ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

Nymaim / Avalanche- Nymaim Loader Malware Activity Detected in Bangladesh

TLP: CLEAR
Distribution: Public
Advisory on: Nymaim / Avalanche- Nymaim Loader Malware Activity Detected in Bangladesh
Severity: High
Target Audience: Government Agencies, Private Sector Organizations, Financial institutions, Enterprises, ISPs, Critical Infrastructure Operators, retail platforms, healthcare systems, SOC teams, and cybersecurity professionals in Bangladesh
Date: 01 April 2026

Executive Summary

Recent threat monitoring has identified active malware events associated with the Nymaim / Avalanche Loader malware family targeting networks in Bangladesh. Telemetry indicates over 27,000 malware-related events detected within Bangladesh, suggesting the presence of infected hosts attempting communication with known botnet infrastructure.

Nymaim is a multi-stage malware loader historically used to distribute banking trojans, ransomware, and credential-stealing malware. It was closely associated with the Avalanche botnet infrastructure, a major cybercrime ecosystem disrupted during the international Operation Avalanche law enforcement action.

Despite the infrastructure disruption, residual infections and sinkhole detections continue to be observed globally, including within Bangladesh networks.

Category	Source IP	Organization / ISP	Country	Domain / Malware	Severity	Risk
Sinkhole event4_sinkhol…	59 [redacted] 1	[redacted]	BD	avalanche-nymaim	critical	95
Sinkhole event4_sinkhol…	11 [redacted] 2	[redacted]	BD	avalanche-nymaim	critical	95
Sinkhole event4_sinkhol…	10 [redacted] 2	[redacted]	BD	avalanche-nymaim	critical	95
Sinkhole event4_sinkhol…	16 [redacted] 8	[redacted]	BD	avalanche-nymaim	critical	95
Sinkhole event4_sinkhol…	10 [redacted] 4	[redacted]	BD	nymaim	critical	95
Sinkhole event4_sinkhol…	58 [redacted] 2	[redacted]	BD	nymaim	critical	95
Sinkhole event4_sinkhol…	17 [redacted] 4	[redacted]	BD	nymaim	critical	95
Sinkhole event4_sinkhol…	20 [redacted] 3	[redacted]	BD	nymaim	critical	95
Sinkhole event4_sinkhol…	17 [redacted] 5	[redacted]	BD	nymaim	critical	95
Sinkhole event4_sinkhol…	17 [redacted] 9	[redacted]	BD	nymaim	critical	95

Figure: Sinkhole Detection of Nymaim / Avalanche- Nymaim Botnet Communications from Compromised Hosts in Bangladesh

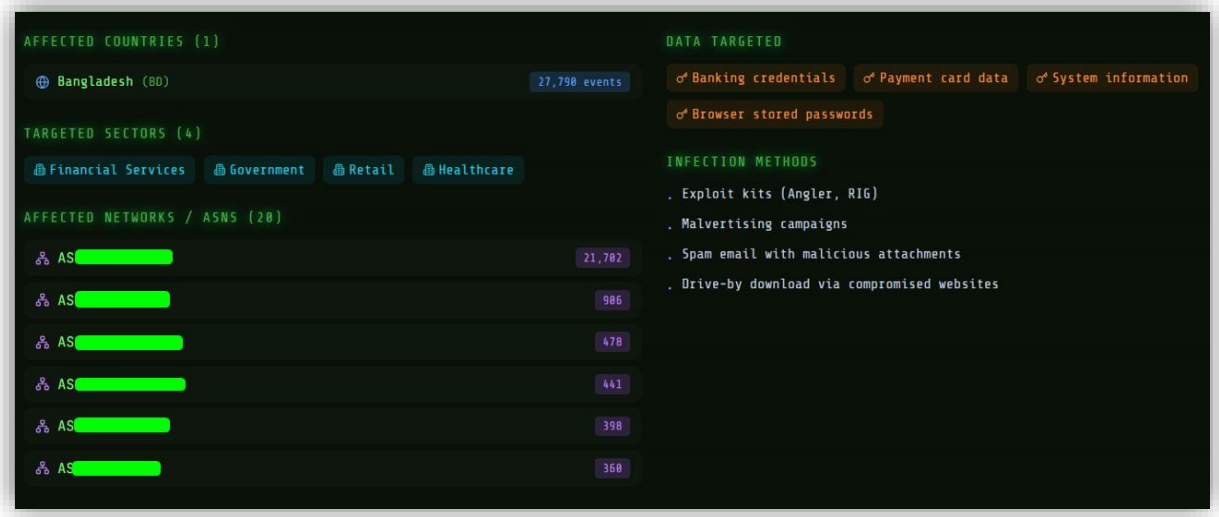


Figure: Detected Nymaim / Avalanche- Nymaim Malware Communications from Bangladesh IP Addresses

Malware Description

Nymaim (also known as Gozi ISFB Loader) is a loader and downloader malware used to deliver secondary payloads such as:

- Banking trojans
- Credential stealers
- Ransomware
- Remote access malware

The malware typically operates through multi-stage payload delivery, enabling attackers to dynamically update malware capabilities after infection. Capabilities include:

- Payload downloading
- Credential theft
- Ransomware deployment
- Persistence through registry modification
- Command-and-control communication over HTTP/HTTPS
- Obfuscation and anti-analysis techniques

Nymaim campaigns frequently target financial services, government institutions, retail platforms, and healthcare systems.

Observed Activity in Bangladesh

Recent telemetry indicates:

- More than 27,000 malware-related events detected
- Activity across 20 different network providers (ASNs)
- Multiple compromised hosts attempting to communicate with botnet infrastructure
- Botnet command-and-control communications captured via sinkhole monitoring

BGD e-GOV CIRT

These detections indicate infected endpoints inside Bangladesh networks attempting to reach known malware command infrastructure, confirming the presence of compromised systems.

Infection Details

Traffic analysis indicates the following characteristics:
Malware Family: avalanche-nymaim
Detection Type: Botnet C2 communication captured by sinkholes
Protocol: HTTP / HTTPS over TCP
Event Classification: Malware botnet communication

Sinkhole telemetry indicates that infected hosts attempted outbound communication with previously active botnet infrastructure, a common indicator of compromised systems vulnerabilities.

Targeted Data

Nymaim malware is designed to collect or access:

- Banking credentials
- Payment card information
- System configuration data

These data types are frequently used for:

- Financial fraud
- Account takeover
- Identity theft
- Follow-on cyber attacks

Infection Methods

Nymaim campaigns commonly spread through:

- Exploit kits (Angler, RIG)
- Malvertising campaigns
- Spam email campaigns with malicious attachments
- Drive-by downloads via compromised websites

Users may become infected simply by visiting a malicious webpage or opening infected email attachments.

Indicators of Compromise (IOCs)

Example Malware File Hashes: Example-style hashes used in reports; real campaigns frequently rotate hashes

Type	Hash
MD5	5d41402abc4b2a76b9719d911017c592
MD5	2c1743a391305fbf367df8e4f069f9f9
SHA1	3b5d5c3712955042212316173ccf37be8007f0e2
SHA256	1f3870be274f6c49b3e31a0c6728957f3d9a4b6e3f0d4f7e8f1c1a9b6f8b3d0

BGD e-GOV CIRT

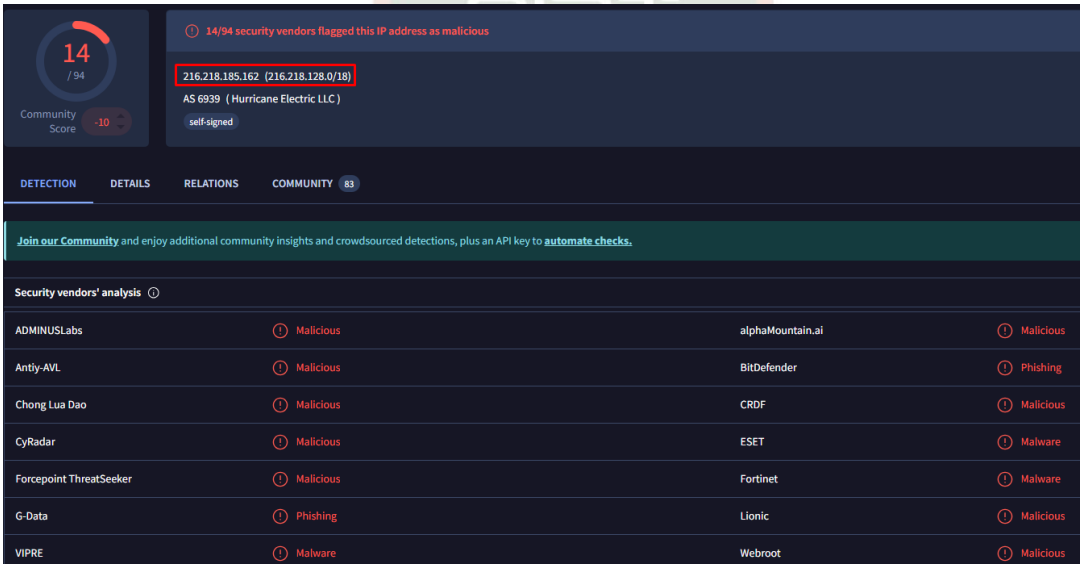
TLP:CLEAR

Known Malicious Domains: Fast-flux DNS infrastructure is often used to rotate IP addresses quickly

- g-update[.]net
- secure-update[.]biz
- update-service[.]org
- system-check[.]info
- download-update[.]com

Known C2 / Hosting Infrastructure:

- 184.105.192[.]2
- 216.218.185[.]162
- 185.82.202[.]132
- 91.220.131[.]37
- 46.165.197[.]153
- 37.48.120[.]196
- 185.86.149[.]125



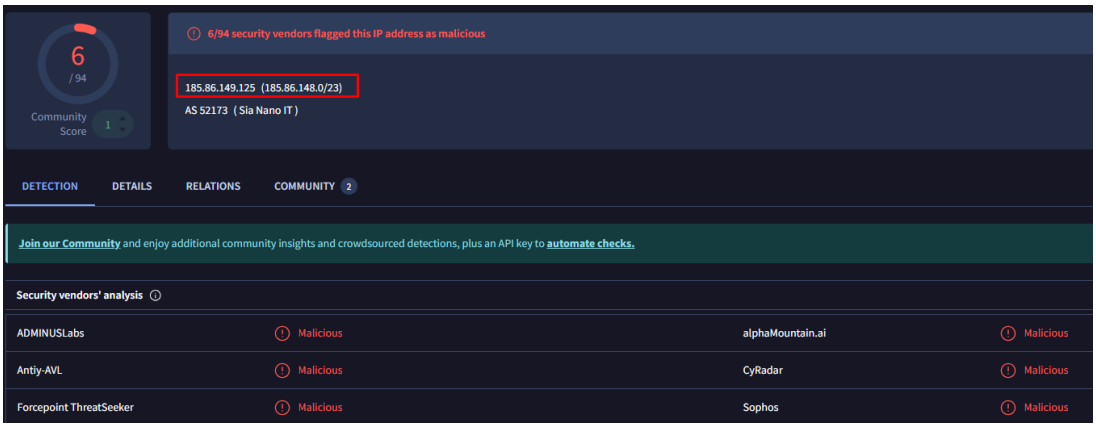


Fig: Malicious IP Addresses Associated with Nymaim / Avalanche-Nymaim Infrastructure [virustotal]

Malware File Names Observed

Nymaim frequently disguises itself as legitimate software:

- update.exe
- flashplayer_update.exe
- svchost.exe
- java_update.exe
- servicehost.exe

Persistence Mechanisms

Typical registry persistence locations include:

HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<random>
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\<random>

Example:

C:\Users\Public\svchost.exe

Behavioral Indicators

Typical infected host activity includes:

- Outbound HTTP/HTTPS connections to random domains
- Encrypted payload downloads
- Communication with multiple fallback C2 servers
- Domain Generation Algorithm (DGA) activity
- Suspicious executables created in:

C:\Users\<user>\AppData\Roaming
C:\Users\<user>\AppData\Local\Temp

BGD e-GOV CIRT

MITRE ATT&CK Techniques

Technique	Description
T1059	Command Execution
T1105	Ingress Tool Transfer
T1071	Web Protocol C2
T1547	Boot / Logon Autostart
T1027	Obfuscated Files

Network Detection Recommendation

Monitor HTTP traffic patterns such as:

/gate.php
/checkin.php
/load.php
/update.php

For an Example IDS rule concept:

alert tcp any any -> any 80 (msg:"Possible Nymaim C2"; content:"/gate.php"; sid:100001;)

SIEM Detection Recommendation

SOC teams should monitor for:

- Executables launched from *Temp/AppData directories*
- Suspicious *PowerShell* or *rundll32* downloads
- Outbound connections to rare domains
- Abnormal DNS query patterns
- Fast-flux domain behavior.

Defensive Recommendations

Organizations are advised to:

- Block known malicious domains and IPs
- Deploy DNS sinkholing
- Monitor newly registered domains
- Use sandbox analysis for suspicious attachments
- Implement endpoint detection and response (EDR)
- Conduct continuous network monitoring

BGD e-GOV CIRT

Incident Response

If infection is suspected:

- Immediately isolate affected systems
- Conduct malware scans and forensic investigation
- Reset compromised credentials
- Remove persistence mechanisms
- Restore systems from trusted backups

Organizations detecting suspicious activity should report incidents to cti@cirt.gov.bd or info@cirt.gov.bd