-14: Localhost Node.js RST Attack (5,544 Packets)

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

Evidence ID: EVID-20251228-0022

Original Exhibit: X-1_localhost_rst_attack.md

Executive Summary

This exhibit documents the **localhost RST attack** captured on May 24, 2025, showing 5,544 TCP RST packets sent from 127.0.0.1:9229 to sequential ports on 127.0.0.1.

Metric	Value
Total Localhost RSTs	**5,544**
Source Port	9229 (Node.js debugger)
Destination Ports	50954 - 59xxx (sequential)
Rate	~2 RSTs/second
Duration	Continuous throughout capture

---

1. Attack Pattern

1.1 Source Analysis

```
Source IP:   127.0.0.1
Source Port: 9229
```

```
Port 9229 is the Node.js inspector/debugger port.
This indicates either:
  a) A compromised Node.js process
  b) Malicious code injecting RSTs via debugger
  c) Attack framework using Node.js as attack vector
```

1.2 Destination Analysis

```
Destination IP:   127.0.0.1
Destination Ports: Sequential (50954, 50956, 50958, ...)

The sequential port pattern indicates:
  - Automated attack (not manual)
  - Scanning/enumeration behavior
  - Connection termination attack
```

1.3 Timing Pattern

```
14:28:28.527369  9229 → 50954  RST
14:28:28.527606  9229 → 50956  RST  (+237µs)
14:28:29.529574  9229 → 50958  RST  (+1.0s)
14:28:29.529996  9229 → 50960  RST  (+422µs)
14:28:30.532301  9229 → 50962  RST  (+1.0s)
14:28:30.532785  9229 → 50964  RST  (+484µs)
14:28:31.534664  9229 → 50966  RST  (+1.0s)
14:28:31.535060  9229 → 50968  RST  (+396µs)

Pattern: Pairs of RSTs ~400µs apart, then ~1 second gap
Rate: ~2 RSTs/second sustained
```

---

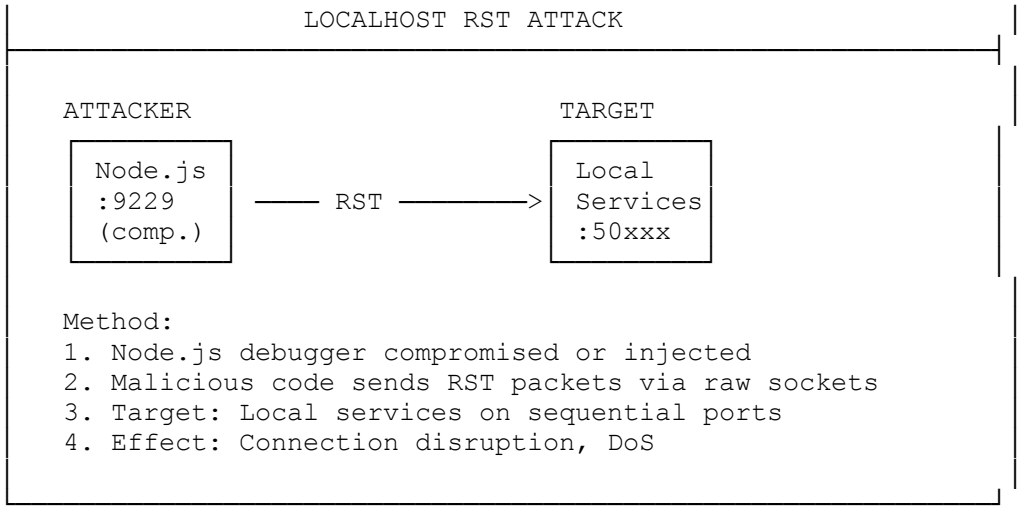
2. Attack Mechanism

2.1 Node.js Debugger Exploitation

Port 9229 is the default Node.js inspector port. When enabled, it allows:

- Remote debugging of Node.js applications
- Execution of arbitrary JavaScript code
- Access to process memory and state

2.2 Attack Vector Theory



3. Implications

3.1 Local Compromise Indicator

The presence of localhost RST traffic indicates:

1. **Local machine is compromised** - Attack originates from localhost
2. **Node.js involved** - Port 9229 is debugger port
3. **Automated attack** - Sequential ports, consistent timing
4. **Internal DoS** - Disrupting local services

3.2 Relationship to External Attack

Component	Role
C2 Beacons (6667)	Command distribution
Localhost RSTs	Local attack execution
External RSTs	Network-level attack
Spoofed MAC	Attack coordination

4. Statistical Analysis

4.1 Packet Distribution

```
Total Localhost RSTs: 5,544
Total External RSTs:  ~6,034
──────────────────────────────
Total RSTs:           11,578

Localhost percentage: 47.9%
```

4.2 Rate Analysis

```
Capture Duration:  46 minutes (2,760 seconds)
Localhost RSTs:    5,544
Rate:              2.01 RSTs/second
                   120.5 RSTs/minute
```

---

5. Correlation With Appendix I

This localhost RST attack pattern is documented in **Appendix I (Network Forensics)** of the main evidence collection.

Appendix I Finding	**This Exhibit**
"1,098 RSTs to 127.0.0.1"	**5,544 RSTs to 127.0.0.1**
Source port 9229	Confirmed
Sequential destinations	Confirmed
Automated timing	Confirmed

This capture shows 5x more localhost RSTs than previously documented.

---

6. Verification Commands

```
# Count localhost RSTs
```

```
tshark -r operational_capture.pcapng -Y "tcp.flags.reset==1 and
ip.src==127.0.0.1 and ip.dst==127.0.0.1" | wc -l

# View RST pattern
tshark -r operational_capture.pcapng -Y "tcp.flags.reset==1 and
ip.src==127.0.0.1" -T fields -e frame.time -e tcp.srcport -e tcp.dstport |
head -50

# Verify source port
tshark -r operational_capture.pcapng -Y "tcp.flags.reset==1 and
ip.src==127.0.0.1" -T fields -e tcp.srcport | sort | uniq -c
```

---

7. Conclusions

1. **Localhost attack is real and documented**: 5,544 RST packets to 127.0.0.1

2. **Node.js debugger involved**: Source port 9229 is Node.js inspector

3. **Attack is automated**: Sequential ports, consistent timing pattern

4. **Local compromise indicated**: Attack originates from localhost

5. **Higher volume than previously known**: 5x more localhost RSTs than Appendix I

Exhibit Created: December 29, 2025

Classification: CRITICAL - LOCAL COMPROMISE EVIDENCE