AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-16 19:42:02 (EDT - America/New_York) | 2026-07-16 23:42:02 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 7 bytes
IOCs Found: 1
ATT&CK Techniques: 0

Severity

Low

Confidence

10% - Very Low Confidence

Confidence Factors

None

Reducing Factors

• AbuseIPDB abuse confidence score is 0 despite multiple reports
• VirusTotal shows 0 malicious or suspicious detections for IP 8.8.8.8
• IP belongs to Google LLC and is used as a Content Delivery Network

Threat Type

Insufficient Evidence

Executive Summary

The IP address 8.8.8.8 is a well-known Google public DNS server with no current malicious detections or suspicious activity. Despite multiple reports in AbuseIPDB, the abuse confidence score is zero and VirusTotal analysis indicates the IP is harmless.

Evidence Supporting Assessment

• AbuseIPDB reports 121 total reports for IP 8.8.8.8 but abuse confidence score is 0
• VirusTotal analysis shows 0 malicious and 0 suspicious detections out of 91 total scans
• IP 8.8.8.8 is registered to Google LLC and classified as Content Delivery Network

Ambiguity Notes

• Multiple reports exist in AbuseIPDB but no confirmed malicious activity or abuse confidence
• No file or behavioral evidence provided to support malicious activity
• No decoded Base64 or PE file content to analyze

Alternative Hypotheses

• Benign use of a public Google DNS server
• False positive or mistaken reports in AbuseIPDB
• Misinterpretation of network traffic involving this IP

Alternative Explanations

• Normal network activity to a widely used public DNS resolver
• Reports may be related to unrelated network events or user errors

Indicators of Compromise

IP Addresses
- 8.8.8.8

MITRE ATT&CK Mapping

None

Recommended Actions

• Verify the context in which IP 8.8.8.8 was observed to rule out misinterpretation
• Monitor network traffic involving 8.8.8.8 for any unusual or unexpected behavior
• Confirm that no internal systems are misconfigured to misuse this IP address

Analyst Notes

None

AI-Assisted Analysis Disclaimer

This report was generated using AI-assisted analysis and is intended to support security investigations. Findings, conclusions, and recommendations should be reviewed and validated by a qualified analyst before operational, legal, or business decisions are made.

