Professional WiFi Security Assessment Report

Report Generated:	2025-09-03 02:04:50 UTC
Network Name:	Oneplus
Scan Timestamp:	2025-09-03T01:46:39.440Z

Executive Summary

Overall Status:	Botnet Activity
Confidence Level:	0.0%
Risk Level:	Minimal
Risk Score:	0
Models Analyzed:	8

Key Findings:

- Potential security concern detected: BOTNET ACTIVITY
- Low confidence in predictions - manual review recommended

Network Configuration Analysis

Ssid:	Oneplus
Encryption:	WPA3-Personal
Signal Strength:	-30 dBm
Channel:	11
Frequency:	2462 MHz
Mac Address:	ca:48:92:f4:cc:ef
Ip Address:	10.19.156.103
Gateway:	10.19.156.164
Dns Servers:	10.19.156.164
Data Rate:	72.2 Mbps
Radio Type:	802.11n

Security Assessment:

Encryption Strength: Excellent (WPA3 - Latest Standard)

Signal Quality: Excellent (-30 dBm or higher)

Channel Congestion: Standard 2.4GHz non-overlapping channel (Good choice)

AI Model Analysis

Ensemble Model Results:

Final Prediction:	BOTNET ACTIVITY
Confidence:	0.0%
Models Used:	8
Agreement Score:	100.0%
Fusion Method:	Weighted Average with Confidence Scoring

Individual Model Results:

Model Name	Prediction	Confidence	Type
Cnn	SECURE NETWORK	19.6%	Convolutional Neural Network (CNN) - Pattern Rec
Cnn Lstm Hybrid	SECURE NETWORK	23.0%	Convolutional Neural Network (CNN) - Pattern Rec
Gnn	SECURE NETWORK	22.0%	Graph Neural Network (GNN) - Network Topology
Gradient Boosting	SECURE NETWORK	18.7%	Gradient Boosting - Advanced Ensemble Learning
Lstm	SECURE NETWORK	23.2%	Long Short-Term Memory (LSTM) - Temporal Anal
Lstm Main	SECURE NETWORK	23.2%	Long Short-Term Memory (LSTM) - Temporal Anal
Lstm Production	SECURE NETWORK	14.7%	Long Short-Term Memory (LSTM) - Temporal Anal
Random Forest	SECURE NETWORK	11.4%	Random Forest - Ensemble Decision Trees

Threat Analysis

Risk Level:	Unknown

Security Recommendations

Ongoing Monitoring:

• **ONGOING:** Enable automatic security updates on all connected devices.

Reason: Ongoing security monitoring

• **ONGOING:** Regularly change WiFi passwords and use strong, unique passwords.

Reason: Ongoing security monitoring

• **ONGOING:** Consider enabling guest network for visitors to isolate main network.

Reason: Ongoing security monitoring

• **ONGOING:** Schedule regular automated security scans

Reason: Continuous monitoring for emerging threats

• **QUARTERLY:** Review and update network access credentials quarterly

Reason: Regular credential rotation reduces long-term exposure risk

WiFi Network Input Features (32 Features)

Raw Network Data Captured:

Network SSID:	Oneplus
MAC Address (BSSID):	ca:48:92:f4:cc:ef
Signal Strength (RSSI):	-30 dBm
WiFi Channel:	11
Operating Frequency:	2462 MHz
Encryption Type:	WPA3-Personal
Authentication Method:	WPA3-Personal
Connection Speed:	72.2 Mbps
Radio Type:	802.11n
Device IP Address:	10.19.156.103
Network Gateway:	10.19.156.164
DNS Servers:	10.19.156.164
Link Quality:	100%

AI Model Input Features (32 Features):

Signal Intelligence Features (0-7)

0. Signal Strength Normalized: RSSI normalized to 0-1 range

1. Signal Quality: Signal quality percentage normalized

2. SNR Normalized: Signal-to-Noise ratio normalized

3. Signal Stability: Signal stability score 0-1

4. Frequency Band: 0=2.4GHz, 0.5=5GHz, 1=6GHz

5. Channel Congestion: Channel utilization 0-1

6. Interference Level: Interference level 0-1

7. Beacon Interval Normalized: Beacon interval normalized

Packet Analysis Features (8-15)

8. Encryption Strength: 0=Open, 0.25=WEP, 0.5=WPA, 0.75=WPA2, 1=WPA3

9. Cipher Suite Score: Cipher strength score 0-1

10. Authentication Method: Auth method score 0-1

11. WPS Vulnerability: 1 if WPS enabled, 0 otherwise

12. PMF Enabled: 1 if PMF enabled, 0 otherwise

13. Enterprise Features: Enterprise security features 0-1

14. Protocol Version: 802.11 version normalized

15. Max Data Rate Normalized: Maximum data rate normalized

Network Protocol Features (16-23)

16. Vendor Trust Score: Vendor trust score 0-1
17. Device Type Score: Device type risk score 0-1
18. SSID Entropy: SSID randomness score 0-1
19. SSID Suspicious Keywords: Suspicious SSID keywords 0-1
20. BSSID OUI Known: Known OUI indicator 0-1
21. Capabilities Count: Number of capabilities normalized
22. Hidden Network: 1 if hidden, 0 otherwise
23. Country Code Match: Country code consistency 0-1

Traffic Pattern Features (24-31)

24. Network Age: How long network has been seen 0-1
25. Signal Trend: 0=degrading, 0.5=stable, 1=improving
26. Connection Attempts: Connection attempt patterns 0-1
27. Bandwidth Capacity: Network capacity estimate 0-1
28. Load Estimate: Current network load 0-1
29. Geographic Anomaly: Geographic inconsistency 0-1
30. Time Pattern Anomaly: Unusual time patterns 0-1
31. Duplicate Detection: Evil twin / duplicate detection 0-1

Feature Extraction Summary:

Total Input Features:	32 normalized features
Feature Engineering:	Real-time extraction from live WiFi data
Normalization Method:	Min-max scaling to 0-1 range
Data Types:	Float32 arrays for AI model compatibility
Feature Categories:	4 categories covering signal, security, protocol, and behavior
Update Frequency:	Real-time during network scanning
Missing Value Handling:	Default values based on network type
Quality Assurance:	Automated validation and bounds checking

Technical Details

Models Analyzed:	8