ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

AsyncRAT Malware Campaign Leveraging Fraudulent Gambling Infrastructure Targeting Bangladesh

TLP: CLEAR
Distribution: Public
Advisory on: AsyncRAT Malware Campaign Leveraging Fraudulent Gambling Infrastructure Targeting Bangladesh
Severity: Critical
Threat Type: Remote Access Trojan (RAT) / Financial Fraud / Credential Theft / Botnet C2 Infrastructure
Date: 17 May 2026

Executive Summary

BGD e-GOV CIRT has identified a malicious cyber campaign involving **AsyncRAT (Asynchronous Remote Access Trojan)** infrastructure actively targeting Bangladesh. Threat intelligence and forensic analysis indicate that the domain **ck44jili[.]com** is functioning as a primary **Command-and-Control (C2) node** associated with an AsyncRAT malware operation.

The campaign combines malware delivery, remote access capabilities, and deceptive financial fraud tactics, where threat actors disguise malicious payloads as legitimate software while simultaneously operating fraudulent online gambling infrastructure targeting Bangladeshi users.

Of particular concern, the malicious infrastructure appears designed to socially engineer Bangladesh-based victims through localized payment mechanisms including **bKash, Nagad, and Rocket**, increasing the likelihood of successful financial fraud and malware infection.

Analysis confirms that the malware payload masquerades as a **WinRAR utility executable (winrar-x64.exe)**, while internally functioning as **AsyncRAT v0.5.8**, enabling full remote control over infected systems.

Bangladesh Threat Context

The campaign presents elevated risk to Bangladesh due to localized targeting characteristics.

Observed indicators suggest:

- Bangladesh-focused fraudulent web infrastructure
- abuse of local financial transaction ecosystems
- social engineering targeting local users
- potential harvesting of credentials and financial information

Threat actors appear to leverage Bangladesh-specific payment channels, increasing victim trust and improving fraud success rates. Potentially affected sectors:

- citizens / consumers
- banking & fintech
- telecom
- e-commerce

- government users
- enterprise employees
- education sector

Technical Analysis

Malware Payload: The analyzed malware sample is identified as:

Attribute	Value
Malware Family	AsyncRAT
Primary Domain	ck44jili[.]com
Operator	TAKA Alliance
Alias Domain	ck444[.]com, ck4444[.]com, ck444club[.]com, mail.emb666[.]com
Malware Alias	Microsoft Defender ID : Trojan:MSIL/AsyncRAT[.]BD!MTB
Version	0.5.8
File Name	winrar-x64.exe
File Type	.NET PE Executable
SHA256	b5c640131a38aa6d40755b114fd53d15e2e23c38f01989c6804dbb660d71aa71
Communication Ports	TCP: 80, 443, 6606, 7707, 8808
Mutex	AHZc9vwHmv0D
Phishing attachments	ZIP, ISO, HTML files
Persistence	Registry / Scheduled Task: CreateLoginTask() via Obfuscator.dll
Exfiltration targets	Browser extensions: MetaMask, Phantom (crypto wallets)
Recon	OS details, AV status, privilege level, active window titles
Protocol	Custom TCP with 4-byte length-prefixed packets, parsed via MessagePack
Data path	Staging in %AppData%

Malware Behavior: AsyncRAT enables attackers to perform:

- full remote desktop access
- credential theft
- browser credential harvesting
- command execution
- keylogging
- file upload/download
- process execution
- registry modification
- malware staging
- payload deployment
- botnet enrollment
- data exfiltration

Attack Chain:

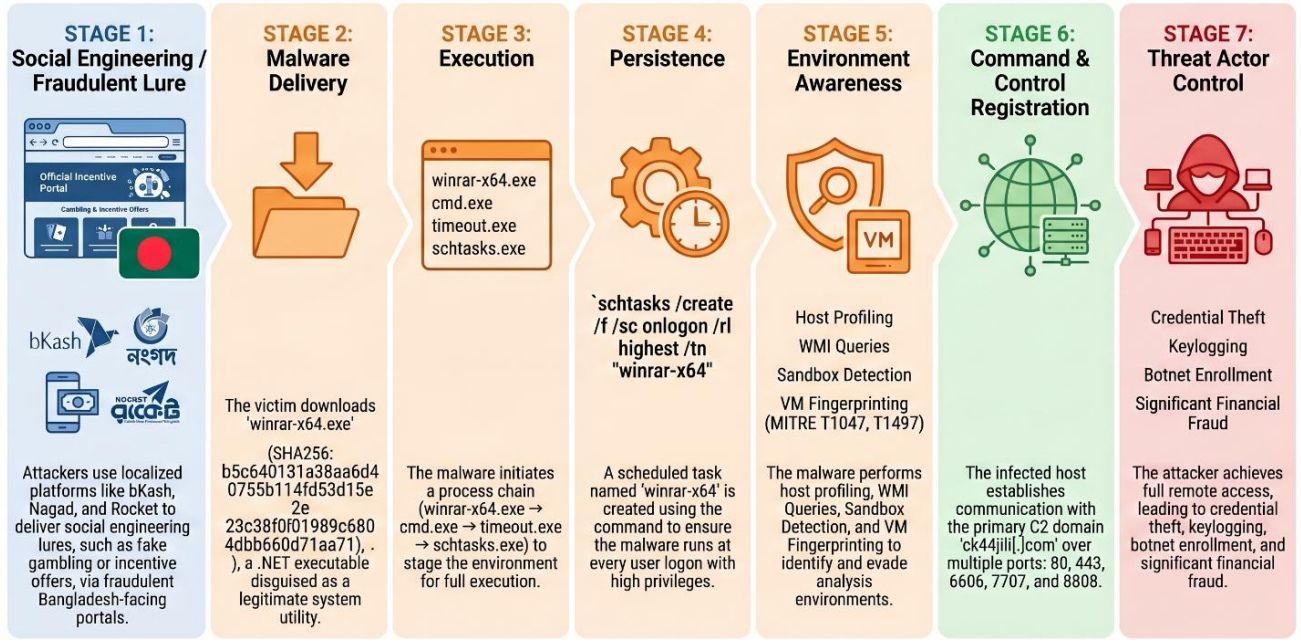

Figure: AsyncRAT Infection Chain Targeting Bangladesh

Persistence Mechanism: The malware establishes persistence using Windows Scheduled Tasks.

Observed command pattern: This allows malware execution at every user logon.

```
</> cmd
schtasks /create /f /sc onlogon /rl highest /tn "winrar-x64"
```

Persistence indicator: `Task Name: winrar-x64`

Defense Evasion Techniques:

The malware employs anti-analysis techniques including:

WMI-Based Fingerprinting: Observed behaviors indicate:

- environment discovery
- virtualization detection
- sandbox evasion
- host profiling

MITRE mapping:

Technique	ID
WMI	T1047
Virtualization/Sandbox Evasion	T1497

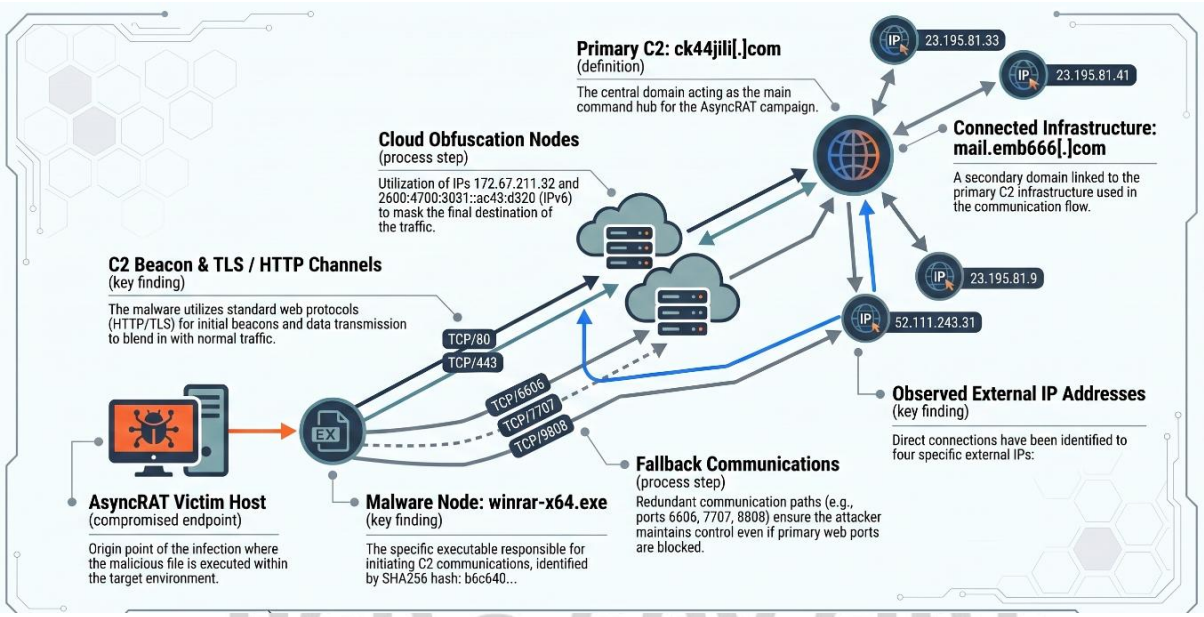

Figure: Observed AsyncRAT C2 Infrastructure and Communication Flow

Indicators of Compromise (IOCs)

Domains & C2

IOC	Type	Notes
ck44jili[.]com	Suspected lure/watering hole	Registered BD, targets local users ck44best.odoo
ck444[.]com, ck4444[.]com, ck444club[.]com, mail.emb666[.]com	Associated domain	Same operator (TAKA Alliance) ck44jili
ronymahmoud.camdvr[.]org	AsyncRAT C2	Subdomain suggests BD-linked operator threatfox.abuse
relay.shipperzone[.]online	Malicious ScreenConnect relay	Used in AsyncRAT delivery chain levelblue
3osch20[.]duckdns[.]org	Confirmed AsyncRAT C2	AES-256 encrypted, TCP-based beacon levelblue

IP Addresses: CDN/cloud-backed infrastructure may change dynamically

- 172.67.211.32
- 23.195.81.33
- 23.195.81.41
- 23.195.81.9
- 52.111.243.31
- 2600:4700:3031::ac43:d320

File Indicators

Type	Indicator
File Name	winrar-x64.exe
SHA256	b5c640131a38aa6d40755b114fd53d15e2e23c38f01989c6804dbb660d71aa71
MD5	0a523b3b96c5739cf509ed55cd572e6e
MD5	1831fc37856d558b02a889e32372d89c

Persistence Indicators: Registry / Scheduled Task: CreateLoginTask() via Obfuscator.dll,

Ports: TCP: 80, 443, 6606, 7707, 8808

Suspicious Processes: winrar-x64.exe, cmd.exe, timeout.exe, schtasks.

MITRE ATT&CK Mapping

Technique	ID	Description
Phishing / Social Engineering	T1566	Initial lure
Scheduled Task	T1053.005	Persistence
WMI	T1047	Host discovery
Sandbox Evasion	T1497	Anti-analysis
Application Layer Protocol	T1071	C2 communications
Command Execution	T1059	Command shell
Remote Access Software	T1219	RAT activity
System Information Discovery	T1082	Reconnaissance

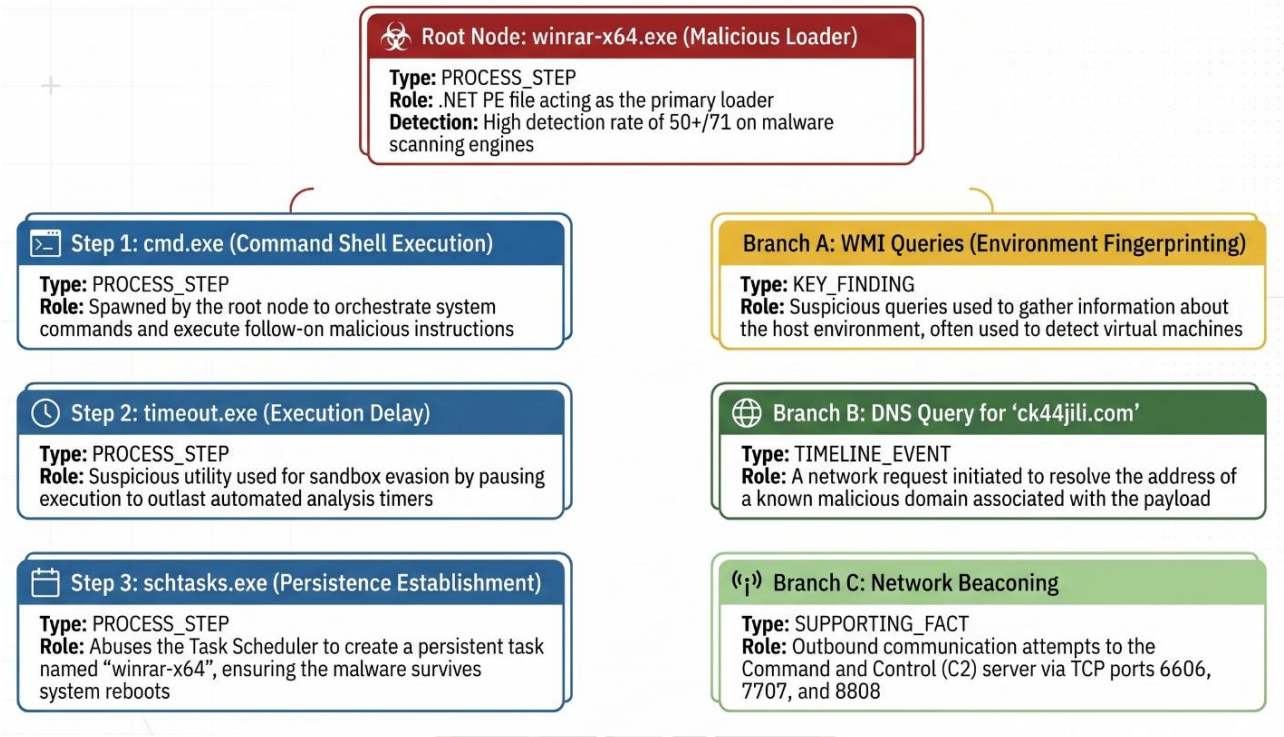

Figure: Observed AsyncRAT C2 Infrastructure and Communication Flow

Detection Recommendations

Hunt for Domains: Monitor DNS and proxy logs for: *ck44jili[.]com, mail.emb666[.]com*
Hunt for Network Activity: Monitor outbound connections to: *TCP 6606, TCP 7707, TCP 8808*
Hunt for Scheduled Tasks: Check: *schtasks /query*; Look for: *winrar-x64*Hunt for File Execution
Hunt for File Execution: Search endpoints for: *winrar-x64.exe*

Recommended Mitigation Action

Immediate Response

- block malicious domains
- block suspicious ports
- isolate infected systems
- preserve forensic evidence

Endpoint Security

- scan endpoints for AsyncRAT indicators
- remove malicious scheduled tasks
- reset compromised credentials
- inspect startup persistence

Network Controls

- restrict outbound unknown ports
- enable DNS filtering
- inspect proxy logs
- block malicious infrastructure

User Awareness

Warn users against:

- suspicious executable downloads
- gambling-themed fraud sites
- fake software installer

Source:

https://otx.alienvault.com/pulse/6a05b2633c378f45ddb96682 [Malachite]