ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

SideWinder-Associated Campaign Targeting South Asian Government and Financial Infrastructure

TLP: CLEAR
Distribution: Public
Advisory on: SideWinder-Associated Campaign Targeting South Asian Government and Financial Infrastructure
Severity: High
Threat Type: Cyber Espionage / Exploit Public-Facing Application / Credential Access / Webshell / C2
Potentially Affected Sectors: Government, Defence, Security, Financial, Revenue, Healthcare, Education and Critical Public Services
Date: 17 September 2026

Executive Summary

BGD e-GOV CIRT Cyber Threat Intelligence Unit is issuing this advisory regarding a newly reported suspected **SideWinder**-associated operational infrastructure targeting organizations across **South Asia**, including government-related infrastructure in Bangladesh.

On 15 September 2026, researchers identified an exposed VPS at `66.179.31[.]191`, hosted on AS399629, that exposed a Python SimpleHTTP directory on TCP/8898. The directory reportedly contained approximately **395 files across nine subdirectories totaling approximately 182 MB**. The recovered material included vulnerability-exploitation scripts, credential-testing tools, session cookies, target lists, C2 configurations, payload-related artifacts and operational logs.

The recovered toolkit included exploitation capability against **GeoServer/GeoTools, Laravel Ignition, Apache Tomcat Manager and Redis**, as well as weak-credential testing against phpMyAdmin. The infrastructure also contained **Sliver and Vshell**, an out-of-band callback service and reverse-shell tooling. Operational logs reportedly showed active scanning, exploitation activity and interactive shell access.

The research identified Bangladesh government infrastructure within recovered target lists and, more significantly, several Bangladesh government-related phpMyAdmin endpoints in a credential-testing script. However**, presence in a target list or credential-testing list must not be interpreted as confirmed compromise**. The researchers explicitly distinguish broad reconnaissance from the smaller set of systems for which active exploitation evidence was recovered.

The tooling, infrastructure and victimology reportedly overlap with publicly documented SideWinder tradecraft. Nevertheless, the available evidence does not conclusively establish attribution to SideWinder or a state sponsor. BGD e-GOV CIRT therefore recommends treating the activity as a high-priority threat-hunting lead rather than as confirmed attribution.

Key Findings

Finding	Details
Primary infrastructure	66.179.31[.]191
Hosting	AS399629 / BL Networks
Reported location	Singapore
Open directory	TCP/8898
Exposed material	~395 files / 9 directories / ~182 MB
C2 framework	Sliver
C2 port	TCP/31337
Additional C2	Vshell
Vshell listener	TCP/8099
Vshell management	TCP/8082
OOB callback	TCP/14333
GeoServer/GeoTools	CVE-2026-76904 exploitation tooling
Laravel	CVE-2021-3129 exploitation tooling
Tomcat	Manager/WAR/JSP webshell attack chain
Redis	Malicious module-based RCE
phpMyAdmin	Weak/default credential testing
Bangladesh relevance	Bangladesh government systems appear in target and credential-testing material
Confirmed government compromise elsewhere	Root-shell activity against infrastructure associated with Nepal was reported
Attribution	Suspected SideWinder overlap; not confirmed

Threat Overview

The reported operation demonstrates a relatively broad attack infrastructure rather than dependence on a single exploit. The observed operational model can be represented as:

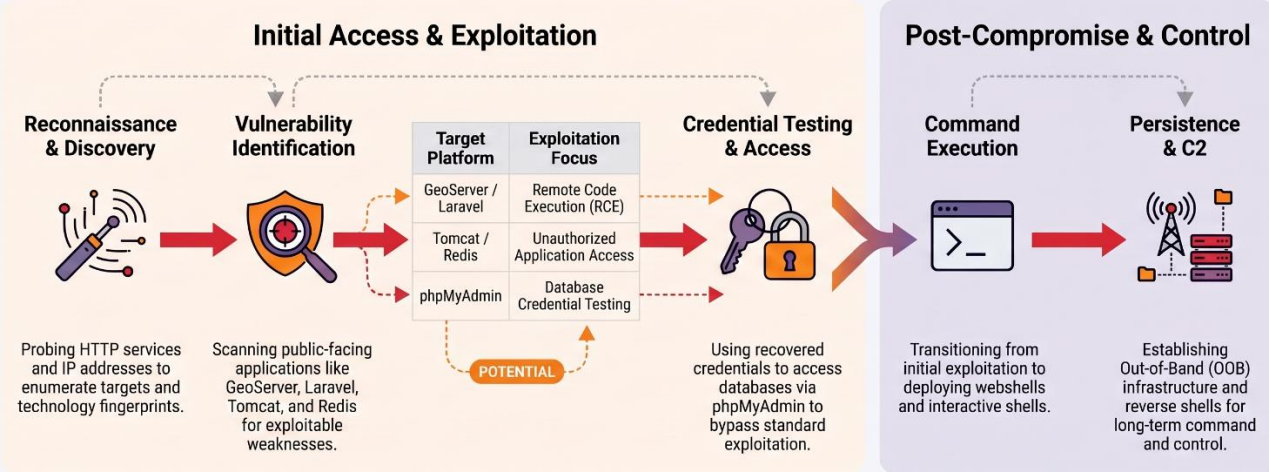

Figure: SideWinder-associated attack lifecycle against South Asian Internet-facing infrastructure

Attacker Infrastructure

The primary VPS identified in the research was:

- 66.179.31[.]191
- AS399629
- BL Networks

The host exposed multiple services over different periods. Researchers reported:

- SSH — TCP/22
- TLS — TCP/8443
- HTTP — TCP/8082
- Vshell — TCP/8099
- Redis-related service — TCP/6666
- Open directory — TCP/8898
- additional services on TCP/8877, 17765 and 25777.

The open directory was exposed through a Python SimpleHTTP server on TCP/8898.

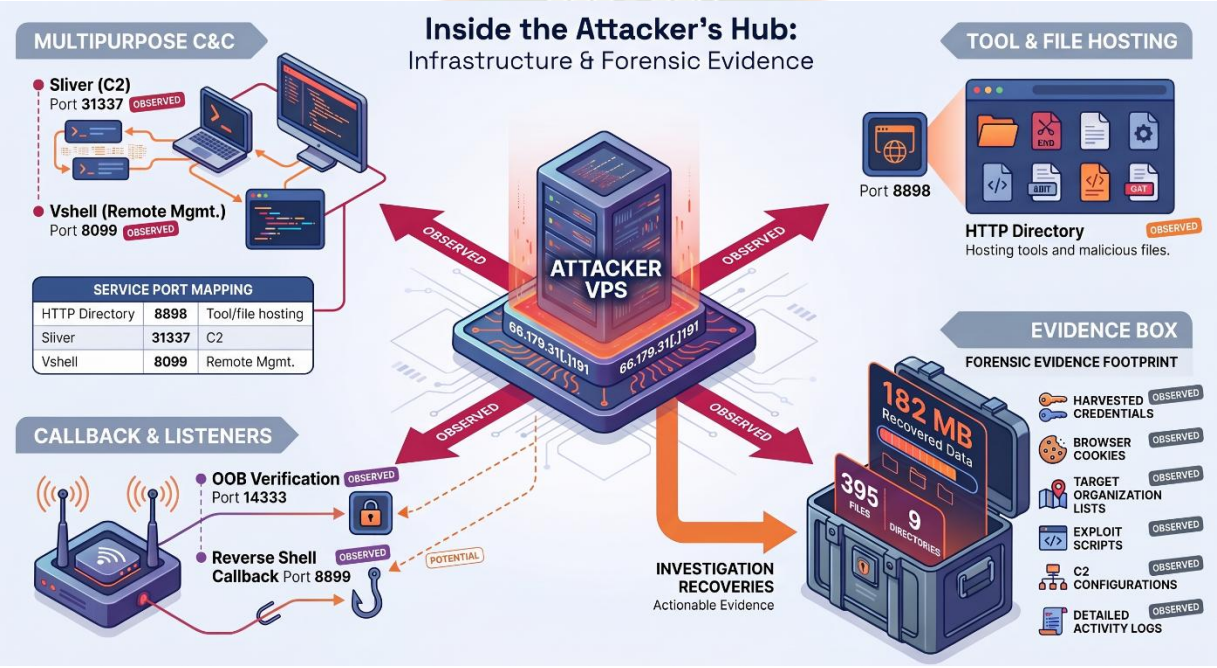

Figure: Reported services and operational components associated with `66.179.31[.]191`

Infrastructure Build-Out Timeline

Researchers reported that the host's services appeared in several waves:

Date	Observed activity
25 May 2026	SSH/TCP 22 first observed
05 Sep 2026	TLS/TCP 8443

06 Sep 2026	8443 no longer observed
09 Sep 2026	HTTP/TCP 8082
10 Sep 2026	Vshell-related TCP/8099
13 Sep 2026	TCP/6666, 8877, 8898, 17765, 25777

Researchers interpreted this clustering as consistent with a host being actively assembled during the observed period.

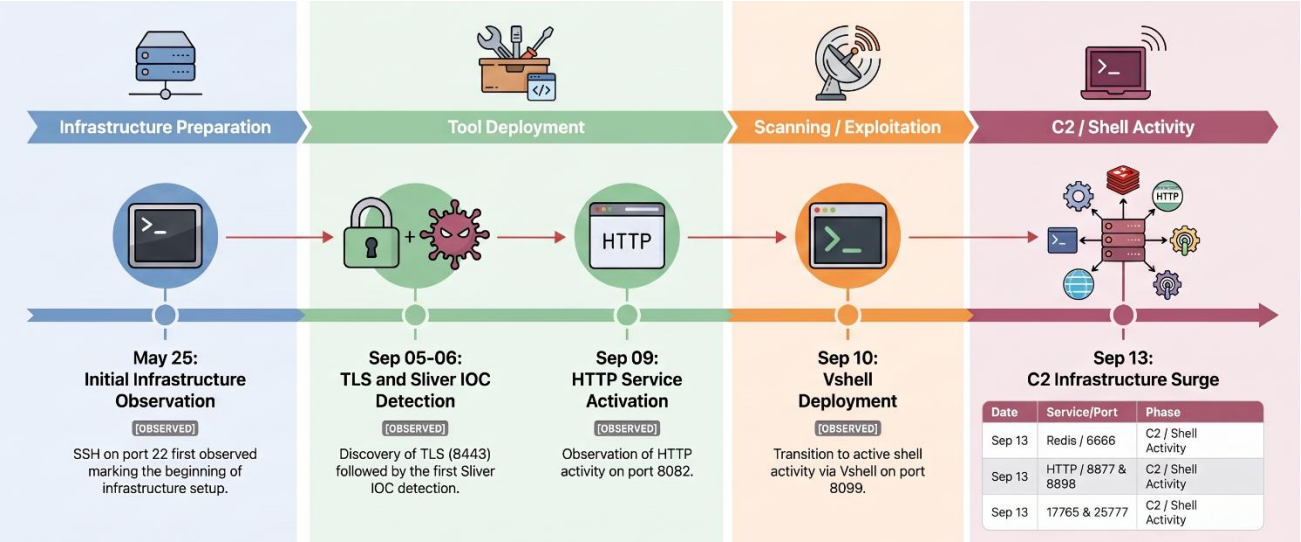

Figure: Infrastructure Build-Out Timeline

Open Directory Exposure

The exposed directory contained approximately 395 files distributed across nine directories.

The researchers categorized the material broadly as:

- exploit scripts;
- target lists;
- credential files;
- session cookies;
- C2 configurations;
- post-exploitation components;
- scanning tools;
- operational logs.

The directory was accessible through the SimpleHTTP server on TCP/8898.

Security significance

The combination of exploit code and operational artifacts provides insight into:

- target discovery;
- vulnerability selection;

- credential testing;
- exploitation;
- C2 deployment;
- post-exploitation;
- operator activity.

Exploitation Toolkit

The recovered toolkit covered multiple technologies.

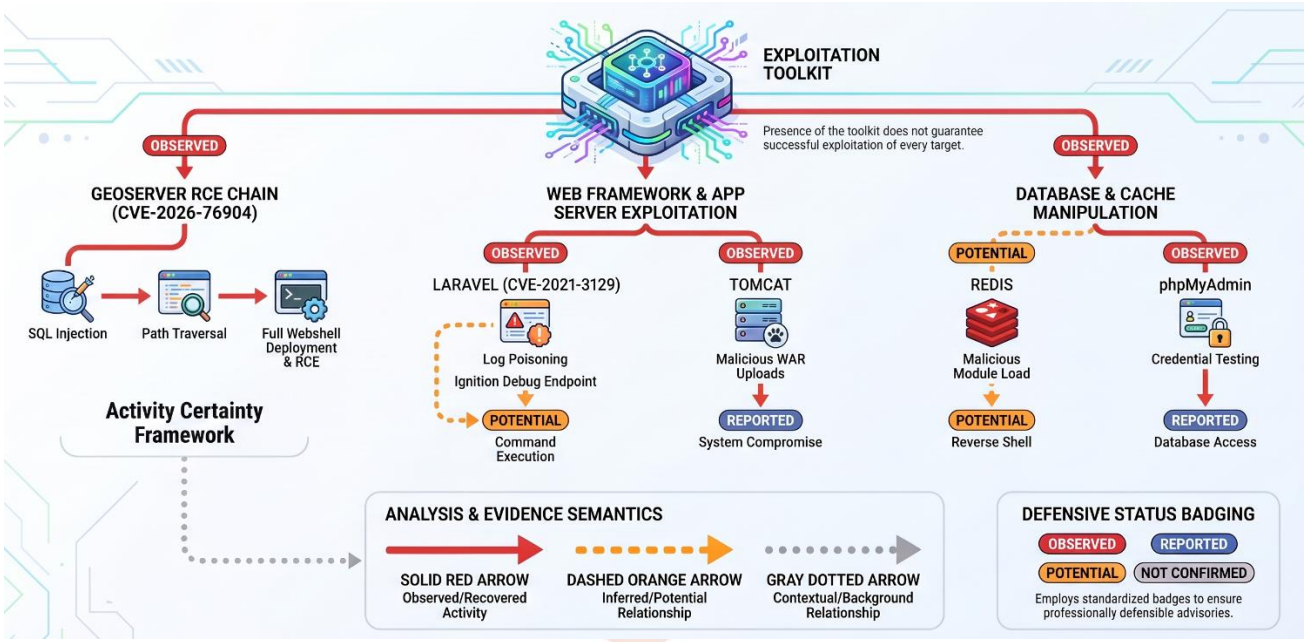

Figure: The recovered toolkit covered multiple technologies.

GeoServer / GeoTools Exploitation

The recovered infrastructure contained an exploit chain targeting **CVE-2026-76904**, described by the researchers as a critical SQL injection vulnerability in GeoTools' jsonArrayContains functionality.

The research states that the vulnerability is present in affected GeoTools versions and can be reached through GeoServer deployments using relevant PostGIS-backed functionality.

The recovered scripts included:

- `cve76904.py`;
- `geoserver_xxe.py`;
- `geoserver_deep_exploit.py`;
- `geoserver_master_exploit.py`;
- `geoserver_rce.py`;

- geoserver_reset_pg.py;
- geoserver_rest_exploit.py;
- geoserver_admin_full.py;
- geoserver_sqlview.py.

The toolkit reportedly covered multiple stages including:

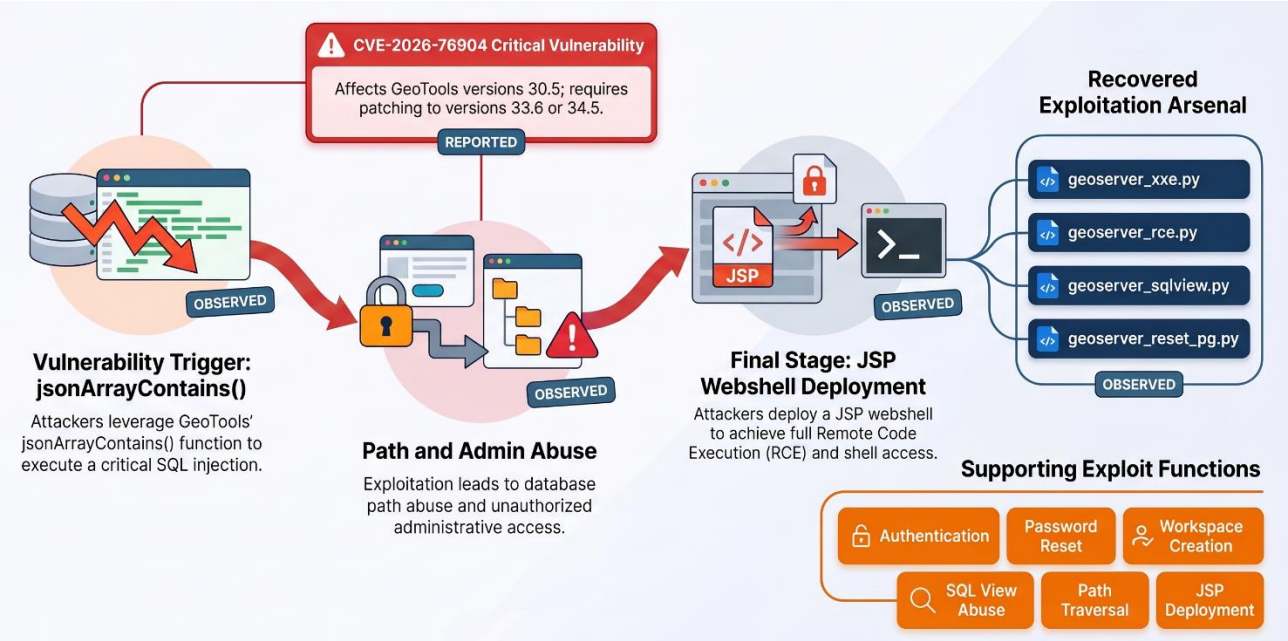

Figure: GeoServer/GeoTools Exploitation Chain (from SQLi to RCE)

Laravel Ignition Exploitation

The toolkit also contained scripts targeting CVE-2021-3129, involving Laravel applications with vulnerable Ignition debug functionality.

The research describes the chain as abusing the: `/_ignition/execute-solution` endpoint to write attacker-controlled content and subsequently achieve code execution under vulnerable conditions.

Recovered files included:

- ignition_auto.py
- ignition_exploit.php
- debug_ignition.py
- debug_targets.py
- find_writable.py
- write_2step.py
- write_final.py
- write_targets.py.

Apache Tomcat Manager Abuse

The recovered toolkit contained a separate Tomcat attack chain. The researchers characterize this as **post-authentication abuse**, rather than a specific Tomcat vulnerability.

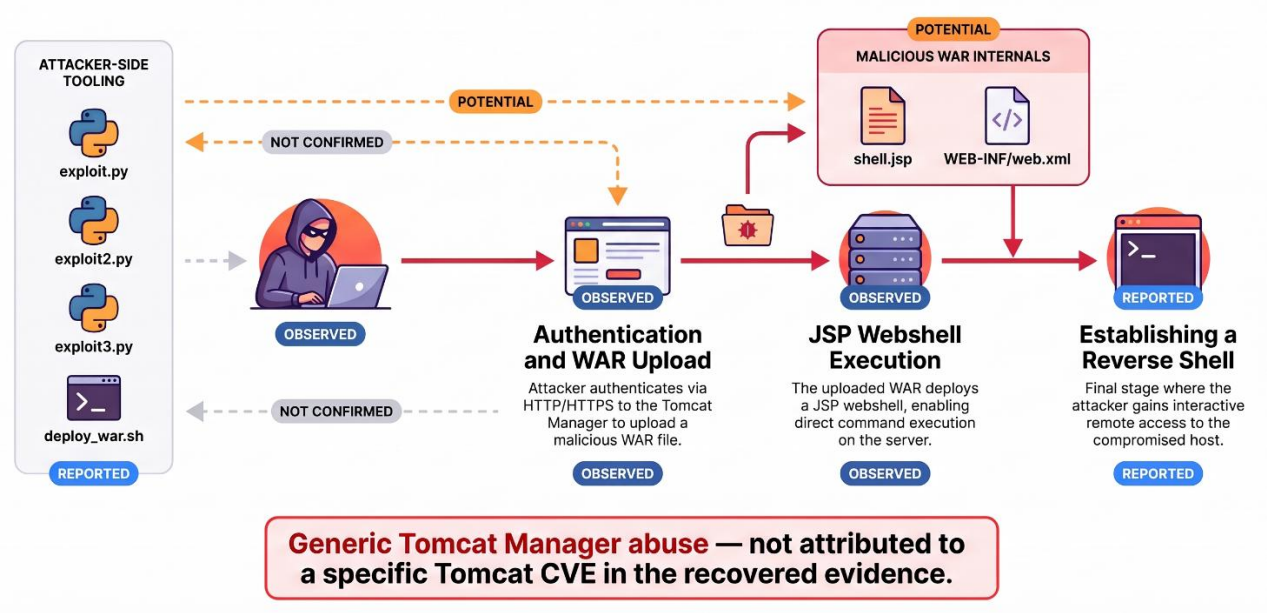

Figure: Tomcat Manager WAR/Webshell Deployment

Redis Module-Based RCE

The recovered Redis tooling included:

- `build_module.sh;`
- `build.sh;`
- `deploy_module.py;`
- `system.so;`
- `evil.c;`
- `listener.sh.`

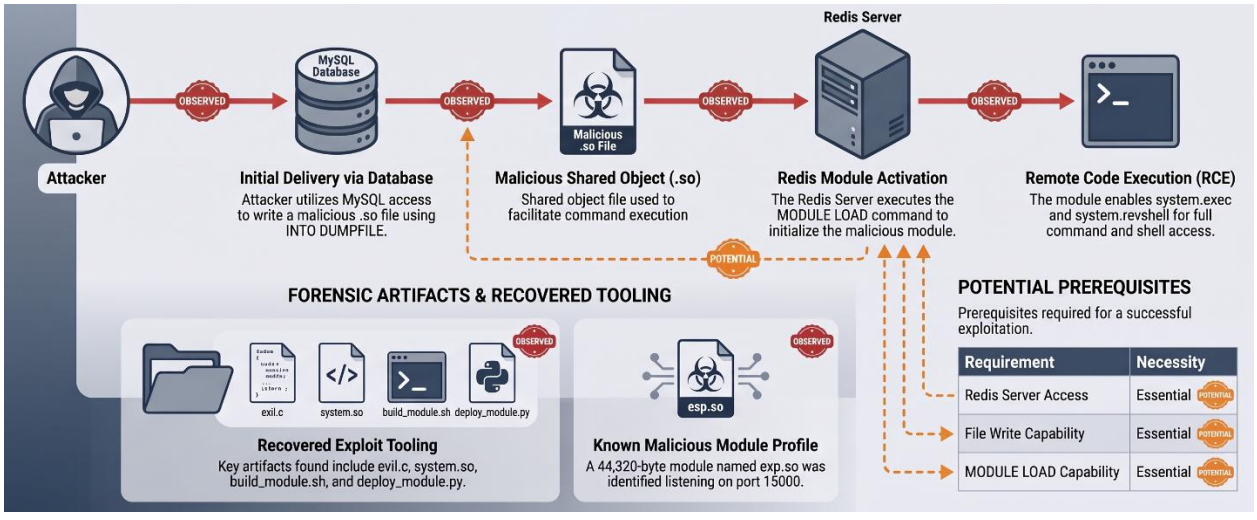

Figure: Redis module-based post-exploitation chain

The researchers report that the malicious Redis module exposed functions associated with command execution and reverse-shell functionality. A reported delivery chain used MySQL `INTO DUMPFILE` to place the module before loading it through Redis module functionality.

phpMyAdmin Credential Testing

The recovered `pma_brute.py` script reportedly tested weak or default credentials against five recovered phpMyAdmin targets.

The list included **Bangladesh** and **Pakistan** government-related infrastructure. This demonstrates that the activity was not exclusively based on exploitation of high-severity vulnerabilities.

The operational model included:

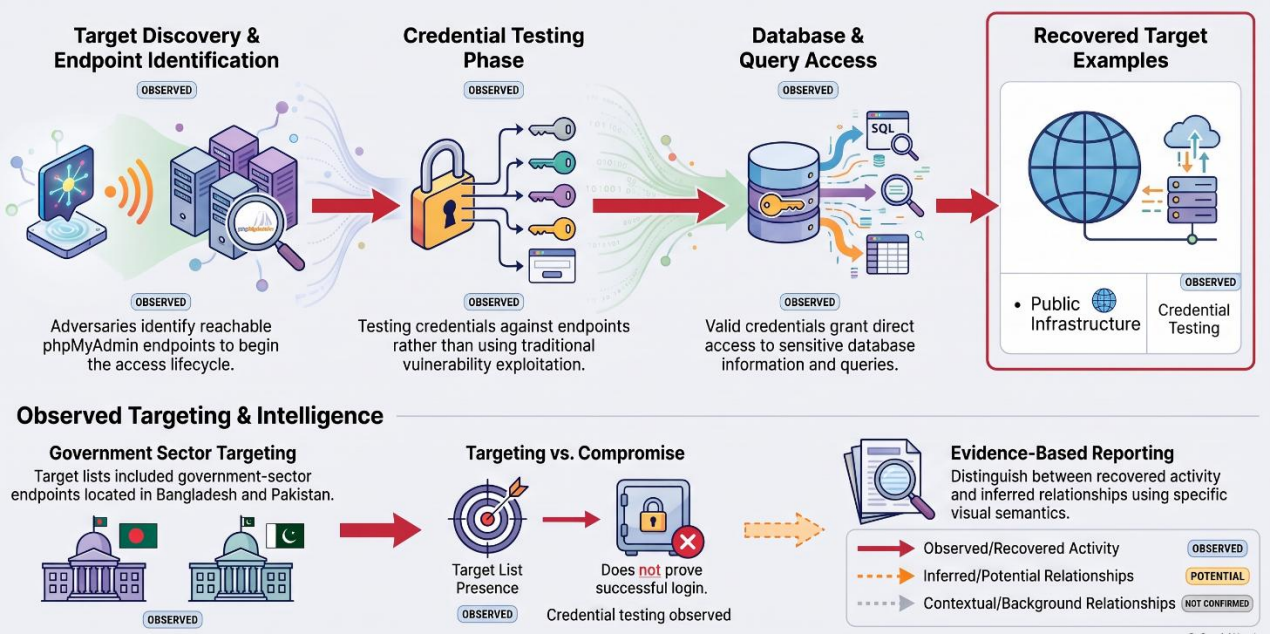

Figure: phpMyAdmin Credential-Based Initial Access

Credential and Session Material

The exposed directory reportedly contained multiple cookie files in Netscape cookie-jar format, including:

- `dcbuner_db.txt`
- `dcbuner_j4.txt`
- `dcbuner_jar2.txt`
- `energy_cookies.txt`
- `hr_cookies.txt`
- `hr_kp_c.txt`
- `hr_kp_login_cookies.txt`

- `hr_login_cookies.txt`
- `hr_pma_cookies.txt`
- `forged_headers.txt`

The research also identifies icc_app_config.txt as containing plaintext database, Kafka, Redis and Elasticsearch credentials and embedded key material.

Reconnaissance and Vulnerability Scanning

The recovered `batch_runner.log` reportedly recorded repeated use of `pdhttpx`, a bulk HTTP probing tool. The infrastructure also contained references to Nuclei templates for:

- `tpl_cpanel_whm.txt`
- `tpl_laravel.txt`

The template content itself was reportedly not recovered. The reconnaissance model was:

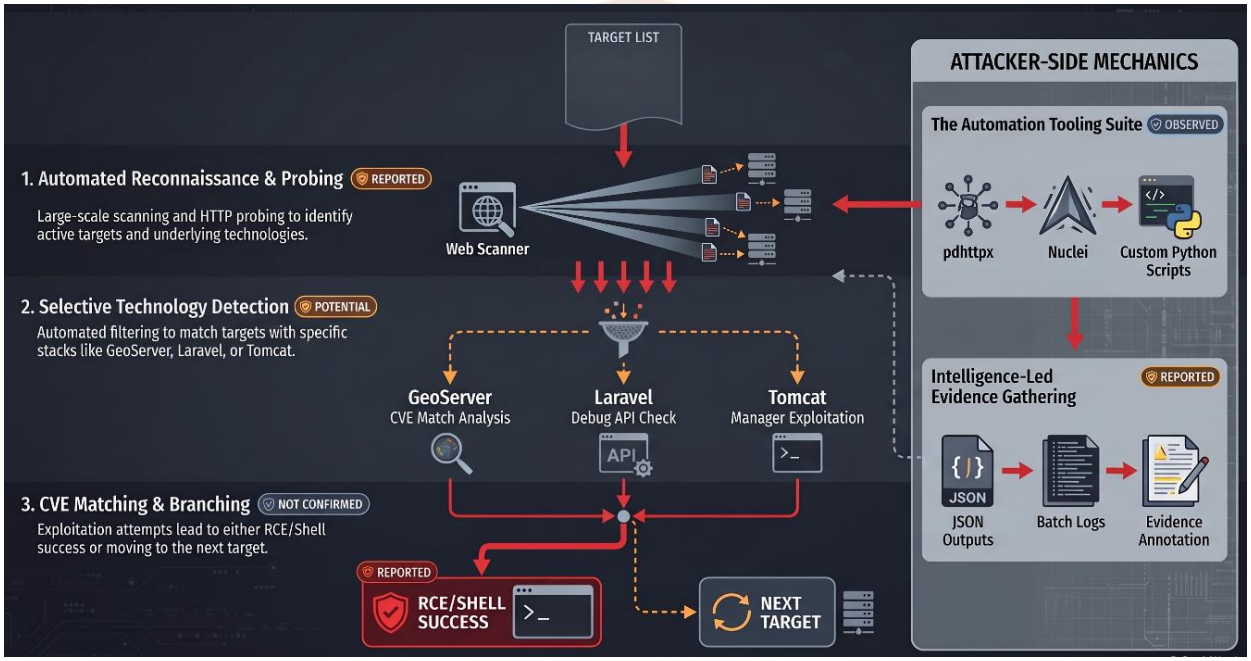

Figure: Automated reconnaissance and exploitation-selection workflow

Out-of-Band Exploitation Verification

The attacker infrastructure reportedly contained a persistent OOB callback server.

`deploy_oob.sh` installed a systemd service running `oob_server.py` on TCP/14333, with callback information written to:

`/var/log/oob/callbacks.log`

The conceptual workflow is:

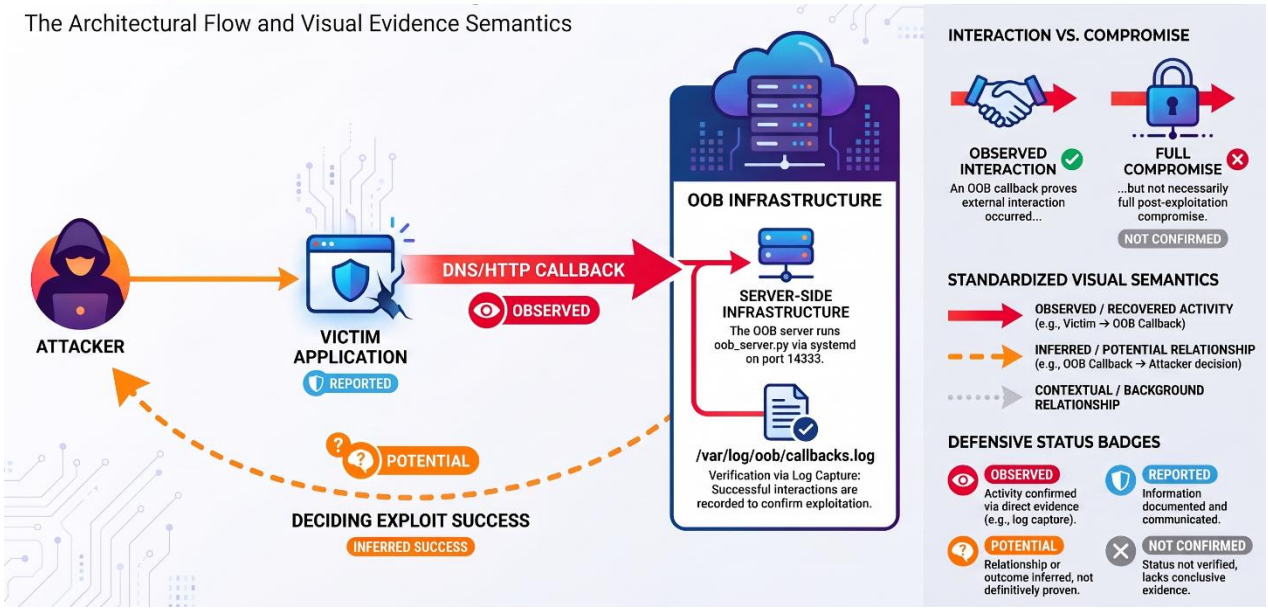

Figure: Out-of-band exploitation verification architecture

Operational Logs

Several recovered logs reportedly indicate operational use:

`batch_runner.log`: Repeated bulk HTTP probing activity.
`rogue.log`: Redis exploitation activity, including malicious shared-object loading and connections from `119.45.14[.]15`.
`nc_rev.txt`: Netcat listener activity associated with `115.89.253[.]189`.
`httpserver.log`: A request for `/linux_beacon_new` from `150.158.85[.]137`.
`shell_16653.log`: An interactive root-shell session associated with a connection from `103.69.124[.]253`.

These artifacts provide stronger evidence of operational activity than the presence of exploit scripts alone.

Reported Root-Shell Activity Against a Govt. Infrastructure

The researchers report that shell_16653.log recorded a reverse-shell callback resulting in an interactive root shell.

The reported target was: `103.69.124[.]253:8070`

The research associates the IP with AS45353/NITC infrastructure and states that a government-related login portal was observed on the address.

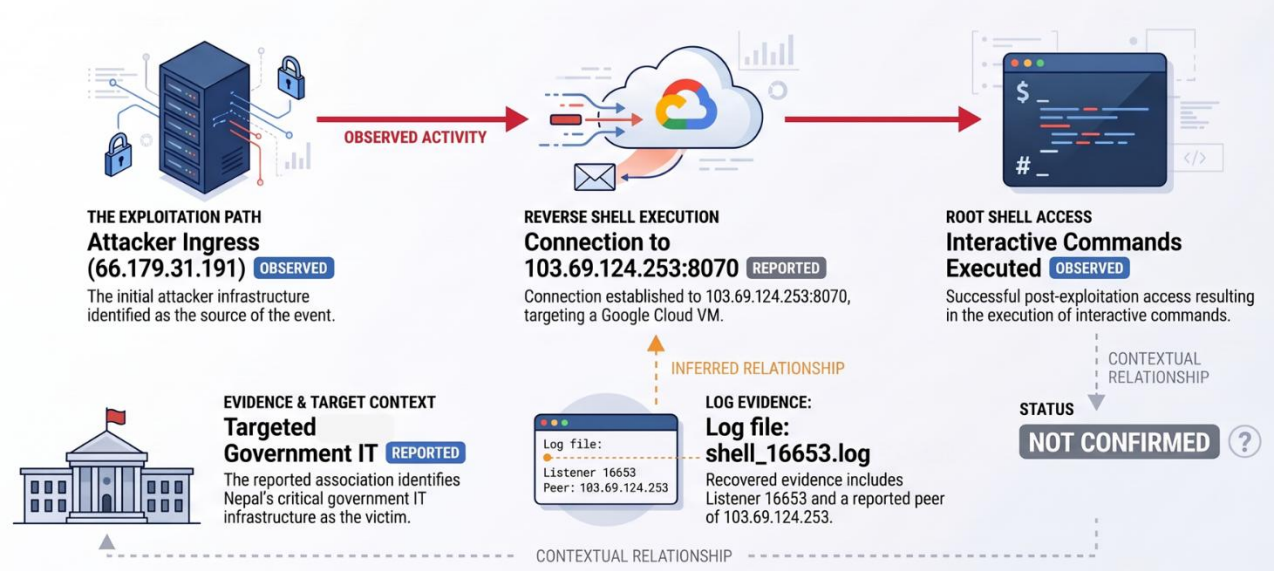

Figure: Reported Root-Shell Event Against a Govt. Infrastructure

Command-and-Control Infrastructure

Two major C2 frameworks were reportedly staged:

Sliver

Recovered configuration reportedly contained:

- operator alias: `wren;`
- LHOST: `66.179.31[.]191;`
- LPORT: `31337;`
- certificate material;
- operator configuration;
- implant-generation capability.

The implant naming convention included `linux_beacon` and an associated request `/linux_beacon_new` was observed in operational logs.

ThreatFox currently lists `66.179.31.191:31337` as a Sliver-related IOC with 75% confidence, first seen 6 September 2026.

Vshell

The researchers report:

- Vshell listener: TCP/8099;
- web management interface: TCP/8082;
- associated tooling;
- multi-architecture staging capability.

Fallback Reverse-Shell Infrastructure

The recovered infrastructure reportedly included additional reverse-shell mechanisms beyond Sliver and Vshell.

The research identifies:

```
LD_PRELOAD reverse shell + Netcat listener + Sliver + Vshell
```

The `evil.c` component reportedly contained a constructor that initiates a Bash reverse shell toward: `66.179.31[.]191:8899`. A separate listener script provided a netcat-based fallback mechanism.

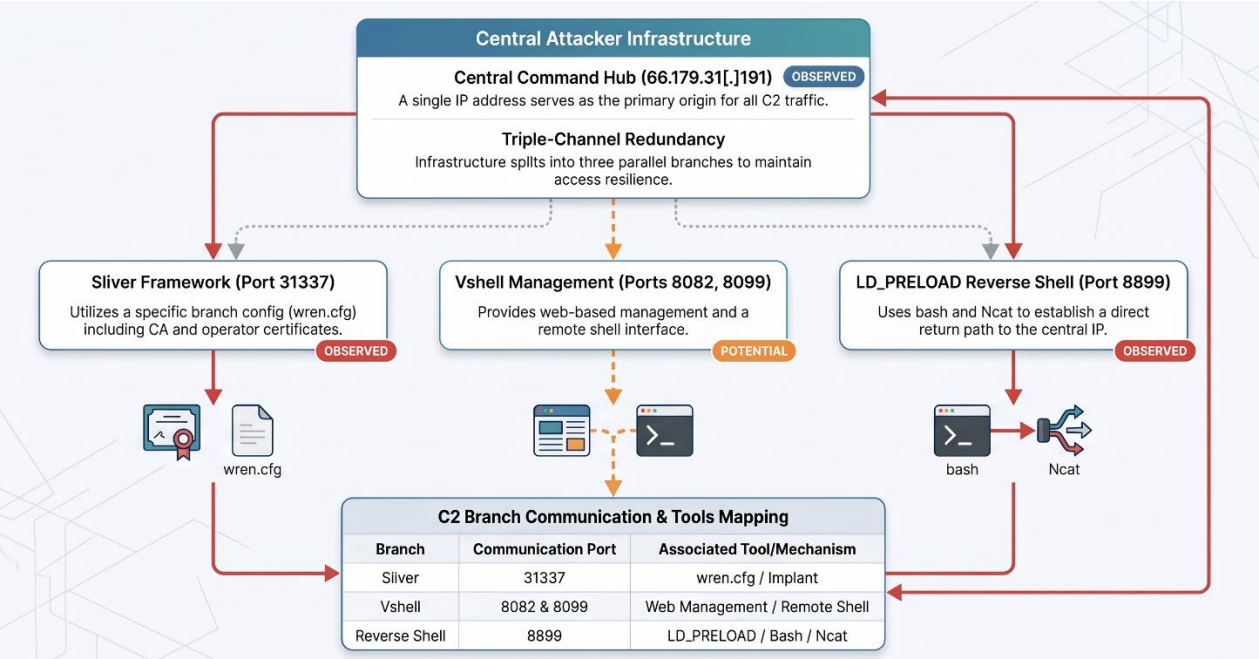

Figure: Multi-Channel C2 Architecture

Bangladesh-Specific Relevance

The Bangladesh portion of the recovered targeting material includes categories such as:

- defence-related infrastructure;
- security organizations;
- government ministries;
- cabinet-related infrastructure;
- revenue/tax systems;
- healthcare authorities;
- municipal and district-level systems.

The research notes that a significant portion of the Bangladeshi entries are UUID-prefixed municipal/district subdomains that appear to have been enumerated rather than individually selected.

More importantly, `pma_brute.py` reportedly contained five Bangladesh/Pakistan government-related phpMyAdmin targets, including Bangladesh government domains.

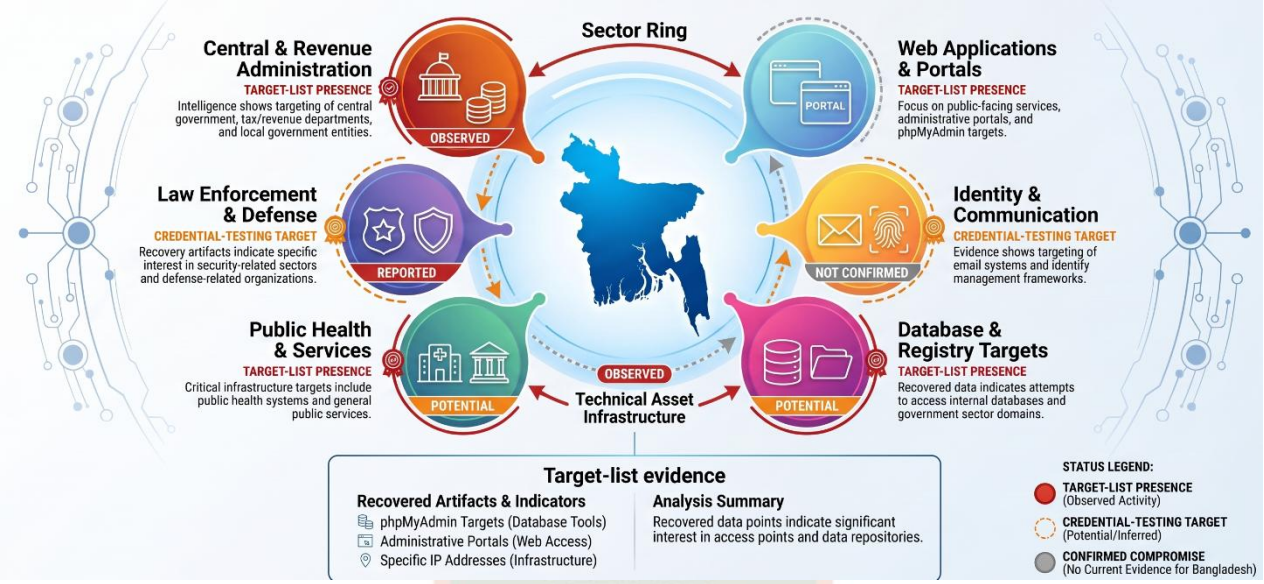

Figure: Reported categories of Bangladesh-related infrastructure targeting

MITRE ATT&CK Mapping

Tactic	Technique	ID	Observed/Reported Evidence
Reconnaissance	Active Scanning: Vulnerability Scanning	T1595.002	`pdhttpx`, Nuclei references
Initial Access	Exploit Public-Facing Application	T1190	GeoServer/GeoTools, Laravel, Tomcat, Redis
Execution	Command and Scripting Interpreter	T1059	Python/Bash/JSP tooling
Persistence	Create or Modify System Process: Systemd Service	T1543.002	OOB callback service
Credential Access	Brute Force	T1110	phpMyAdmin credential testing
Credential Access	Unsecured Credentials	T1552	Plaintext configuration credentials
Command & Control	Multi-Stage Channels	T1104	staging/loader activity
Command & Control	Ingress Tool Transfer	T1105	payload/module transfer
Defense Evasion	Indicator Removal	T1070	cleanup of interaction tooling

Indicators of Compromise (IoC)

Network Indicators

Type	Indicator	Role / Context
IPv4	66.179.31[.]191	Reported attack infrastructure
IPv4:Port	66.179.31[.]191:31337	Sliver C2
IPv4:Port	66.179.31[.]191:8898	Open directory
IPv4:Port	66.179.31[.]191:14333	OOB callback server
IPv4:Port	66.179.31[.]191:8099	Vshell listener
IPv4:Port	66.179.31[.]191:8082	Vshell management
IPv4:Port	66.179.31[.]191:8899	Reported reverse-shell destination
IPv4	119.45.14[.]15	Peer associated with Redis activity
IPv4:Port	103.69.124[.]253:8070	Reported Nepal target associated with root-shell event
IPv4	115.89.253[.]189	Netcat reverse-shell peer
IPv4	150.158.85[.]137	Source of /linux_beacon_new request

Host / File Indicators

Indicator	Type	Context
wren.cfg	Configuration	Sliver operator profile
linux_beacon	Implant naming	Sliver-related naming
/linux_beacon_new	HTTP path	Associated beacon request
system.so	Shared object	Redis module
evil.c	Source artifact	Reverse-shell component
slt_public.sh	Shell script	Reported multi-architecture stage loader
deploy_oob.sh	Shell script	OOB callback service
oob_server.py	Python	OOB callback server
pma_brute.py	Python	phpMyAdmin credential testing
cve76904.py	Python	GeoTools exploitation
debug_ignition.py	Python	Laravel exploitation
batch_runner.log	Log	Bulk HTTP probing
rogue.log	Log	Redis exploitation
shell_16653.log	Log	Reverse-shell/root-shell activity

Indicators of Attack — Behavioral Hunting

Static IoCs should be supplemented with behavioral detection.

IoA	Detection Logic
Bulk HTTP probing	One source rapidly probes many URLs/hosts
Vulnerability-specific probing	Requests targeting GeoServer/Laravel/Tomcat functionality
phpMyAdmin credential spraying	Multiple authentication attempts across accounts/hosts
Tomcat WAR deployment	New WAR followed by JSP execution
Web process spawning shell	`java/php/nginx/apache → bash/sh`
Redis module loading	Redis → unexpected `.so`
Redis reverse connection	Redis host initiating unexpected external connection
New systemd service	Service created shortly after exploitation
LD_PRELOAD modification	Unexpected loader/persistence changes
Sliver C2	Connection to reported infrastructure/behavioral indicators
Vshell C2	Unexpected persistent listener/client behavior
OOB callback	Server unexpectedly contacting external callback infrastructure
Root shell	Web/database service followed by privileged shell
Credential reuse	Recovered credentials used from unusual infrastructure

Detection and Threat Hunting

Internet-Facing Applications

Organizations should identify: (Prioritize systems exposed directly to the Internet)

- GeoServer/GeoTools;
- Laravel;
- Apache Tomcat;
- Redis;
- phpMyAdmin;
- cPanel/WHM;
- other externally accessible administrative applications.

Web Application Hunting

Search for:

- suspicious GeoServer requests;
- abnormal SQL-related errors;
- Laravel `/_ignition/` requests;
- unexpected Tomcat Manager access;
- WAR deployment;
- unexpected JSP creation;
- unexpected PHP files;

- webshell behavior

Redis Hunting

Monitor for: (Any Internet-exposed Redis service should receive immediate review)

Redis

```
|
├— Unexpected MODULE LOAD
├— New .so file
├— Process creation
├— Reverse connection
└— Internet-originated administration
```

Linux Host Hunting

Look for:

- recently created systemd services;
- unexpected `.so` files;
- `LD_PRELOAD` configuration changes;
- `bash` spawned by web/database processes;
- `nc`/netcat listeners;
- unusual outbound connections;
- unknown Python scripts;
- unexpected files under `/tmp`;
- unexplained root shells.

Detection & Correlation Model

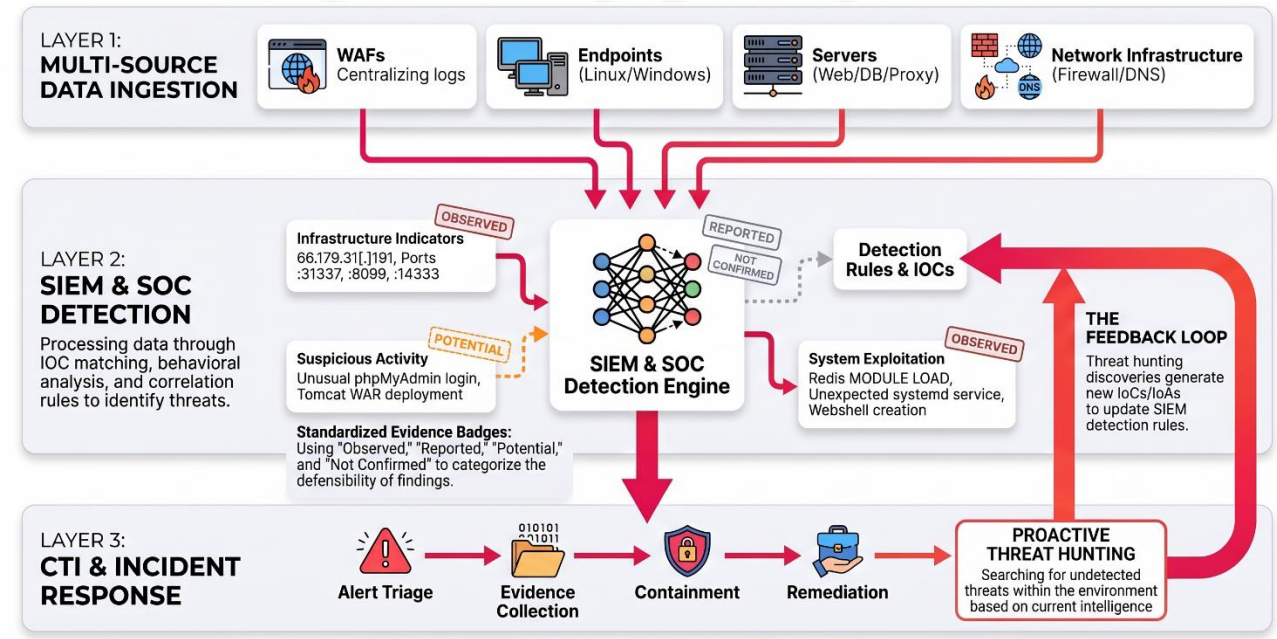

Figure: Detection & Correlation Architecture

Recommended Actions

Organizations should prioritize the following activities:

- Identify all Internet-facing GeoServer/GeoTools deployments.
- Verify GeoTools/GeoServer versions and patch status.
- Identify Laravel applications using vulnerable Ignition versions.
- Confirm Laravel production debug mode is disabled.
- Identify Internet-accessible Tomcat Manager interfaces.
- Review Tomcat Manager authentication logs.
- Identify Internet-exposed Redis services.
- Search for unexpected Redis module loading.
- Identify Internet-accessible phpMyAdmin installations.
- Review phpMyAdmin authentication failures and successful logins.
- Search DNS, firewall, proxy, NDR and EDR telemetry for `66.179.31[.]191`.
- Search for connections to TCP/31337, 8082, 8099, 8898 and 14333.
- Review outbound connections from web and database servers.
- Search for unexpected JSP/PHP/WAR/shared-object files.
- Search Linux hosts for recently created systemd services.
- Search for `linux_beacon` and `/linux_beacon_new`.
- Review root-level shell activity.
- Hunt for suspicious nc, bash, Python or shell processes spawned by application services.
- Review credentials and session cookies associated with affected systems.
- Rotate credentials if exposure is suspected.

If suspicious activity is identified:

- Containment: Isolate affected hosts, restrict external access, preserve evidence, and block malicious infrastructure.
- Evidence Collection: Collect application, web, authentication, EDR/NDR, firewall, systemd, process, network, and suspicious-file data.
- Credential Protection: Rotate application, database, API, administrator, and session credentials.
- Eradication: Remove webshells, malicious modules/services, unauthorized accounts and tools; patch vulnerabilities and disable unnecessary services.
- Recovery: Rebuild compromised systems where necessary, restore from trusted sources, validate configurations, and increase SIEM/EDR/NDR monitoring.
- Identify additional accounts targeted through internal messaging or impersonation, as compromised accounts may have been used to facilitate subsequent social engineering.

References

- https://akatsukilegion.com/post.php?slug=suspected-sidewinder-campaign-against-south-asian-governments-and-finance-targets
- https://www.cirt.gov.bd/advisories/sidewinder-spear-campaign
- https://threatfox.abuse.ch/ioc/1902081/
- https://nvd.nist.gov/vuln/detail/cve-2021-3129