THREAT INTELLIGENCE REPORT

IP Address: 93.174.95.106
Generated: 2025-12-15 18:40:20 UTC

RISK ASSESSMENT

Risk Score: 62/100 - MEDIUM RISK

Confidence: 83% - VERY HIGH

Metric	Value
Risk Score	62/100
Risk Level	MEDIUM RISK
Confidence Score	83%
Confidence Level	VERY HIGH
Malicious	YES
Total Reports	8384

TECHNICAL DETAILS

Field	Value
Country	Netherlands
Country Code	NL
ISP	FiberXpress BV
Domain	fiberxpress.net
Last Reported	2025-12-15T23:16:50+00:00

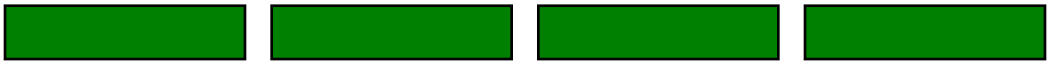
THREAT INTELLIGENCE

Categories: LAMP, ssh, fatt, SQL Injection, Telnet, Exploited Host, honeytrap, IoT Targeted, Fraud Orders, sentrypeer
Threat Types: LAMP, ssh, honeytrap, sentrypeer, Telnet, webscanner, bruteforce, web app attack,

ipphoney, probing, dionaea, cowrie

API Source Health:

4/4 sources



AbuseIPDB | AlienVault | VirusTotal | GreyNoise

MITRE ATT&CK; TECHNIQUES

Technique ID	Name	Tactic
T1021.004	SSH	Lateral Movement
T1190	Exploit Public-Facing Application	Initial Access
T1564.014	Extended Attributes	Defense Evasion
T1021	Remote Services	Lateral Movement
T1563	Remote Service Session Hijacking	Lateral Movement
T1557	Adversary-in-the-Middle	Credential Access
T1592	Gather Victim Host Information	Reconnaissance
T1564.012	File/Path Exclusions	Defense Evasion
T1133	External Remote Services	Persistence
T1110	Brute Force	Credential Access
...	+ 23 more techniques	

Total: 33 technique(s) mapped | Reference: attack.mitre.org

CYBER KILL CHAIN ANALYSIS

6/7 Stages Detected

Stage	Status
1. Reconnaissance	● IDENTIFIED
2. Weaponization	■ Not Detected
3. Delivery	● IDENTIFIED
4. Exploitation	● IDENTIFIED
5. Installation	● IDENTIFIED
6. Command & Control	● IDENTIFIED
7. Actions on Objectives	● IDENTIFIED

Attack spans 6 stage(s): 1. Reconnaissance, 3. Delivery, 4. Exploitation, 5. Installation, 6. Command & Control, 7. Actions on Objectives | Reference: Lockheed Martin Cyber Kill Chain

NETWORK PROFILE

Field	Value
Usage Type	Data Center/Web Hosting/Transit
Autonomous System	AS202425 - ip volume inc
Unique Reporters	433

TEMPORAL INTELLIGENCE

Observation	Timestamp
Last Observed	2025-12-15

COMMUNITY INTELLIGENCE

Source	Information
VirusTotal Votes	Harmless: 1 | Malicious: 19 | Total: 20
Community Tags	LAMP, ssh, honeytrap, sentrypeer, Telnet, webscanner, bruteforce, web app attack,

RECOMMENDATION

Action	MONITOR
Priority	MEDIUM
Justification	Risk score: 62/100 | Confidence: 83% (VERY HIGH) | 8384 report(s) from threat intelligence sources | Flagged as malicious by one or more sources | High confidence assessment from multiple agreeing sources
Confidence Note	High confidence assessment from multiple agreeing sources