■■ TICE Threat Intelligence Report

Generated: 2025-11-07 05:54:26

IP Address: 1.222.92.35

Executive Summary

Metric	Value
Threat Score	95/100
Risk Level	Critical
Classification	MALICIOUS
Confidence	30%

Geographic Information

Field	Value
Country	South Korea
Region	Gyeonggi-do
City	Hwaseong-si
ISP	Unknown
Organization	Unknown

Network Indicators

Status: No suspicious network indicators detected

Threat Categories

Category	Severity
APT Infrastructure	MEDIUM
Espionage	MEDIUM
C2 Server	MEDIUM

Intelligence Sources

Source	Status	Data Received
IPAPI	✓ Active	Yes

■ MITRE ATT&CK; Threat Intelligence

Historical attack context for law enforcement investigations

Intelligence Confidence Level	CRITICAL

■■ Identified Threat Actors

APT41 (Double Dragon) - ATTRIBUTION: China

Also known as: APT41, Wicked Panda, Double Dragon

Campaign: Operation ShadowPad India **-** Targeting government and critical infrastructure

Target Sectors: Government, Healthcare, Telecommunications, Education

Target Regions: India, Bangladesh, Sri Lanka, Nepal

■ Identified Malware

ShadowPad, PlugX, Cobalt Strike

■■ Attack Techniques (MITRE ATT&CK;)

Tactics: Initial Access, Persistence, Command and Control, Exfiltration

Technique ID	Technique Name	Description
T1566.001	Phishing: Spearphishing Attachment	APT41 uses spearphishing with malicious attachments to gain initial access
T1059.001	Command and Scripting Interpreter: PowerShell	PowerShell used for execution and establishing persistence
T1071.001	Application Layer Protocol: Web Protocols	HTTPS-based C2 communication to blend with normal traffic
T1041	Exfiltration Over C2 Channel	Data exfiltration through encrypted C2 channels
T1587.001	Develop Capabilities: Malware	Custom malware development for targeted operations

■ Intelligence Sources

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

■■■
■■■■■■■■■■■■■■■■■■■■■

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

Report ID: 1-222-92-35-20251107055427