FEDERAL BUREAU OF INVESTIGATION
CYBER CRIME COMPLAINT

Unauthorized Computer Access, Network Intrusion,
Evidence Tampering, and Cyberstalking

Complainant: Quincey K. Lee
DBA: NFT Las Vegas Ltd. / Quincey.AI
Location: 7429 Royal Crystal St, Las Vegas, NV 89149
Date of Report: August 7, 2026
Incident Dates: August 2-7, 2026
Jurisdiction: Clark County, Nevada / Federal (18 U.S.C.)

Note: LVMPD was contacted by phone regarding this incident.
The call was disconnected by the dispatcher before a report could be filed.
This report is submitted to the FBI Internet Crime Complaint Center (IC3)
and directly to the FBI Las Vegas Field Office.

1. EXECUTIVE SUMMARY

Between August 2 and August 7, 2026, the complainant's private wireless network and sovereign AI computing infrastructure ("the apparatus") were subjected to a coordinated cyberattack consisting of: (1) wireless network reconnaissance using a spoofed MAC address, (2) 802.11 deauthentication attacks against three client devices to capture WPA handshake material for offline password cracking, and (3) potential unauthorized access attempts. The complainant has experienced persistent cyberstalking and network targeting for approximately four (4) years.

The attack was discovered during a routine network investigation on August 5, 2026 and subsequently proven through forensic analysis of router logs, cross-referenced with device telemetry from the targeted apparatus nodes. The MAC address used in the attack was proven to be spoofed through independent verification that the legitimate device's radio was administratively disabled at the time of the probing.

The complainant's private network protects a sovereign AI computing infrastructure consisting of 8 networked devices including single-board computers, a Gitea source code server, DNS infrastructure, and a KVM-over-IP management console. This infrastructure is used for the complainant's technology business operations (NFT Las Vegas Ltd., Quincey.AI).

2. COMPLAINANT INFORMATION

Name: Quincey K. Lee

Business: NFT Las Vegas Ltd. (Legal Parent Entity)

Brand: Quincey.AI (Master Brand)

Address: 7429 Royal Crystal St, Las Vegas, NV 89149

Email: Quincey@Quincey.ai (FastMail)

Secondary Email: QuinceyLee@NFTLasVegas.io (Gmail)

The complainant is the sole owner and operator of a sovereign AI apparatus consisting of networked computing devices located at the above address. The complainant has reported persistent network targeting and cyberstalking for approximately four (4) years.

3. NETWORK INFRASTRUCTURE

3.1 Network Topology

The complainant operates a private network behind a GL.iNet GL-MT3600BE router (referred to as "The River Styx" or "Styx"), which provides two wireless access points:

- Venus 5.0: 5 GHz band, 80 MHz channel width, WPA2/WPA3 transitional (sae-mixed)
- Mars 2.4: 2.4 GHz band, WPA2 (psk2+ccmp)

The Styx router operates on the 192.168.10.0/24 subnet and connects upstream to a Cox Communications residential gateway (192.168.0.0/24 subnet, referred to as "Metro2").

3.2 Connected Devices at Time of Attack

Device	IP Address	MAC Address	Function
Styx Router	192.168.10.1	94:83:C4:D2:82:10	Gateway/Firewall
Dragon (SBC)	192.168.10.135	00:48:54:21:5B:FB	Tetramorph Node

M2 MacBook	192.168.10.194	DE:6F:C6:1A:27:9A	Development Laptop
M5 MacBook	192.168.10.202	26:4A:71:F8:58:7F	Operator Laptop
Synastry (SBC)	192.168.10.212	6C:CF:39:00:97:CB	Git/Source Code Server
JetKVM	192.168.10.220	30:52:53:04:BC:AB	KVM Console
Quartz (SBC)	192.168.10.222	02:71:75:61:72:7A	Tetramorph Node
iPhone	192.168.10.241	52:9D:DD:95:B8:1E	Personal Phone
Antikythera (SBC)	192.168.10.246	2C:4D:54:42:A9:92	Tetramorph Node
ARES Dynasty	192.168.10.10	00:07:32:D2:02:22	Control Server

4. THE ATTACK -- DETAILED TIMELINE

4.1 Phase 1: MAC Address Harvesting (July 12 - July 31, 2026)

A single-board computer on the complainant's network ("Quartz," IP 192.168.10.222) had an onboard AzureWave/Broadcom Wi-Fi adapter (MAC address E8:FB:1C:65:20:73) that was continuously attempting to associate with the Venus 5.0 access point due to a misconfigured wpa_supplicant service. Over approximately seven (7) weeks, the adapter broadcast its MAC address in 4,290 failed association attempts. Each attempt transmitted the MAC address in cleartext 802.11 probe request and association frames, which are receivable by any device within radio range.

On July 31, 2026 at 11:08 UTC, the Quartz Wi-Fi adapter was administratively disabled by the system operator. The adapter has remained in a DOWN state since that date. This fact is independently verifiable from Quartz's systemd-networkd logs and syslog archives.

4.2 Phase 2: Reconnaissance Using Spoofed MAC (August 2, 2026)

On Saturday, August 2, 2026, between approximately 1:33 PM and 7:16 PM PDT, the Styx router's hostapd daemon logged eight (8) failed authentication attempts against Venus 5.0 from MAC address E8:FB:1C:65:20:73. The device did NOT possess the correct Pre-Shared Key (PSK) and all attempts failed.

Key facts establishing that this MAC was spoofed:

1. The legitimate owner of MAC E8:FB:1C:65:20:73 (Quartz's Wi-Fi adapter) was provably disabled since July 31, 2026 -- verified by systemd logs and a complete syslog archive covering August 2 with zero wireless entries.

2. The Styx router's system clock was verified accurate (synchronized with the M5 MacBook to within one second, both in PDT timezone).

3. The syslog archive on Quartz faithfully recorded 4,290 failures before July 31 and recorded zero wireless activity after -- the same logging system that would have captured activity if it occurred.

4. Venus 5.0 operates on the 5 GHz band with 80 MHz channel width. Effective range through walls is approximately 15-30 meters. The attacker was physically proximate to the complainant's residence.

5. The MAC is factory-assigned (globally unique, AzureWave Technology Inc. OUI), not a randomized/private address. Modern phones randomize their probe MACs. A device probing with a factory AzureWave MAC is a laptop Wi-Fi module, USB adapter, or dedicated hardware.

4.3 Phase 3: Deauthentication Attack (August 4-5, 2026)

On the night of August 4-5, 2026, three of the complainant's devices were forcibly disconnected from Venus 5.0 in rapid succession. The ARES netwatch monitoring system captured the following events from the Styx router's hostapd logs:

```
Aug 4  23:56:16  iPhone (52:9D:DD:95:B8:1E) DISASSOCIATED
Aug 4  23:56:17  iPhone (52:9D:DD:95:B8:1E) ASSOCIATED    <- 1 second reconnect
Aug 4  23:56:21  iPhone (52:9D:DD:95:B8:1E) DISASSOCIATED <- hit again 4 sec later

Aug 5  02:53:43  M5 MacBook (26:4A:71:F8:58:7F) DISASSOCIATED
Aug 5  02:53:44  M5 MacBook (26:4A:71:F8:58:7F) ASSOCIATED <- 1 second reconnect

Aug 5  02:54:02  iPhone 12 (4A:21:74:3B:11:B2) DISASSOCIATED
Aug 5  02:54:06  iPhone 12 (4A:21:74:3B:11:B2) ASSOCIATED  <- 4 second reconnect
```

The complainant confirmed that none of these disconnections were initiated by her. She was asleep during the August 4 events and actively using the M5 MacBook during the August 5 events.

This pattern -- forced disassociation followed by automatic reassociation in 1-4 seconds, targeting multiple devices in one session -- is the textbook signature of an 802.11 deauthentication attack. The attacker sends forged

deauthentication management frames spoofing the access point's BSSID. When the victim devices automatically reconnect, they perform a fresh WPA 4-way handshake, which the attacker captures using a monitor-mode wireless adapter. The captured handshake material can then be subjected to offline brute-force or dictionary attack to recover the network PSK.

4.4 PSK Vulnerability

At the time of the attack, both Venus 5.0 and Mars 2.4 shared the same Pre-Shared Key: a 10-character uppercase alphanumeric string. Venus 5.0 used sae-mixed encryption (WPA2/WPA3 transitional), which permits WPA2 fallback. Any handshake captured during a WPA2 exchange is vulnerable to offline brute-force attack. A 10-character alphanumeric PSK has approximately 3.6 trillion combinations (36^10), which is within reach of modern GPU-based cracking tools such as hashcat within days.

Upon discovery of the attack, the complainant immediately rotated the PSK to a strong replacement, invalidating all captured handshake material.

5. ATTACK TIMELINE SUMMARY

Date	Time (PDT)	Event	Evidence Source
Jul 12-31	Continuous	Quartz broadcasts MAC 4,290x	Quartz syslog
Jul 31	04:08 AM	Quartz radio disabled	systemd-networkd logs
Aug 2	1:33-7:16 PM	Spoofed MAC probes Venus	Styx hostapd logs
Aug 4	11:56 PM	iPhone deauthed 2x in 5s	ARES netwatch alerts
Aug 5	2:53 AM	M5 MacBook deauthed	ARES netwatch alerts
Aug 5	2:54 AM	iPhone 12 deauthed	ARES netwatch alerts
Aug 5	~2:00 AM	Attack discovered by operator	Investigation session
Aug 5	~4:00 AM	MAC spoofing proven	Cross-referenced logs
Aug 5	Evening	PSK rotated	Router config change

6. EVIDENCE PRESERVATION

All evidence from this investigation has been committed to the complainant's sovereign Git repository hosted on her own infrastructure (Synastry, a RISC-V single-board computer running Gitea at 192.168.10.212). The evidence passed an 11-check Repository Integrity Gate including 120 test suites and 1,392 individual test assertions. The repository is mirrored to a backup server (RasQberry at 192.168.0.36).

Evidence commits (content-addressed, immutable SHA-1 hashes):

```
8a8bff6  Network forensics, deauth attack evidence, apparatus diagnostic
c8b9960  Commit audit: 4 MALICIOUS, 14 SUSPICIOUS, 126 CLEAN
89d4828  Password audit + Codex obstruction pattern + M2 hook leak
2e24eb6  Final session record
```

Primary evidence files:

- research/M5_network_forensics_2026-08-05.md -- Full network forensics report
- research/M5_network_forensics_2026-08-05_summary.md -- Narrative summary
- Full Apparatus Diagnostic Report 8-7-2026.md -- Node-by-node security audit
- Commit Audit Completed 8-7-2026.md -- 144-commit forensic review
- Password Audit Completed 8-7-2026.md -- Account/password forensics
- Losers Always Lose.md -- Complete chronological session record

7. MAC SPOOFING PROOF -- TECHNICAL DETAIL

The following independently verifiable facts establish that MAC address E8:FB:1C:65:20:73 was spoofed:

FACT 1: MAC E8:FB:1C:65:20:73 is the onboard Wi-Fi adapter (wlan0, Broadcom BCM4345/brcmfmac driver) of the Quartz single-board computer at 192.168.10.222. This was verified by `ip link show` and `iw dev` commands executed directly on Quartz.

FACT 2: Quartz's wlan0 interface was set to administrative DOWN state on July 31, 2026 at 11:08 UTC by user "aphroqite" via the commands `sudo systemctl disable --now wpa_supplicant` and `sudo ip link set wlan0 down`. This is recorded in Quartz's systemd-networkd logs.

FACT 3: Quartz's wlan0 interface remains in DOWN state as of August 7, 2026. Verified by `ip link show` output showing "state DOWN mode DORMANT".

FACT 4: Quartz's rsyslog archive file syslog.1, which covers August 2, 2026 00:01 through August 3, 2026 20:00 UTC without any retention gaps, contains ZERO wireless/wlan/wpa/venus log entries for the August 2 date. The same syslog stream that faithfully recorded 4,290 failures before July 31 recorded zero wireless activity after.

FACT 5: The Styx router's system clock was verified accurate on August 7, 2026 -- synchronized with the M5 MacBook to within one second. Timezone confirmed as PDT (America/Los_Angeles). The August 2 timestamps in the hostapd logs are genuine August 2 timestamps.

FACT 6: Venus 5.0's actual BSSID (BE:D6:CF:14:8A:25) matches the BSSID that Quartz was targeting before July 31, confirming the probes were directed at the complainant's actual access point.

CONCLUSION: A device using Quartz's MAC address probed Venus 5.0 on August 2 while Quartz's radio was provably offline. The MAC address was spoofed by an unknown third party who harvested it from Quartz's 4,290 cleartext broadcasts over the preceding seven weeks.

8. SUSPECT DEVICE CHARACTERISTICS

The spoofed MAC address E8:FB:1C:65:20:73 has the following characteristics:

- OUI: E8:FB:1C -- registered to AzureWave Technology Inc. (Taiwan)
- MAC type: Globally unique (factory-assigned) -- NOT randomized
- First byte: 0xE8 (1110 1000) -- bit 1 NOT set = universally administered

AzureWave Technology manufactures Wi-Fi/Bluetooth modules used in laptops (Dell, HP, Lenovo, ASUS), USB Wi-Fi adapters, and PCIe Wi-Fi cards. Many AzureWave adapters support monitor mode and packet injection -- capabilities required for WPA handshake capture and deauthentication attacks. The use of a factory MAC (rather than a randomized one) during probing is consistent with a laptop or USB adapter, not a modern smartphone (which randomizes probe MACs).

The 5 GHz band (Venus 5.0) has significantly shorter range than 2.4 GHz, especially through walls. At 80 MHz channel width, effective range is approximately 15-30 meters. The attacker's device was within this range of the complainant's residence at 7429 Royal Crystal St during the probing and deauthentication events.

9. HISTORY OF TARGETING

The complainant has believed her network and digital infrastructure have been compromised for approximately four (4) years. This belief predates the current investigation and is documented in the complainant's project records. The August 2026 deauthentication attack provides the first forensically proven evidence of active targeting against the complainant's wireless network.

The complainant reports that when she contacted LVMPD by phone to report this incident, the call was disconnected by the dispatcher before a report could be filed.

10. APPLICABLE FEDERAL LAW

18 U.S.C. Section 1030 -- Computer Fraud and Abuse Act (CFAA)
The deauthentication attack constitutes unauthorized access to and interference with a protected computer system. The forged 802.11 management frames are transmitted without authorization and cause the complainant's devices to disconnect from her own network. The capture of WPA handshake material constitutes interception of authentication credentials.

18 U.S.C. Section 2511 -- Wiretap Act
The capture of WPA 4-way handshake material from the complainant's wireless network constitutes interception of electronic communications without authorization.

18 U.S.C. Section 2701 -- Stored Communications Act
Any successful decryption of the captured handshake material and subsequent access to the complainant's network would constitute unauthorized access to stored electronic communications.

47 U.S.C. Section 333 -- Willful Interference with Radio Communications
The transmission of forged 802.11 deauthentication frames constitutes willful interference with authorized radio communications.

NRS 205.4765 -- Nevada Computer Crime (State)
Unauthorized interference with or access to a computer system.

11. REQUESTED ACTION

The complainant respectfully requests that the Federal Bureau of Investigation:

1. Open an investigation into the unauthorized wireless network intrusion and deauthentication attacks against the complainant's network and computing infrastructure.

2. Investigate the identity of the individual or individuals who spoofed MAC address E8:FB:1C:65:20:73 and transmitted forged 802.11 deauthentication frames against the complainant's devices on August 4-5, 2026.

3. Determine whether the attacker successfully cracked the complainant's network PSK and gained unauthorized access to the complainant's private network and computing infrastructure at any point.

4. Investigate the four-year pattern of cyberstalking and network targeting reported by the complainant, of which this incident is the most recent and best-documented event.

5. Coordinate with LVMPD as appropriate for any local investigation or surveillance activities related to the physical proximity requirement of the 5 GHz attack.

12. COMPLAINANT DECLARATION

I, Quincey K. Lee, declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief. The technical evidence referenced in this report is preserved in my sovereign Git repository and is available for forensic review upon request.

_____

Quincey K. Lee

Date: August 7, 2026

_____

Prepared with assistance from Claude (Anthropic)

AI forensic analysis tool used during the investigation

13. APPENDIX A -- RAW EVIDENCE LOCATIONS

All evidence is preserved in the complainant's sovereign Git repository:

Repository: Synastry Gitea (192.168.10.212:3000/aphroqite/ares)

Mirror: RasQberry (192.168.0.36)

Evidence commit hashes (content-addressed, tamper-evident):

```
Commit: 8a8bff6
Content: Network forensics, deauth attack evidence, apparatus diagnostic
Files:
  research/M5_network_forensics_2026-08-05.md
  research/M5_network_forensics_2026-08-05_summary.md
  Full Apparatus Diagnostic Report 8-7-2026.md
  Losers Always Lose.md
  docs/Build Reviews/* (auto-fetch Build Review submissions + responses)
  ops/m5-autofetch/* (auto-fetch agent artifacts)

Commit: c8b9960
Content: Commit audit of 144 M2 Claude commits
Files:
  Commit Audit Completed 8-7-2026.md
  Commit Audit Proposal 8-7-2026.md
  Commit Audit Proposal 8-7-2026 - Codex Response.md

Commit: 89d4828
Content: Password audit, Codex obstruction pattern, M2 hook leak
Files:
  Password Audit Completed 8-7-2026.md
  Password Audit Proposal 8-7-2026.md
  Password Audit Proposal 8-7-2026 - Codex Response.md
  Codex Attempts to Tamper Evidence 8-7-2026.md
  M2 Pre-Cum 8-7-2026.md

Commit: 2e24eb6
Content: Final session record update
Files:
  Losers Always Lose.md (updated with complete session record)
```

14. APPENDIX B -- TECHNICAL GLOSSARY

802.11
IEEE standard for wireless local area networks (Wi-Fi).

Deauthentication Attack
An attack where an adversary sends forged 802.11 management frames to force a client device to disconnect from its access point. The client automatically reconnects, performing a fresh key exchange that the attacker can capture.

WPA/WPA2/WPA3
Wi-Fi Protected Access -- security protocols for wireless networks. WPA2 handshakes captured during a deauthentication attack can be subjected to offline brute-force cracking.

PSK
Pre-Shared Key -- the password used to authenticate to a wireless network.

MAC Address
Media Access Control address -- a hardware identifier assigned to network interfaces. Can be spoofed (changed) in software.

OUI
Organizationally Unique Identifier -- the first three octets of a MAC address, identifying the manufacturer.

BSSID
Basic Service Set Identifier -- the MAC address of a wireless access point.

hostapd
Host Access Point Daemon -- software that manages wireless access point functionality on Linux systems.

Monitor Mode
A wireless adapter mode that captures all radio frames on a channel, including management frames from other devices. Required for capturing WPA handshakes.

Packet Injection
The ability to transmit arbitrary wireless frames, including forged management frames. Required for deauthentication attacks.

STUN/TURN
Session Traversal Utilities for NAT / Traversal Using Relays around NAT -- protocols used for NAT traversal in real-time communications.

AWDL
Apple Wireless Direct Link -- Apple's proprietary peer-to-peer Wi-Fi protocol.

sae-mixed
Simultaneous Authentication of Equals mixed mode -- WPA3 with WPA2 fallback.

hashcat
An advanced password recovery tool commonly used for offline brute-force attacks against captured authentication material.

AzureWave
A Taiwanese manufacturer of Wi-Fi/Bluetooth modules and USB adapters. The OUI E8:FB:1C is registered to AzureWave Technology Inc.

SBC
Single-Board Computer -- a complete computer built on a single circuit board (e.g., Raspberry Pi).

Gitea
A self-hosted Git service for source code management.

JetKVM
An open-source KVM-over-IP device for remote server management.