AI-Assisted Investigation Report

Analyst

MalwareLab User

Analysis Time

2026-07-16 19:40:35 (EDT - America/New_York) | 2026-07-16 23:40:35 UTC

Model

gpt-4.1-mini

Version

beta-v2.0

Report Metrics

Input Size: 13 bytes
IOCs Found: 1
ATT&CK Techniques: 0

Severity

High

Confidence

90% - High Confidence

Confidence Factors

• AbuseIPDB reports 100 abuse confidence score with 167 total reports for IP 185.220.101.1
• VirusTotal shows 14 malicious and 2 suspicious detections for IP 185.220.101.1

Reducing Factors

None

© 2026 MalwareLab.ai

Threat Type

Malicious Infrastructure

Executive Summary

The IP address 185.220.101.1 is strongly associated with malicious activity based on high abuse confidence from AbuseIPDB and multiple malicious detections on VirusTotal.

Evidence Supporting Assessment

• AbuseIPDB reports 100% abuse confidence score for IP 185.220.101.1 with 167 abuse reports
• VirusTotal reputation score of -22 with 14 malicious and 2 suspicious detections out of 91 total scans
• IP is registered to ISP 'Artikel10 e.V.' and AS owner 'Stiftung Erneuerbare Freiheit' in Germany

Ambiguity Notes

• No direct evidence of specific attack types or campaigns associated with this IP in the provided data
• No file or executable artifacts linked to this IP to further characterize threat behavior

Alternative Hypotheses

• The IP could be part of a compromised or hijacked network used for malicious activity
• The IP may be used by a proxy or VPN service that is abused by attackers
• Possible false positive due to misattribution or outdated reports

Alternative Explanations

• The IP is a commercial ISP address that may host legitimate services alongside malicious actors
• Reports may reflect past abuse that has since been mitigated

Indicators of Compromise

IP Addresses
- 185.220.101.1

MITRE ATT&CK Mapping

None

Recommended Actions

• Block or monitor network traffic to and from IP 185.220.101.1
• Investigate any connections or communications involving this IP in network logs

 © 2026 MalwareLab.ai

Recommended Actions — continued

• Correlate with endpoint telemetry for potential indicators of compromise
• Review firewall and IDS/IPS alerts related to this IP
• Consider threat intelligence updates for emerging activity linked to this IP

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.

MalwareLab.ai
AI-Assisted Investigation Platform

 © 2026 MalwareLab.ai