TICE Threat Intelligence Report

Generated: 2025-11-07 09:15:56

IP Address: 45.142.212.61

Executive Summary

Metric	Value
Threat Score	48.0/100
Risk Level	Medium
Classification	BENIGN
Confidence	40%

Geographic Information

Field	Value
Country	Moldova
Region	Chisinau Municipality
City	Chisinau
ISP	Unknown
Organization	Unknown

Network Indicators

Detected: VPN Detected, Proxy Detected

Threat Categories

Category	Severity
Proxy/VPN	MEDIUM

VPN	MEDIUM

Intelligence Sources

Source	Status	Data Received
ABUSEIPDB	✓ Active	No
IPAPI	✓ Active	No
IPQUALITYSCORE	✓ Active	No

■ MITRE ATT&CK; Threat Intelligence

Historical attack context for law enforcement investigations

Intelligence Confidence Level **HIGH**

■ Identified Threat Actors

MuddyWater (G0069) - ATTRIBUTION: Iran

MuddyWater is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS).[1] Since at least 2017, MuddyWater has targeted a range of government and private organizations across sectors, including telecommunications, local government, defen

■ Attack Timeline

Event	Date
First Detected	2022-02-24T18:21:41.999000
Last Detected	2025-10-17T06:20:18.207000
Activity Span	1330 days

■ Identified Malware

S0194, S0591, S0250, S0488, S1243, S0594, S1047, S0349, S0363, S0002

■ Intelligence Sources

Source	Findings
AlienVault OTX	13 threat pulses
ThreatFox IOC	0 malware indicators
MITRE ATT&CK	1 threat group profiles
C2 Server	NO
Botnet	NO

■■

This report was automatically generated by TICE (Threat Intelligence Correlation Engine)

Report ID: 45-142-212-61-20251107091556