

■■ TICE Threat Intelligence Report

Generated: 2025-11-06 20:36:53

IP Address: 45.142.212.61

Executive Summary

Metric	Value
Threat Score	10/100
Risk Level	Low
Classification	BENIGN
Confidence	30%

Geographic Information

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

Network Indicators

Detected: Proxy Detected

Threat Categories

Category	Severity
Proxy/VPN	MEDIUM

Intelligence Sources

Source	Status	Data Received
IPAPI	✓ Active	Yes

Historical attack context for law enforcement investigations

HIGH

muddywater (G0069) - **ATtribution: Iran**

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

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

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: 45-142-212-61-20251106203653