Alien Security

Security Intelligence & Threat Analysis Platform

IP Intel Pro Analysis Report

Comprehensive Analysis from Multiple Sources

Generated: Tuesday, December 16, 2025 at 05:27:59 PM

VirusTotal Analysis

IP ADDRESS: 172.16.0.1	
Community Score	**0/98** security vendors flagged this as malicious
Last Analysis Date	Tue Dec 9 20:39:43 2025
Reputation	0
Times Submitted	152
Last Final URL	http://172.16.0.1/
Last Analysis Stats	Malicious: 0, Suspicious: 0, Harmless: 67, Undetected: 31
VirusTotal Report	View Full Report

ENGINE NAME	CATEGORY	RESULT	METHOD
Criminal IP	undetected	unrated	blacklist
alphaMountain.ai	undetected	unrated	blacklist
ArcSight Threat Intelligence	undetected	unrated	blacklist
AutoShun	undetected	unrated	blacklist
Axur	undetected	unrated	blacklist
Bfore.Ai PreCrime	undetected	unrated	blacklist
Bkav	undetected	unrated	blacklist
ChainPatrol	undetected	unrated	blacklist
Cluster25	undetected	unrated	blacklist
CSIS Security Group	undetected	unrated	blacklist
Cyan	undetected	unrated	blacklist
Ermes	undetected	unrated	blacklist
GCP Abuse Intelligence	undetected	unrated	blacklist
Gridinsoft	undetected	unrated	blacklist
Hunt.io Intelligence	undetected	unrated	blacklist

ENGINE NAME	CATEGORY	RESULT	METHOD
Kaspersky	undetected	unrated	blacklist
Lumu	undetected	unrated	blacklist
MalwareURL	undetected	unrated	blacklist
Mimecast	undetected	unrated	blacklist
Netcraft	undetected	unrated	blacklist
0xSI_f33d	undetected	unrated	blacklist
PhishFort	undetected	unrated	blacklist
PhishLabs	undetected	unrated	blacklist
PrecisionSec	undetected	unrated	blacklist
SafeToOpen	undetected	unrated	blacklist
Sansec eComscan	undetected	unrated	blacklist
SOCRadar	undetected	unrated	blacklist
Underworld	undetected	unrated	blacklist
URLQuery	undetected	unrated	blacklist
VIPRE	undetected	unrated	blacklist
ZeroFox	undetected	unrated	blacklist
Artists Against 419	harmless	clean	blacklist
Acronis	harmless	clean	blacklist
Abusix	harmless	clean	blacklist
ADMINUSLabs	harmless	clean	blacklist
Lionic	harmless	clean	blacklist
AILabs (MONITORAPP)	harmless	clean	blacklist
AlienVault	harmless	clean	blacklist
AlphaSOC	harmless	clean	blacklist
Antiy-AVL	harmless	clean	blacklist
benkow.cc	harmless	clean	blacklist
BitDefender	harmless	clean	blacklist
BlockList	harmless	clean	blacklist
Blueliv	harmless	clean	blacklist
Certego	harmless	clean	blacklist
Chong Lua Dao	harmless	clean	blacklist
CINS Army	harmless	clean	blacklist
Snort IP sample list	harmless	clean	blacklist
CMC Threat Intelligence	harmless	clean	blacklist
Xcitium Verdict Cloud	harmless	clean	blacklist

ENGINE NAME	CATEGORY	RESULT	METHOD
CRDF	harmless	clean	blacklist
Cyble	harmless	clean	blacklist
CyRadar	harmless	clean	blacklist
desenmascara.me	harmless	clean	blacklist
DNS8	harmless	clean	blacklist
Dr.Web	harmless	clean	blacklist
Emsisoft	harmless	clean	blacklist
ESET	harmless	clean	blacklist
ESTsecurity	harmless	clean	blacklist
EmergingThreats	harmless	clean	blacklist
Feodo Tracker	harmless	clean	blacklist
Fortinet	harmless	clean	blacklist
G-Data	harmless	clean	blacklist
Google Safebrowsing	harmless	clean	blacklist
GreenSnow	harmless	clean	blacklist
Heimdal Security	harmless	clean	blacklist
IPsum	harmless	clean	blacklist
Juniper Networks	harmless	clean	blacklist
Malwared	harmless	clean	blacklist
MalwarePatrol	harmless	clean	blacklist
malwares.com URL checker	harmless	clean	blacklist
OpenPhish	harmless	clean	blacklist
Phishing Database	harmless	clean	blacklist
Phishtank	harmless	clean	blacklist
PREBYTES	harmless	clean	blacklist
Quick Heal	harmless	clean	blacklist
Quttera	harmless	clean	blacklist
Rising	harmless	clean	blacklist
Sangfor	harmless	clean	blacklist
Scantitan	harmless	clean	blacklist
SCUMWARE.org	harmless	clean	blacklist
Seclookup	harmless	clean	blacklist
Sophos	harmless	clean	blacklist
Spam404	harmless	clean	blacklist
StopForumSpam	harmless	clean	blacklist
Sucuri SiteCheck	harmless	clean	blacklist

ENGINE NAME	CATEGORY	RESULT	METHOD
securolytics	harmless	clean	blacklist
Threatsourcing	harmless	clean	blacklist
ThreatHive	harmless	clean	blacklist
Trustwave	harmless	clean	blacklist
URLhaus	harmless	clean	blacklist
Viettel Threat Intelligence	harmless	clean	blacklist
ViriBack	harmless	clean	blacklist
VX Vault	harmless	clean	blacklist
Webroot	harmless	clean	blacklist
Forcepoint ThreatSeeker	harmless	clean	blacklist
Yandex Safebrowsing	harmless	clean	blacklist
ZeroCERT	harmless	clean	blacklist

IP ADDRESS: 35.230.66.101	
Community Score	**6/98** security vendors flagged this as malicious
Last Analysis Date	Mon Dec 8 07:26:43 2025
Reputation	0
Times Submitted	43
Last Final URL	http://35.230.66.101/
Last Analysis Stats	Malicious: 6, Suspicious: 1, Harmless: 61, Undetected: 30
VirusTotal Report	View Full Report

ENGINE NAME	CATEGORY	RESULT	METHOD
alphaMountain.ai	malicious	phishing	blacklist
BitDefender	malicious	malware	blacklist
CRDF	malicious	malicious	blacklist
CyRadar	malicious	malicious	blacklist
G-Data	malicious	malware	blacklist
Webroot	malicious	malicious	blacklist
AlphaSOC	suspicious	suspicious	blacklist
AutoShun	undetected	unrated	blacklist
Axur	undetected	unrated	blacklist
Bfore.Ai PreCrime	undetected	unrated	blacklist
Bkav	undetected	unrated	blacklist
ChainPatrol	undetected	unrated	blacklist
Cluster25	undetected	unrated	blacklist
CSIS Security Group	undetected	unrated	blacklist

ENGINE NAME	CATEGORY	RESULT	METHOD
Cyan	undetected	unrated	blacklist
Ermes	undetected	unrated	blacklist
GCP Abuse Intelligence	undetected	unrated	blacklist
Gridinsoft	undetected	unrated	blacklist
Hunt.io Intelligence	undetected	unrated	blacklist
Kaspersky	undetected	unrated	blacklist
Lumu	undetected	unrated	blacklist
MalwareURL	undetected	unrated	blacklist
Mimecast	undetected	unrated	blacklist
Netcraft	undetected	unrated	blacklist
0xSI_f33d	undetected	unrated	blacklist
PhishFort	undetected	unrated	blacklist
PhishLabs	undetected	unrated	blacklist
PrecisionSec	undetected	unrated	blacklist
SafeToOpen	undetected	unrated	blacklist
Sansec eComscan	undetected	unrated	blacklist
SOCRadar	undetected	unrated	blacklist
Trustwave	undetected	unrated	blacklist
Underworld	undetected	unrated	blacklist
URLQuery	undetected	unrated	blacklist
VIPRE	undetected	unrated	blacklist
Forcepoint ThreatSeeker	undetected	unrated	blacklist
ZeroFox	undetected	unrated	blacklist
Artists Against 419	harmless	clean	blacklist
Acronis	harmless	clean	blacklist
Abusix	harmless	clean	blacklist
ADMINUSLabs	harmless	clean	blacklist
Lionic	harmless	clean	blacklist
Criminal IP	harmless	clean	blacklist
AILabs (MONITORAPP)	harmless	clean	blacklist
AlienVault	harmless	clean	blacklist
Antiy-AVL	harmless	clean	blacklist
ArcSight Threat Intelligence	harmless	clean	blacklist
benkow.cc	harmless	clean	blacklist
BlockList	harmless	clean	blacklist
Blueliv	harmless	clean	blacklist

ENGINE NAME	CATEGORY	RESULT	METHOD
Certego	harmless	clean	blacklist
Chong Lua Dao	harmless	clean	blacklist
CINS Army	harmless	clean	blacklist
Snort IP sample list	harmless	clean	blacklist
CMC Threat Intelligence	harmless	clean	blacklist
Xcitium Verdict Cloud	harmless	clean	blacklist
Cyble	harmless	clean	blacklist
desenmascara.me	harmless	clean	blacklist
DNS8	harmless	clean	blacklist
Dr.Web	harmless	clean	blacklist
Emsisoft	harmless	clean	blacklist
ESET	harmless	clean	blacklist
ESTsecurity	harmless	clean	blacklist
EmergingThreats	harmless	clean	blacklist
Feodo Tracker	harmless	clean	blacklist
Fortinet	harmless	clean	blacklist
Google Safebrowsing	harmless	clean	blacklist
GreenSnow	harmless	clean	blacklist
Heimdal Security	harmless	clean	blacklist
IPsum	harmless	clean	blacklist
Juniper Networks	harmless	clean	blacklist
Malwared	harmless	clean	blacklist
MalwarePatrol	harmless	clean	blacklist
malwares.com URL checker	harmless	clean	blacklist
OpenPhish	harmless	clean	blacklist
Phishing Database	harmless	clean	blacklist
Phishtank	harmless	clean	blacklist
PREBYTES	harmless	clean	blacklist
Quick Heal	harmless	clean	blacklist
Quttera	harmless	clean	blacklist
Rising	harmless	clean	blacklist
Sangfor	harmless	clean	blacklist
Scantitan	harmless	clean	blacklist
SCUMWARE.org	harmless	clean	blacklist
Seclookup	harmless	clean	blacklist
Sophos	harmless	clean	blacklist

ENGINE NAME	CATEGORY	RESULT	METHOD
Spam404	harmless	clean	blacklist
StopForumSpam	harmless	clean	blacklist
Sucuri SiteCheck	harmless	clean	blacklist
securolytics	harmless	clean	blacklist
Threatsourcing	harmless	clean	blacklist
ThreatHive	harmless	clean	blacklist
URLhaus	harmless	clean	blacklist
Viettel Threat Intelligence	harmless	clean	blacklist
ViriBack	harmless	clean	blacklist
VX Vault	harmless	clean	blacklist
Yandex Safebrowsing	harmless	clean	blacklist
ZeroCERT	harmless	clean	blacklist

MetaDefender Analysis

	35.230.66.101
COMMUNITY SCORE	0/21 : security vendors flagged this as malicious
GEO INFO	Country : United States City : The Dalles Location : 45.5517 , -121.219
LAST ANALYSIS DATE	2025-12-16 11:57:59

SOURCE	ASSESSMENT	LAST DETECTED	LAST UPDATE	RESULT
Offline Reputation	suspicious		2025-12-16T07:35:18.994Z	2
webroot.com	trustworthy		2025-12-16T07:35:19.051Z	0
check.torproject.org			2025-12-16T07:35:19.301Z	5
www.usom.gov.tr			2025-12-16T07:35:19.301Z	5
dataplane.org			2025-12-16T07:35:19.301Z	5
www.team-cymru.org			2025-12-16T07:35:19.301Z	5
stopforumspam.com			2025-12-16T07:35:19.301Z	5
sblam.com			2025-12-16T07:35:19.301Z	5
blocklist.de			2025-12-16T07:35:19.301Z	5

SOURCE	ASSESSMENT	LAST DETECTED	LAST UPDATE	RESULT
spamhaus.org			2025-12-16T07:35:19.301Z	5
urlhaus.abuse.ch			2025-12-16T07:35:19.301Z	5
openphish.com			2025-12-16T07:35:19.301Z	5
normshield.com			2025-12-16T07:35:19.301Z	5
rules.emergingthreats.net			2025-12-16T07:35:19.301Z	5
botscout.com			2025-12-16T07:35:19.301Z	5
tracker.viriback.com			2025-12-16T07:35:19.301Z	5
danger.rulez.sk			2025-12-16T07:35:19.301Z	5
reputation.alienvault.com			2025-12-16T07:35:19.301Z	5
vxvault.net			2025-12-16T07:35:19.301Z	5
mirc.com			2025-12-16T07:35:19.301Z	5
isc.sans.edu			2025-12-16T07:35:19.301Z	5

AbuseIPDB Analysis

IP ADDRESS: 172.16.0.1	
Is Public	False
IP Version	4
Is Whitelisted	False
Abuse Confidence Score	**0**
Country Code	None
Usage Type	Reserved
ISP	Private IP Address LAN
Domain	None
Hostnames	N/A
Is Tor	False
Total Reports	1
Number of Distinct Users	1
Last Reported At	2025-09-20T17:37:03+00:00

IP ADDRESS: 35.230.66.101	
Is Public	True
IP Version	4
Is Whitelisted	False
Abuse Confidence Score	**0**
Country Code	US
Usage Type	Data Center/Web Hosting/Transit
ISP	Google LLC
Domain	google.com
Hostnames	101.66.230.35.bc.googleusercontent.com
Is Tor	False
Total Reports	0
Number of Distinct Users	0
Last Reported At	2025-08-31T13:42:00+00:00

AlienVault OTX Analysis

	172.16.0.1
ASN	Unknown
REPUTATION LEVEL	Clean
REPUTATION SCORE	0/7
THREAT PULSES	0

	35.230.66.101
ASN	AS396982 google
ASSOCIATED URLS	0
CITY	The Dalles
CONTINENT	NA
COUNTRY	United States of America
LATITUDE	45.5999
LONGITUDE	-121.1871
MALWARE SAMPLES	0
PASSIVE DNS RECORDS	1
REPUTATION LEVEL	Clean
REPUTATION SCORE	0/7
THREAT PULSES	50

PULSE NAME	TAGS	CREATED	TLP	THREAT SCORE

PULSE NAME	TAGS	CREATED	TLP	THREAT SCORE
PurpleSynapz		2019-12-05T07:11:22.913000	white	0
Georgs Honeypot	honeypot, kfsensor, rdp, ssh	2021-04-07T09:05:05.353000	white	0
Fakelabs Honeynet Project	cowrie, ssh, honeypot	2022-06-21T00:32:00.646000	white	0
Uzaktan Tetiklenen Kara Delik	RTBH, DDoS	2024-09-02T00:03:00.003000	green	0
Laboratorio5-1	honeypot, kfsensor, rdp, ssh	2025-03-22T17:45:22.902000	white	0
Laboratorio5-1	honeypot, kfsensor, rdp, ssh	2025-03-22T17:45:26.728000	white	0
Automated Threat Intelligence - Brute-force hosts for 2024-08-26	brute force, ssh	2024-08-26T01:26:55.613000	white	0
Automated Threat Intelligence - Scanning hosts for 2024-08-26	scan, ssh, sip, sipvicious	2024-08-26T01:27:11.633000	white	0
ETIC Cybersecurity 2024-09-01 Port Scan		2024-08-31T22:00:51.114000	white	0
ETIC Cybersecurity 2024-09-01 Port Scan		2024-08-31T22:01:57.079000	white	0

GreyNoise Analysis

IP ADDRESS: UNKNOWN IP	
Status	Not observed by GreyNoise
Classification	Unknown
Noise Level	Not in dataset
Riot (Trust List)	No
Risk Level	Unknown - Not in GreyNoise dataset

IP ADDRESS: 35.230.66.101	
Status	Not observed by GreyNoise
Classification	Unknown
Noise Level	Not in dataset
Riot (Trust List)	No
Risk Level	Unknown - Not in GreyNoise dataset

IPQualityScore Analysis

IP ADDRESS: 172.16.0.1	
Fraud Score	**100**/100

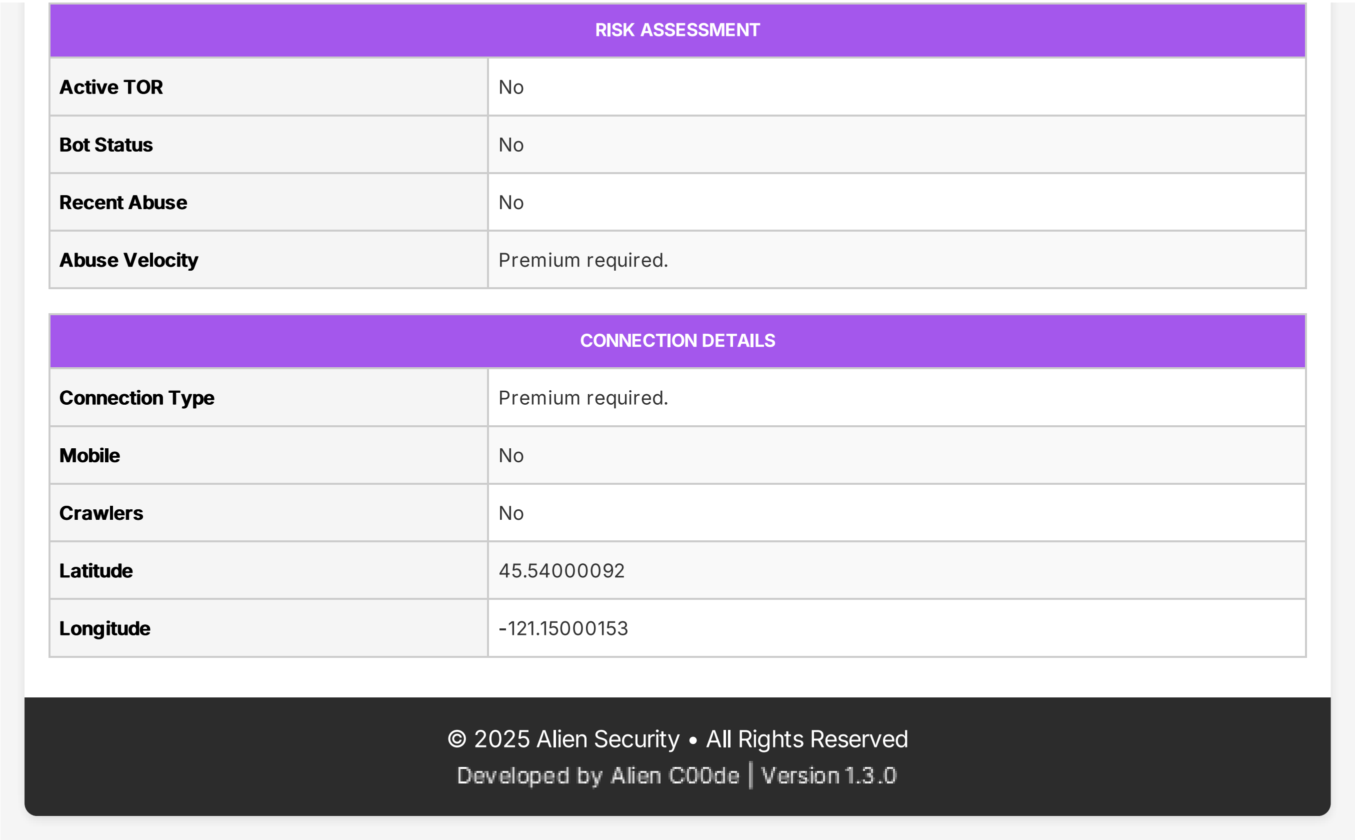
IP ADDRESS: 172.16.0.1	
Country	N/A - N/A, N/A
ISP	Private IP Address
Organization	Private IP Address
ASN	0
Host	N/A
Timezone	N/A

RISK ASSESSMENT	
Proxy	Yes
VPN	Yes
TOR	No
Active VPN	No
Active TOR	No
Bot Status	Yes
Recent Abuse	Yes
Abuse Velocity	Premium required.

CONNECTION DETAILS	
Connection Type	Premium required.
Mobile	No
Crawlers	No
Latitude	0
Longitude	0

IP ADDRESS: 35.230.66.101	
Fraud Score	**0**/100
Country	US - Oregon, The Dalles
ISP	Google
Organization	Google Workspace
ASN	396982
Host	101.66.230.35.bc.googleusercontent.com
Timezone	America/Los_Angeles

RISK ASSESSMENT	
Proxy	No
VPN	No
TOR	No
Active VPN	No



RISK ASSESSMENT	
Active TOR	No
Bot Status	No
Recent Abuse	No
Abuse Velocity	Premium required.

CONNECTION DETAILS	
Connection Type	Premium required.
Mobile	No
Crawlers	No
Latitude	45.54000092
Longitude	-121.15000153

Developed by Alien C00de | Version 1.3.0