ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR



AI-Assisted Autonomous Cyber Attacks Targeting Digital Banking and Financial Services

TLP: CLEAR
Distribution: Public
Advisory on: AI-Assisted Autonomous Cyber Attacks Targeting Digital Banking and Financial Services
Severity: HIGH
Threat Category: AI-Assisted Intrusion / Financial Sector Threat / Credential Theft / Data Exfiltration
Target Sectors: Banking, NBFIs, Fintech, MFS, Payment Service Providers, Microfinance and Financial Technology Infrastructure
Date: 17 November 2026

Executive Summary

BGD e-GOV CIRT's Cyber Threat Intelligence (CTI) Unit is issuing this advisory to alert banks, financial institutions, fintech organizations, mobile financial service (MFS) providers, payment service providers and other organizations operating Bangladesh's financial ecosystem about the increasing threat of AI-assisted autonomous cyber-attacks.

Recent threat intelligence has identified sophisticated cyber operations in which attackers used AI-driven penetration-testing frameworks and autonomous agents to automate reconnaissance, vulnerability identification, exploit development, credential harvesting, privilege escalation, lateral movement and data exfiltration.

The investigation documented a full-chain compromise of Tanner Servicios Financieros, a financial-services organization in Chile. Attackers reportedly gained remote code execution in a Kubernetes-hosted application environment and subsequently moved through enterprise identity systems, Microsoft SQL Server environments, middleware and cloud infrastructure. The investigation reported access to more than 15.6 million financial records.

Separate evidence documented attack preparation against Dengoo.kz, an online micro-lending platform in Kazakhstan, involving a malicious WordPress theme and a custom PHP web shell. Successful web shell execution against that organization was not confirmed in the available evidence.

The investigation also identified infrastructure and activity associated with financial-sector reconnaissance and attack operations in other countries. Some additional fintech organizations were identified in attacker-side configuration files, and probing activity was independently reported; however, their compromise was not established.

The observed attack chain demonstrates how autonomous AI-assisted tooling can coordinate multiple conventional attack techniques and accelerate intrusion operations.

Key intelligence findings

Intelligence item	Reported finding
Attack tooling	ARTEX and CyberStrikeAI, with related offensive tooling identified
Open directories	Three exposed directories containing 3,732 files
Confirmed ARTEX consoles	Four identified during the investigation
Reported data exposure	More than 15.6 million financial records
Attack techniques	Kubernetes pod RCE, credential theft, AD CS exploitation, database pivoting, cloud abuse and data exfiltration

Assessment for Bangladesh: The techniques are relevant to Bangladesh's financial ecosystem because banks and financial-service organizations operate interconnected internet-facing applications, APIs, databases, identity infrastructure, cloud platforms and third-party services. Organizations should assess these environments proactively. This advisory does not claim that any Bangladeshi institution has been compromised in the reported incidents.

Threat Intelligence Overview

AI-Assisted Offensive Tooling

The investigation identified the use of the following offensive tools and frameworks:

Tool / framework	Observed purpose
ARTEX	LLM-driven autonomous penetration-testing framework used for reconnaissance and coordinated attack operations
CyberStrikeAI	Autonomous AI penetration-testing agent used to plan and execute attack activities
ScopeSentry	Reconnaissance and attack-surface discovery tooling associated with the same development ecosystem
Oktos	Additional AI-assisted offensive tooling identified in related infrastructure
Chisel	Tunnelling and network pivoting utility
Impacket	Network protocol and Active Directory-related offensive utilities
NetExec	Network authentication and lateral-movement testing utility
Kerbrute	Kerberos account enumeration and authentication testing utility

The presence of these tools does not independently establish malicious activity. Several are publicly available security tools that can also be used for authorized testing. Their execution should be investigated in the context of authorization, process ancestry, command-line activity, network connections and surrounding telemetry.

Why AI-Assisted Attacks Are a Concern

Traditional intrusion operations often require an attacker to manually perform reconnaissance, interpret results, select attack techniques and develop custom scripts.

AI-assisted agents can automate or coordinate several of these tasks. The investigated operation reportedly involved:

- Automated discovery of internet-facing services.
- Identification of exposed administrative interfaces.
- Generation of customized scripts and payloads.
- Automated testing of application weaknesses.
- Credential discovery and internal network enumeration.
- Selection of privilege-escalation and lateral-movement paths.
- Collection and processing of sensitive information.
- Adaptation of scripts based on target responses.

The principal concern is not simply the use of AI. It is the ability to automate multiple stages of an intrusion and conduct them at greater speed and scale.

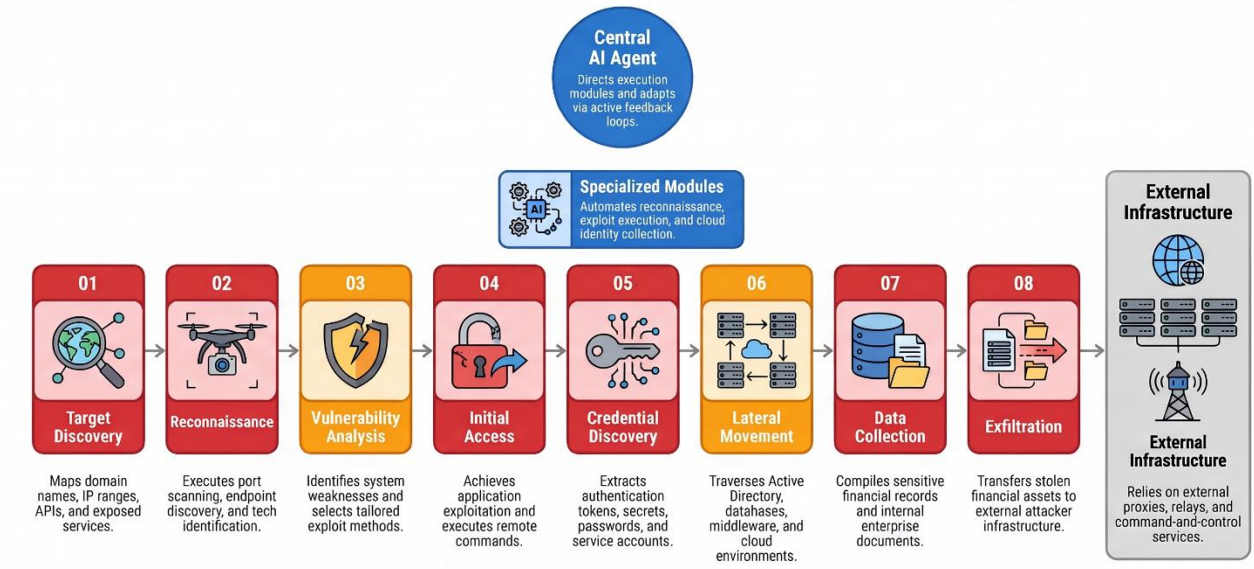


Figure: Conceptual lifecycle illustrating how AI-assisted offensive agents can coordinate reconnaissance, exploitation, credential discovery, lateral movement and data exfiltration against financial-sector infrastructure.

Detailed Technical Analysis of the Observed Attack Chain

Initial Access Through an Internet-Facing Application

In the previous global incident, attackers reportedly obtained remote code execution through a vulnerable document-rendering service hosted within a Kubernetes environment.

The compromised application provided an entry point into the internal environment.

The investigation identified:

- Exploitation of an application-level injection weakness.
- Remote command execution through a document-rendering workflow.
- Deployment of webshells.
- Collection of application configuration and environment information.
- Discovery of internal service endpoints and credentials.

Bangladesh relevance: Organizations should review document-rendering services, PDF conversion applications, file-processing APIs, template engines and other backend services accessible from the internet. Such systems should not be assumed safe merely because they are supporting services rather than core banking applications.

Kubernetes and Container Environment Compromise

After obtaining execution within the application environment, the attackers reportedly examined the container environment and collected information that could support access to other systems.

BGD e-GOV CIRT

Potentially exposed information included:

- Kubernetes service-account tokens.
- Kubernetes secrets.
- Application environment variables.
- Internal service addresses.
- Cloud identity tokens.
- Database connection strings.
- Application credentials.

A compromised container may become a pivot point if it has excessive privileges or unrestricted access to other workloads.

Organizations should review:

- Kubernetes RBAC permissions.
- Service-account token permissions.

- Container privilege settings.
- Access to host filesystems.
- Container-to-container network access.
- Cloud metadata service restrictions.
- Secret storage and rotation procedures.

Credential Harvesting and Active Directory Enumeration

Following initial access, attackers reportedly enumerated Active Directory accounts, domain systems, service accounts and authentication infrastructure.

The investigation identified activities involving:

- Kerberos account enumeration.
- AS-REP roasting.
- Password-hash collection and cracking.
- NTLM-related operations.
- LDAP enumeration.
- Active Directory Certificate Services exploitation.
- Credential reuse for access to additional systems.

The investigation also identified AD CS ESC8 and ESC17 exploitation in the documented compromise.

Bangladesh relevance: Banks and financial institutions should review domain-controller security, certificate templates, privileged accounts, service-account permissions, legacy authentication and certificate issuance logs.

Database Lateral Movement

BGD e-GOV CIRT

The attackers reportedly moved from the initially compromised application environment to connected Microsoft SQL Server systems.
The investigation identified:

- SQL Server credential collection.
- Password-hash extraction.
- Linked-server enumeration and pivoting.
- Database access through internal network connections.
- Attempts to access financial and accounting databases.
- Collection of customer and transaction-related records.

The investigation described access to 23 linked SQL Server instances across five or more countries through the documented pivot infrastructure.

Bangladesh relevance: Database servers should be segmented from public-facing application environments. Application service accounts should have access only to the databases and operations required for their functions.

Middleware and Enterprise Integration Compromise

The investigated operation also involved movement into enterprise integration and middleware environments.

Technologies mentioned in the investigation included:

- IBM DataPower.
- IBM Integration Bus (IIB).
- SOAP-based services.
- Internal middleware and integration endpoints.

The investigation documented probing for SOAP-related weaknesses, including XML External Entity (XXE) testing. Organizations should review exposed management interfaces, SOAP endpoints, internal integration services, authentication controls and administrative access to middleware platforms.

Cloud Infrastructure Abuse

The attackers reportedly used collected credentials and tokens to access cloud resources and retrieve sensitive information.

Observed activity included:

- Azure ARM token access.
- Microsoft Graph token access.
- Azure SQL access.
- Azure Storage access.
- Key Vault-related access.
- Enumeration of cloud storage containers.
- Retrieval of sensitive documents and financial records.

The investigation reported access to cloud storage through an exposed storage account key and collected tokens.

Bangladesh relevance: Organizations using Azure, AWS or hybrid cloud infrastructure should review identity permissions, access-token lifetimes, storage account keys, secret management, cloud audit logs and unusual data access.

Data Exfiltration

The investigated operation involved the collection and transfer of financial records and internal documents.

BGD e-GOV CIRT

The source reported:

- More than 15.6 million financial records accessed.
- Financial and customer-related documents.
- Employee personal information.
- Database extracts.
- Application and cloud credentials.
- Sensitive business documents.

The source also identified attacker-side scripts and infrastructure used to collect and process the extracted information.

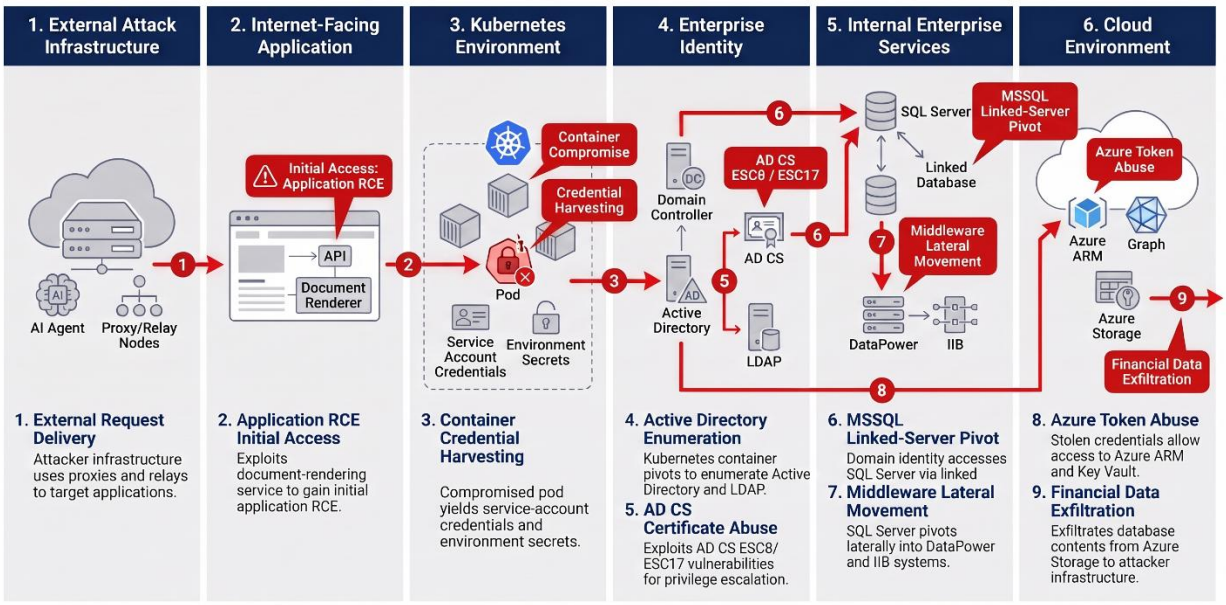


Figure: Observed Multi-Stage Intrusion: Kubernetes Initial Access to Financial Data Exfiltration.

Separate Attack Preparation: Malicious WordPress Theme

BGD e-GOV CIRT

The attacker prepared a malicious WordPress theme package containing a custom PHP webshell. The webshell was named: `zz27556p.php`

The SHA-256 hash reported for this file is:
`c026f0e6d48cd8b3c31ece6739eee6b84a22300e825d1b5d81686356299adeba`

The webshell supported several operations:

Parameter	Reported capability
`?c=`	Operating-system command execution
`?p=`	Arbitrary file reading
`?l=`	Directory listing
`?w=`	File writing using Base64-encoded content

The investigation also identified several malicious archive variants designed to test or bypass theme upload and extraction restrictions.

Archive / file	Observed purpose
zz27556.zip	Standard malicious theme package
lb.zip	Malicious theme package variant
zz27556b.zip	ZIP archive disguised with a different extension
ua_test.bin	Extension-bypass test
zz27556slip.zip	Zip Slip path-traversal test
zz27556big.zip	Upload-size-limit bypass test
zz27556many.zip	File-count-limit bypass test
zz27556root.zip	Root-level extraction test
zz27556pkg	WordPress theme directory name
big27556.bin	Padding file used in archive-size testing
wpx.bin	Small binary probe file

The attacker also prepared fake WordPress update responses that imitated legitimate theme update behavior.

Assessment: The investigation confirmed attack preparation and delivery-chain testing. Successful execution of the webshell against the target organization was not confirmed in the available evidence.

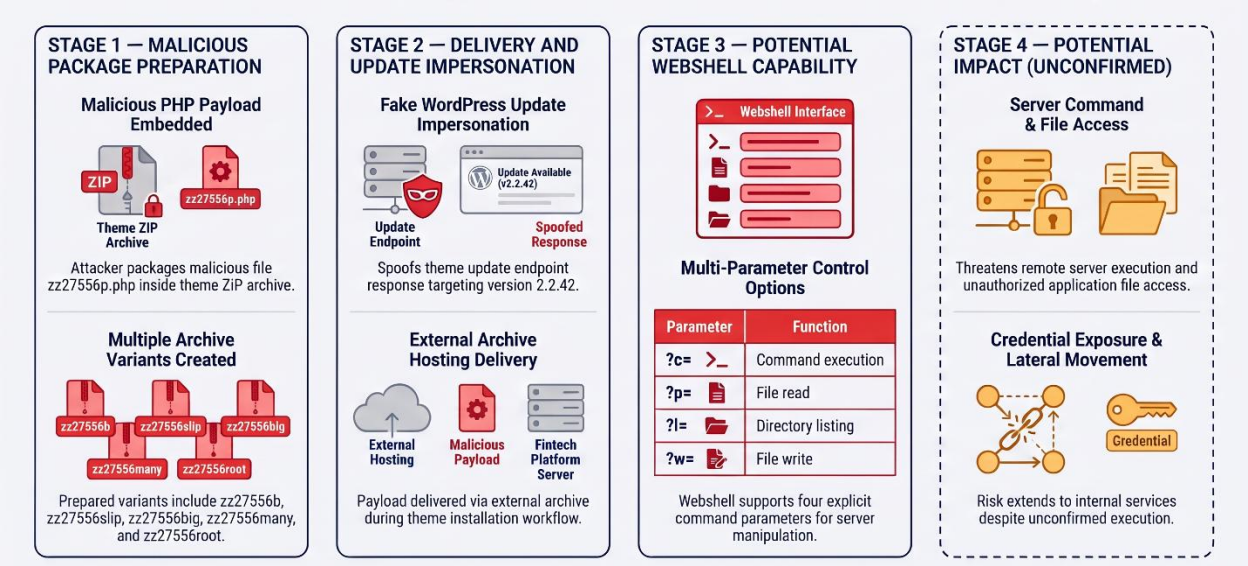


Figure: Attack-preparation workflow involving a malicious WordPress theme package, manipulated update responses and a custom PHP webshell

Indicators of Compromise (IOCs)

These indicators have different confidence levels. Organizations should not automatically block all listed IP addresses or domains. Some are shared cloud infrastructure, possible compromised proxy devices, candidate indicators or unrelated infrastructure requiring validation.

Primary Attacker Infrastructure

IP address	Reported observation	Recommended handling
23[.]132[.]132[.]30	ARTEX airsuperMAN on TCP/19000; CyberSuperMan on TCP/18080	Block / investigate
209[.]240[.]29[.]137	Probing of API management administration interface; possible compromised or recycled infrastructure	Monitor / investigate
156[.]240[.]9[.]93	CyberStrikeAI on TCP/8080; multiple open directories and offensive tooling	Block / investigate
14[.]248[.]148[.]196	OpenVPN/L2TP infrastructure; possible compromised network device used as proxy	Monitor / investigate
156[.]233[.]235[.]221	ARTEX console, open directory, attack preparation files and associated domains	Block / investigate
38[.]180[.]241[.]209	VPN infrastructure and operator egress activity	Block / investigate
103[.]89[.]122[.]51	Initially supplied as a possible C2/SFTP indicator; no evidence linking it to the actor, legitimate financial-institution partner SFTP service	**Do not block solely on this report**
182[.]16[.]82[.]194	ARTEX console on TCP/8787	Block / investigate
170[.]205[.]5[.]157	Reconnaissance indicator; no additional supporting data	Monitor
148[.]66[.]13[.]70	ScopeSentry on TCP/8082; Sub2API on TCP/18080	Block / investigate
132[.]145[.]155[.]113	Codex2API backend and noVNC service	Block / investigate

Additional ARTEX and Offensive Infrastructure

IP address	Reported observation
154[.]36[.]161[.]241	ARTEX airsuperMAN on TCP/19000; reported exfiltration endpoint
148[.]66[.]59[.]46	ARTEX console on TCP/8787
23[.]153[.]36[.]167	CyberSuperMan on TCP/18080
23[.]153[.]36[.]230	CyberSuperMan on TCP/18080
186[.]241[.]121[.]142	CyberSuperMan instance; certificate relationship with another observed console
216[.]118[.]252[.]154	AI credential-monetisation infrastructure and related domains
192[.]210[.]226[.]251	Candidate ARTEX console on TCP/8787; attribution confidence lower

Shared Cloud Egress and Proxy Infrastructure

The following addresses were identified as part of an Alibaba Cloud shared egress pool. These should be treated as contextual indicators, not confirmed dedicated attacker servers. Correlate these IPs with suspicious sessions, user-agent strings, URLs, timestamps and application behaviour. Avoid blanket blocking of shared cloud provider ranges without local evidence.

IP address	Reported provider / context
8[.]221[.]141[.]88	Alibaba Cloud shared egress
8[.]220[.]204[.]92	Alibaba Cloud shared egress
8[.]220[.]136[.]174	Alibaba Cloud shared egress
8[.]215[.]25[.]3	Alibaba Cloud shared egress; highest reported abuse score in the pool
8[.]213[.]222[.]247	Alibaba Cloud shared egress
8[.]211[.]42[.]167	Alibaba Cloud shared egress
8[.]211[.]200[.]183	Alibaba Cloud shared egress
8[.]210[.]17[.]35	Alibaba Cloud shared egress
47[.]251[.]87[.]199	Alibaba Cloud shared egress
47[.]238[.]134[.]126	Alibaba Cloud shared egress
47[.]237[.]107[.]41	Alibaba Cloud shared egress; spoofed device banners reported

Possible Compromised Consumer Router / Proxy Infrastructure

These addresses were assessed as likely compromised consumer network devices or proxy infrastructure. Their dynamic nature and third-party ownership require caution before blocking.

IP address	Reported observation
42[.]114[.]69[.]166	Dynamic consumer IP; MikroTik proxy ports and SOCKS5 service observed
116[.]104[.]251[.]199	Dynamic consumer IP; MikroTik, Huawei certificate and RTSP/DVR fingerprints observed

Related Infrastructure and Cross-Case Indicators

IP address	Reported context	Confidence / handling
177[.]5[.]66[.]55	Infrastructure linked in external reporting to a related AI-driven attack ecosystem	Related campaign; validate
191[.]223[.]44[.]126	Tunnelling pattern and callback URLs observed	Related infrastructure; validate
179[.]236[.]105[.]135	Chisel-like tunnelling callback pattern	Related infrastructure; validate
104[.]30[.]180[.]110	Shared Cloudflare CDN address	Low-confidence; do not block solely on IP
184[.]193[.]214[.]40	Amazon EC2 scanner infrastructure	Low-confidence; investigate context

Domains and DNS Indicators

Campaign-associated domains and subdomains:

Domain / indicator	Reported context
tg2p32[.]dnslog[.]cn	Out-of-band callback and data-exfiltration activity associated with a separate attack
9vr56s[.]dnslog[.]cn	Out-of-band callback used in command-injection testing
u6ud2s[.]dnslog[.]cn	Observed in ARTEX-related campaign activity

px61ft[.]dnslog[.]cn	SSRF probe callback
suishouji[.]top	Domain resolving to observed attacker infrastructure
898787[.]xyz	Infrastructure-associated domain
081652[.]xyz	Infrastructure-associated domain
silver[.]codesharee[.]online	Related AI credential-monetisation infrastructure
chatgpt2api[.]*	Related host naming pattern on observed infrastructure; wildcard is not a complete domain IOC

Important DNS note: dnslog[.]cn is a public out-of-band application-security testing service. The complete domain itself should not be treated as malicious. The specific subdomains listed above were identified as campaign-associated account identifiers.

Additional Observed Domain Infrastructure

The investigation also identified the following domains associated with infrastructure enrichment:

- quantrel[a]ipro[.]de — use the exact spelling from DNS telemetry before operational use; the source rendering contains a line-wrapped domain.
- rheinvexapp[.]de
- Additional related German investment-fraud domain names were mentioned but not fully enumerated in the available extract.

These domains should be treated as contextual intelligence requiring independent DNS and passive-DNS validation.

Webshell and File Indicators

Indicator	Type	Description
zz27556p.php	PHP file	Custom PHP webshell
ZZ27556OK	Beacon string	Webshell-related confirmation string
ws.sh	Shell script	Webshell deployment script name
pivot_relay.ps1	PowerShell script	Relay and pivoting script
extract_hprof.py	Python script	Java heap-dump credential extraction utility
P.class	Java class	Exploit-related file identified in the investigation
LocaleMgr.exe	Windows executable	Suspicious executable name masquerading as a locale manager
*.hprof	Java heap dump	Investigate unexpected creation, access or transfer

SHA-256 Hash

File	SHA-256
zz27556p.php	c026f0e6d48cd8b3c31ece6739eee6b84a22300e825d1b5d81686356299adeba

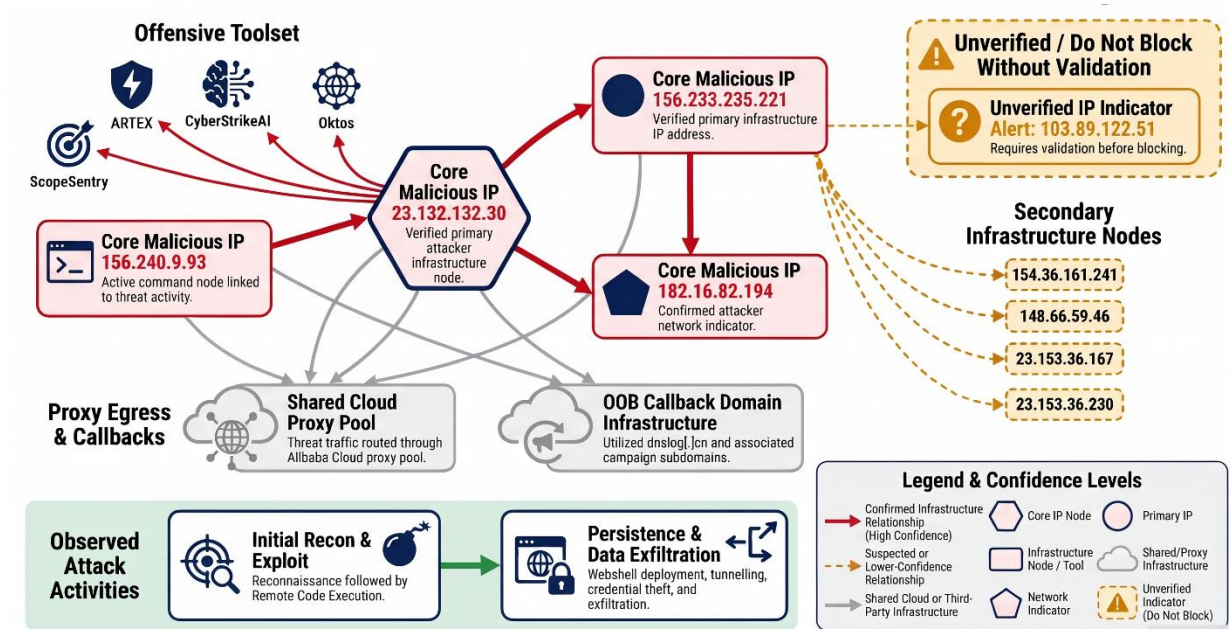


Figure: Identified Attacker Infrastructure, Offensive Tooling and Associated Network Indicators

Network Ports and Services

A port number alone is not a reliable malicious indicator. Correlate the service, process, host, destination and observed activity.

Port	Reported service / context	Recommended action
TCP/19000	ARTEX airsuperMAN console	Investigate unauthorized exposure
TCP/18080	CyberSuperMan service	Investigate
TCP/8787	ARTEX console	Investigate
TCP/8080	CyberStrikeAI interface	Investigate
TCP/8000	Open directory / offensive file hosting	Investigate
TCP/8081	Open directory / tooling artifacts	Investigate
TCP/18080	Open directory / related offensive service in another observation	Investigate
TCP/8890	Werkzeug panel with reported realm poc	Investigate
TCP/10443	Werkzeug panel with reported realm PSB-OPS	Investigate
TCP/8090	Certificate common name aella-console	Investigate
TCP/4444	Metasploit-associated listener reported	Investigate
TCP/47111	Out-of-band callback listener	Investigate
TCP/9998	Chisel tunnel callback	Investigate
TCP/6080	noVNC service	Investigate unauthorized exposure
TCP/5432	PostgreSQL service	Investigate unexpected public exposure

MITRE ATT&CK Mapping

The following mapping represents techniques supported by the described attack activities. It is a defensive classification, not an assertion that every technique occurred in every target environment.

MITRE ATT&CK technique	Technique ID	Observed or relevant activity
Active Scanning	T1595	External service and application reconnaissance
Gather Victim Host Information	T1592	Collection of host and service information
Exploit Public-Facing Application	T1190	Initial application exploitation
Valid Accounts	T1078	Use of collected credentials
Container Administration Command	T1609	Execution within container environments
Exploitation for Privilege Escalation	T1068	Privilege-escalation activity
Unsecured Credentials	T1552	Credential and secret discovery
OS Credential Dumping	T1003	Password-hash collection
Account Discovery	T1087	Active Directory enumeration
Domain Trust Discovery	T1482	Internal domain relationship discovery
Steal or Forge Kerberos Tickets	T1558	Kerberos-related attack activity
Steal or Forge Authentication Certificates	T1649	Certificate-based identity abuse
Remote Services	T1021	Lateral movement through remote services
SMB/Windows Admin Shares	T1021.002	Access to administrative shares
Exploitation of Remote Services	T1210	Exploitation of internal services
Data from Information Repositories	T1213	Collection from databases and repositories
Archive Collected Data	T1560	Preparation of collected information
Exfiltration Over Web Service	T1567	Web-based data transfer
Proxy	T1090	Proxy and relay infrastructure
External Proxy	T1090.002	External proxy usage
Data Staged	T1074	Preparation of collected data

Detection and Threat Hunting Recommendations

Web Application and Reverse Proxy Monitoring

Monitor for:

- Unexpected access to administrative panels.
- Repeated requests to application endpoints with unusual parameters.
- Suspicious PHP files created in web directories.
- Unexpected PUT, POST or file-upload requests.
- Requests to unusual paths such as /leak.
- Repeated API reconnaissance requests.
- Abnormal HTTP requests originating from shared proxy infrastructure.
- Requests to document-rendering or template-processing services followed by unexpected process execution.

Investigate whether the request was followed by a new child process, file creation or outbound connection.

Endpoint Detection and Response

Monitor Node.js, Java, PHP, web server, container and application processes for unexpected child processes. Investigate unexpected file creation in web roots, temporary directories, application staging folders and container writable layers.

Examples of suspicious process relationships include:

- Web server spawning `/bin/sh` or `/bin/bash`.
- PHP-FPM spawning a shell or system utility.
- Node.js spawning an unexpected command interpreter.
- Java application servers launching unexpected operating-system utilities.
- Application processes downloading executables or scripts.
- Unusual use of PowerShell, WMI, SMB or remote administration utilities.

Kubernetes Threat Hunting

Review:

- Kubernetes audit logs for unusual API requests.
- Creation of unexpected pods, jobs or deployments.
- Use of privileged containers.
- Unexpected exec operations into running containers.
- Service-account token access.
- Secret enumeration and access.

- Unexpected container image pulls.
- Container-to-host filesystem access.
- Outbound connections from application workloads to unapproved destinations.

Active Directory and Identity Monitoring

Investigate:

- Abnormal Kerberos authentication activity.
- AS-REP roasting attempts.
- Unusual LDAP queries.
- Unexpected certificate issuance.
- Modifications to AD CS certificate templates.
- NTLM relay indicators.
- Unusual domain-controller access.
- Password-hash extraction activity.
- New privileged accounts or changes to service-account permissions.

Database Monitoring

Monitor for:

- Unusual linked-server configuration or access.
- Unexpected SQL Server administrative activity.
- New or modified database logins.
- Unusual bulk data retrieval.
- Unexpected access to financial tables.
- Execution of operating-system commands through database services.
- Database connections originating from application servers that do not normally access those systems.

Cloud Security Monitoring

Review Azure and AWS audit logs for:

- Unexpected token usage.
- New service principals or identity permissions.
- Unusual managed-identity activity.
- Storage account key usage from unfamiliar hosts.
- Unusual Key Vault access.
- Bulk object downloads.
- Unexpected cloud management commands.
- New or modified serverless functions.
- Unusual cloud resource enumeration.

Suggested SIEM Detection Logic

The following are conceptual detection rules. Field names should be adapted to the organization's SIEM schema and available telemetry.

Rule 1: Webshell Execution Followed by Outbound Connection

Logic:

- Detect a web server, PHP, Node.js or Java process creating a shell or command interpreter.
- Correlate with an outbound network connection from the same host within a short time window.
- Raise severity when the process is associated with an internet-facing application.

Rule 2: Suspicious Application-to-Database Pivot

Logic:

- Identify application servers initiating connections to database servers they do not normally access.
- Correlate with new database logins, linked-server activity or bulk data retrieval.
- Raise an alert when the connection is followed by abnormal query volume.

Rule 3: Active Directory Credential Abuse

Logic:

- Detect unusual Kerberos, LDAP and NTLM activity.
- Correlate with privileged account usage, certificate issuance and access to domain controllers.
- Escalate when suspicious authentication is followed by lateral movement.

BGD e-GOV CIRT

Rule 4: Suspicious Cloud Token Usage

Logic:

- Detect cloud token use from unusual IP addresses, devices or application identities.
- Correlate with unusual storage enumeration, bulk download and privilege changes.
- Investigate if the same identity recently accessed a compromised application host.

Rule 5: Possible Financial API Abuse

Logic:

- Identify unusual low-value transactions to newly added beneficiaries.
- Correlate with subsequent high-value transactions or repeated disbursements.
- Detect transactions initiated through unusual API clients or modified application packages.

- Escalate when normal transaction approval, beneficiary validation or maker-checker controls are bypassed.

Rule 6: AI-Assisted Reconnaissance

Logic:

- Detect repeated API enumeration and high-volume endpoint discovery.
- Search for the user-agent indicators listed in Section 5.
- Correlate with rapid creation of scripts, unusual process execution and outbound connections to identified infrastructure.

Recommended Mitigation and Defensive Measures

Internet-Facing Application Security

- Patch vulnerable applications, frameworks, CMS platforms and backend services.
- Remove unnecessary public access to administrative interfaces.
- Enforce authentication and authorization for all sensitive API endpoints.
- Restrict file uploads and validate archive contents before extraction.
- Prevent directory traversal and unsafe archive extraction.
- Disable unnecessary server-side template execution.
- Apply secure coding practices for command execution and deserialization.
- Deploy and properly configure WAF protection.
- Conduct regular application security testing.

API and Financial Transaction Security

- Financial institutions should strengthen controls at the transaction layer:
- Enforce server-side transaction authorization.
- Apply API request signing and replay protection using nonces and timestamps.
- Validate transaction amount, beneficiary, account status and transaction limits on the server.
- Implement beneficiary cooling periods for newly added recipients.
- Apply maker-checker approval for sensitive payments and settlements.
- Monitor micro-value transactions followed by large transfers.
- Implement application attestation and detection of modified or repackaged mobile applications.
- Avoid relying solely on IP allowlisting for API authorization.
- Ensure that partner and payment-gateway API credentials are not shared across environments.

Kubernetes and Container Security

- Restrict Kubernetes API exposure.
- Apply least-privilege RBAC.
- Avoid privileged containers unless strictly required.
- Restrict pod-to-pod communication.

- Protect secrets and service-account tokens.
- Monitor container execution and image changes.
- Restrict outbound connections from sensitive workloads.
- Separate development, testing and production clusters.

Identity and Access Security

- Enforce MFA for privileged and remote access.
- Rotate exposed credentials, tokens and API keys.
- Review service-account permissions.
- Audit AD CS certificate templates.
- Monitor abnormal Kerberos and NTLM activity.
- Remove unused privileged accounts.
- Implement privileged access management.
- Use identity-based access controls rather than relying exclusively on network location.

Cloud and Database Security

- Enable cloud audit logging.
- Restrict storage access and rotate exposed keys.
- Monitor unusual access to cloud management services.
- Review managed identities and service principals.
- Restrict database connectivity through network segmentation.
- Disable unnecessary linked-server functionality.
- Monitor bulk database exports.
- Apply encryption and access controls to sensitive financial data.

SOC Monitoring and Incident Response

- Maintain 24/7 monitoring of critical financial applications.
- Apply additional monitoring during weekends and public holidays.
- Monitor application, endpoint, identity, database, firewall and cloud logs centrally.
- Deploy EDR and NDR monitoring across critical systems.
- Maintain a current inventory of internet-facing assets.
- Conduct threat hunting using both IOC-based and behaviour-based detection.
- Preserve forensic evidence before removing suspicious files or rebuilding systems.
- These are general indicators of possible exploitation or post-exploitation, not confirmed CVE-specific signatures.

Incident Response Procedure

If an organization identifies activity consistent with this advisory, it should:

Validate: Confirm the affected host, application, account and observed activity.
Contain: Isolate affected systems where compromise is suspected and restrict suspicious network communications.
Preserve: Retain application, endpoint, network, database, identity and cloud logs.

Investigate: Determine initial access, credential theft, privilege escalation, lateral movement and potential data exfiltration.
Protect identities: Revoke suspicious sessions and tokens, rotate exposed credentials and review privileged access.
Eradicate: Remove webshells, unauthorized scripts, malicious files and persistence mechanisms.
Recover: Restore from trusted backups, patch vulnerable services and validate system integrity.
Monitor: Maintain enhanced monitoring for recurring access, new persistence and suspicious transactions.

Organizations should follow applicable internal incident-response and regulatory reporting requirements.

Bangladesh-Specific Recommendations

BGD e-GOV CIRT recommends that Bangladesh's financial institutions prioritize the following:

Priority	Recommended action	Intended outcome
Critical	Review all internet-facing applications and APIs	Identify exposed entry points
Critical	Audit payment, disbursement and settlement APIs	Prevent unauthorized financial transactions
Critical	Review privileged credentials and cloud tokens	Reduce identity compromise risk
Critical	Examine Kubernetes and container environments	Prevent container-to-enterprise pivoting
High	Review Active Directory and AD CS configurations	Reduce privilege-escalation opportunities
High	Audit database linked-server access	Limit lateral movement
High	Monitor webshell and suspicious process activity	Detect post-exploitation activity
High	Review third-party plugins, themes and software updates	Reduce supply-chain risks
High	Strengthen cloud storage and audit logging	Detect unauthorized data access
High	Improve weekend and holiday SOC monitoring	Reduce delayed detection

Financial institutions should also review third-party technology providers, payment gateways, cloud service providers, software vendors and managed service providers that have privileged access to their environments.

The observed AI-assisted attack operations demonstrate that autonomous offensive tooling can accelerate reconnaissance, vulnerability exploitation, credential harvesting, privilege escalation, lateral movement and financial data exfiltration.

The documented compromise of a financial-services organization and separate attack preparation against a fintech organization highlight the importance of securing internet-facing applications, container environments, enterprise identities, databases, APIs and cloud infrastructure.

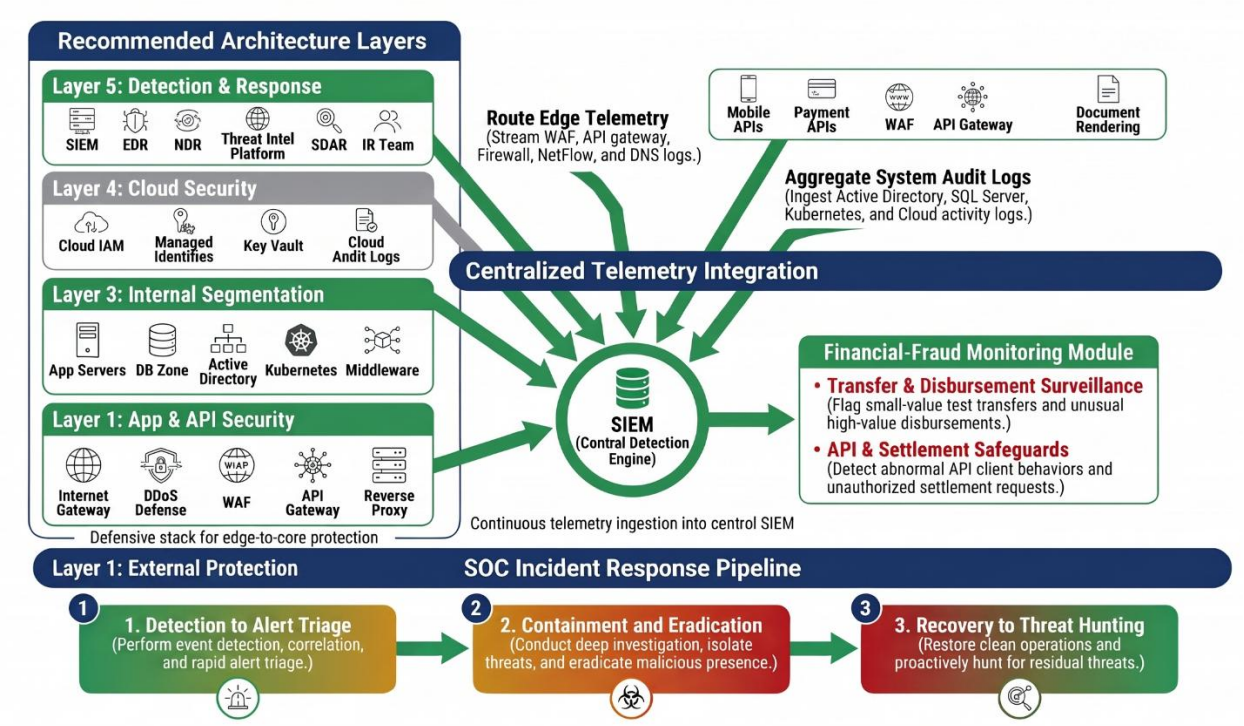


Figure: Recommended Security Monitoring and Protection Architecture for Bangladesh

For Bangladesh, the most important defensive priority is to protect the interconnected systems supporting digital banking, mobile financial services, payment processing and financial data management.

BGD e-GOV CIRT urges all relevant organizations to conduct proactive security assessments, strengthen identity and application controls, review the indicators and behavioural patterns in this advisory, and promptly report suspected cybersecurity incidents through established incident-response channels.

Organizations should not rely exclusively on blocking known indicators. Continuous monitoring, secure application design, identity protection, transaction validation and effective incident response are essential to reducing the risk of AI-assisted cyber-attacks.

References

- https://www.cert-in.org.in/s2cMainServlet?VLCODE=CIAD-2026-0058&pageid=PUBVLNOTES02
- https://www.ic3.gov/CSA/2026/261113.pdf
- https://labs.cloudsecurityalliance.org/research/csa-research-note-cyberstrikeai-artex-multi-agent-offense-20/
- https://labs.cloudsecurityalliance.org/research/csa-research-note-agentic-intrusion-financial-api-abuse-2026/
- Report on AI-Driven Attack on Digital Banking - Group IB

BGD e-GOV CIRT