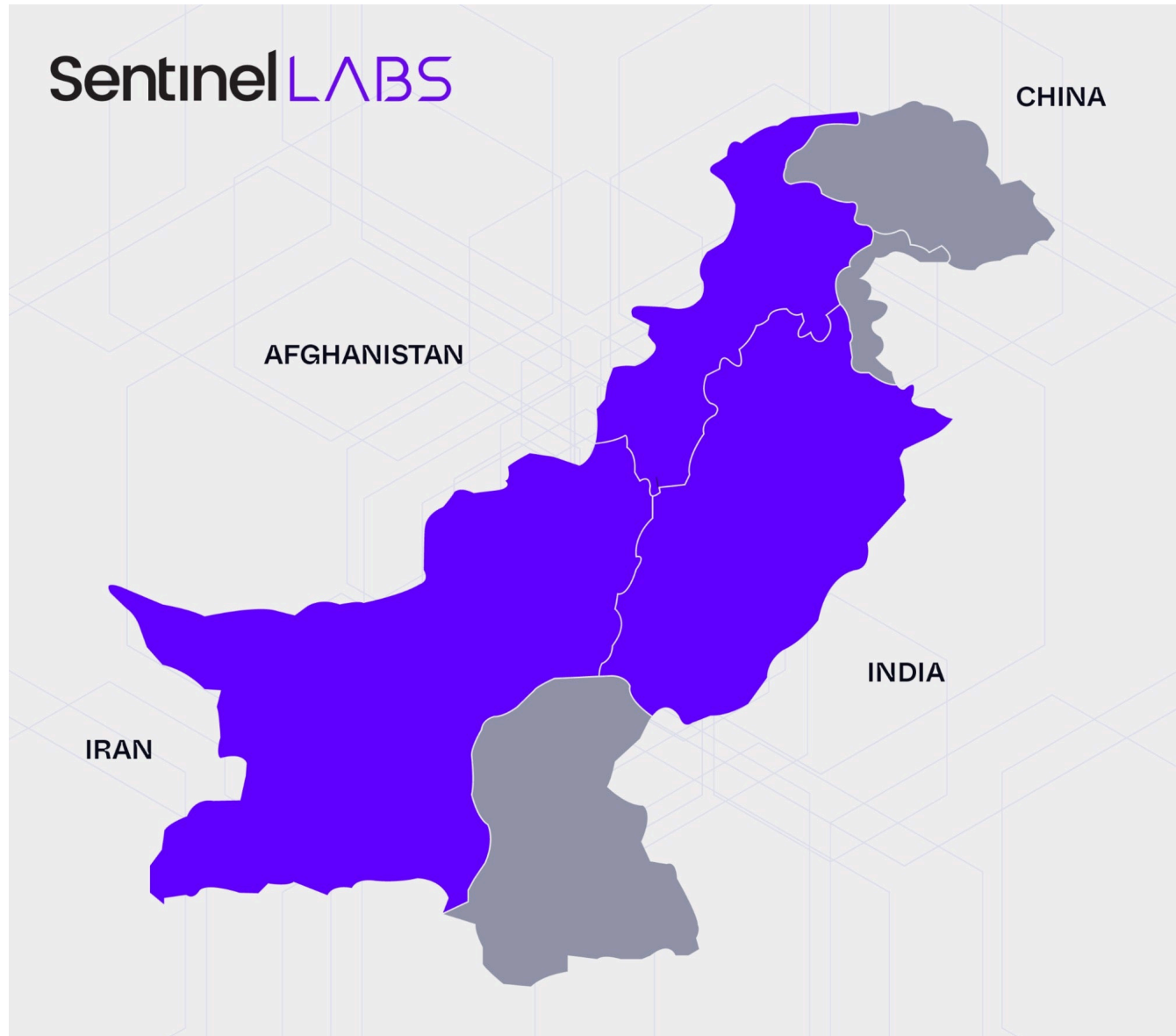


One Target, Two Flags | Rival Espionage Actors Converge On Pakistani Law Enforcement

 sentinelone.com/labs/one-target-china-india-espionage-converge-on-pakistani-law-enforcement

Aleksandar Milenkoski

July 9, 2026



Pakistani provinces with affected law enforcement organizations

Executive Summary

- SentinelLABS has been tracking sustained cyberespionage activity against several Pakistani law enforcement organizations, taking place from February 2024 to April 2026.

- All these actors converged on Balochistan Police over this period, bringing both a partner and an adversary of Pakistan to the same police force in a province shaped by a separatist insurgency and the regional tensions it has drawn in.
- At Balochistan Police, the compromised assets included servers hosting web applications that manage police and citizen data, such as criminal and biometric records.
- A suspected China-nexus actor planted implants in one of the web applications, which serves both police staff and citizens, weaponizing a tool of Pakistan's police digitalization against its users.
- Pakistani law enforcement organizations attract cyber collection because they hold information on Pakistan's internal security that regional powers have an incentive to pursue.
- For China, the likely primary concern is the safety of its nationals, the target of repeated deadly attacks Pakistan has failed to prevent, leading Beijing to assess that threat for itself rather than rely on its partner alone.
- For India, the strongest motive is probably its rivalry with Pakistan, with Balochistan Police offering insight into the security posture of a Pakistani province prominent in wider mutual accusations over cross-border support for militancy.

Overview

Suspected China- and India-nexus threat actors carried out intrusions into several Pakistani law enforcement organizations between 2024 and 2026. Our analysis of C2 netflow data revealed that suspected China- and India-nexus threat actors operating PlugX, ShadowPad, Cobalt Strike, and Remcos infrastructure have converged on this victim class.

All of these threat actors were active against Balochistan Police, the principal police force serving the Pakistani province of the same name, at various points between 2024 and 2026. The affected assets spanned network appliances and servers hosting web applications that manage biometric records, hotel and tenant registrations linked to national identity records, criminal case files, and personnel records. A suspected China-nexus threat actor also compromised one of these web applications, deploying custom implants masquerading as a portal update. The application is used by police staff and by citizens interacting with law enforcement through it, and the compromise put both user groups within the threat actor's reach.

When multiple cyberespionage actors operate against law enforcement institutions of a single state, the convergence itself is a signal of target value. What draws them is a particular kind of institution: one that holds the government's internal security picture, what it knows about the threats inside its borders, and how it acts against them. Each of the states suspected to be

behind the activities covered in this post has its own stake in the threats monitored by Pakistani law enforcement.

Strategic Motives | Distrust and Accusations

The China-nexus activity is most likely motivated primarily by concern for the safety of Chinese nationals. Their presence across Pakistan is substantial, tied in large part to the China-Pakistan Economic Corridor (CPEC), Beijing's flagship Belt and Road infrastructure program in the country. Chinese nationals have been the target of repeated deadly attacks, some of which were claimed by the Balochistan Liberation Army (BLA), a Baloch separatist group opposed to China's presence in the Pakistani resource-rich southwest. Notable attacks include the [October 2024 Karachi airport attack](#) and the [March 2024 suicide bombing](#) in northwestern Pakistan.

The attacks have fueled explicit Chinese dissatisfaction with Pakistani counter-militancy performance. In October 2024, China's Ambassador to Pakistan [publicly called them "unacceptable"](#), warning that the security situation was the main obstacle to CPEC. The threat to Chinese nationals remains unresolved. As recently as January 2026, China's Minister of Public Security and Pakistan's Interior Minister [agreed to expand counterterrorism coordination](#), deepen police training exchanges, and establish a special unit in Islamabad to protect Chinese nationals.

Pakistani law enforcement is a natural collection target for China. The data it holds would let China assess the security environment its nationals face independently, rather than relying on a partner whose protection has repeatedly fallen short.

For the India-nexus activity, which was focused on Balochistan, the strongest motive is probably the adversarial security relationship between India and Pakistan, in which the province is a recurring flashpoint. Pakistan has [long accused](#) India of backing the Baloch insurgency, [describing the BLA](#) as an "Indian proxy", a charge it has not publicly substantiated and that India denies. India, in turn, accuses Pakistan of [backing the militant groups](#) behind attacks in Indian-administered Kashmir, which Pakistan denies.

The Baloch insurgency is a front in the antagonism between the two states, and Balochistan Police would hold the operational record of how Pakistan manages the province's security. For India, that material could offer visibility into a conflict at the center of the accusations and counter-accusations between them.

Balochistan Police is the same law enforcement institution the China-nexus actors were active against, approached from the opposite direction. To China, it is the police force of a partner that cannot be trusted to protect Chinese nationals in Balochistan. To India, it is the police

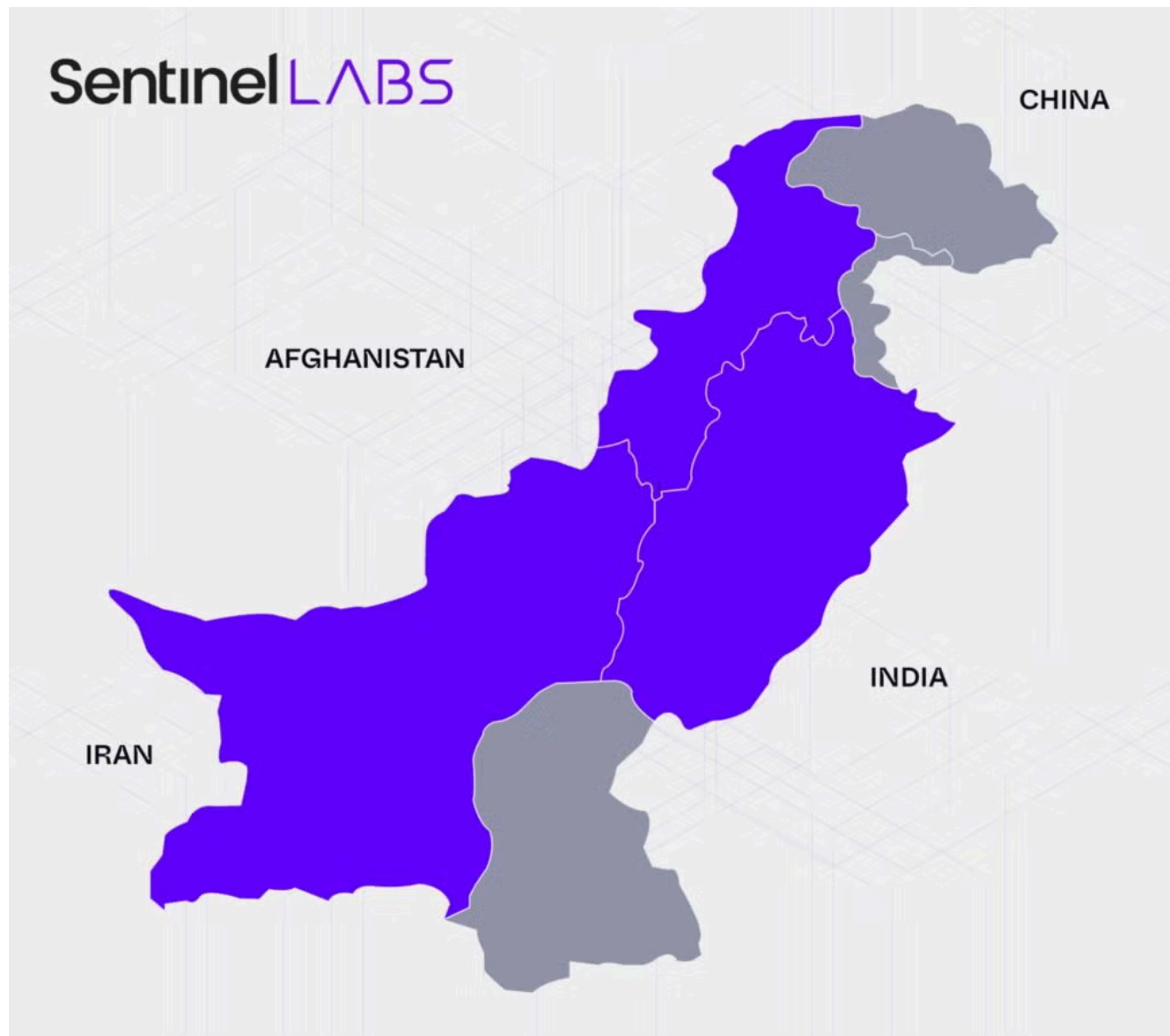
force of a rival, with deep insight into the security of a province central to the friction between the two states.

Intrusions Into Pakistani Law Enforcement Organizations

We observed the highest concentration of intrusions at Balochistan Police. They affected network appliances and web servers hosting several of its web applications, one of which, the Complaint Management System (CMS), drew particular attention. The next two sections discuss the impacted assets in greater detail.

We also identified compromised infrastructure associated with several other Pakistani law enforcement organizations:

- the Khyber Pakhtunkhwa Police, the police force of Khyber Pakhtunkhwa province;
- the Islamabad Police, which serves the Islamabad Capital Territory;
- the Punjab Safe Cities Authority (PSCA), an autonomous government body that operates the integrated command, control and communication system for the police in the major cities of Punjab province.



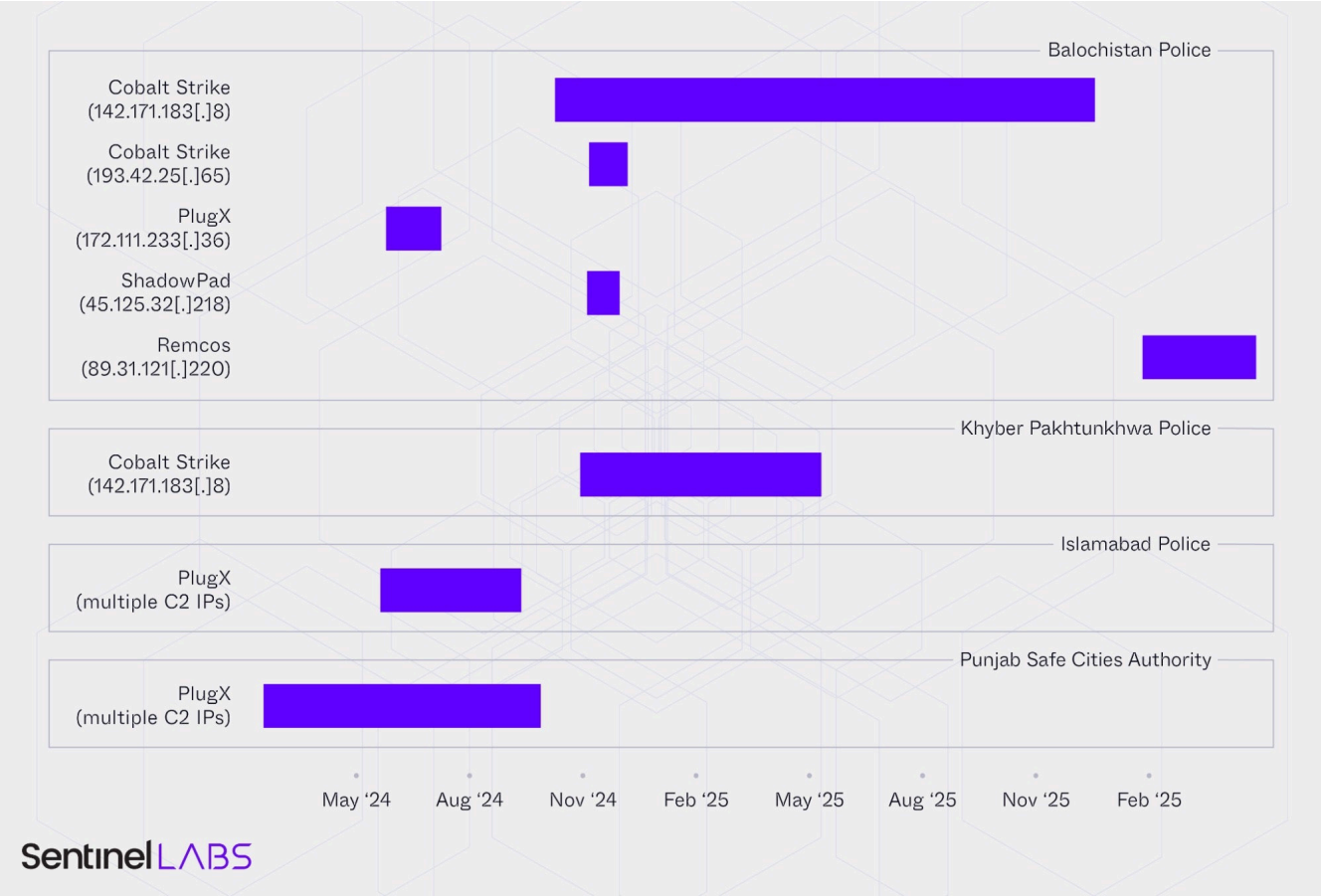
Pakistani provinces with affected law enforcement organizations

We group the C2 activity we observed against all these targets into four clusters, each associated with a single malware family or tool: PlugX, ShadowPad, Cobalt Strike, and Remcos.

Because we cluster based on tooling, not on actor attribution, the number of threat actors behind each C2 activity cluster differs. We associate the Remcos cluster with a single actor, while the PlugX, ShadowPad, and Cobalt Strike clusters are built on shared or commodity tooling and may each involve more than one operator.

The table below presents the constituent servers of each C2 activity cluster, along with the first and last dates on which any of its servers communicated with Pakistani law enforcement infrastructure. The figure that follows shows how each cluster's activity was distributed across the targeted organizations over time.

C2 activity cluster	C2 servers	First seen	Last seen
PlugX	172.111.233[.]36, 172.111.233[.]96, 172.111.233[.]12, 172.111.233[.]105, 172.111.233[.]26, 172.94.9[.]49, 172.94.9[.]43, 172.94.9[.]19, 45.74.6[.]17	27 February 2024	28 September 2024
ShadowPad	45.125.32[.]218	5 November 2024	29 November 2024
Cobalt Strike	142.171.183[.]8, 193.42.25[.]65	12 October 2024	5 December 2025
Remcos	89.31.121[.]220	13 January 2026	9 April 2026



Timeline of C2 traffic to Pakistani law enforcement organizations

The sections below cover the basis for each cluster's attribution and its broader victimology. The observation windows we present there are generally wider, spanning all per-cluster victims.

C2 Activity Cluster | PlugX and ShadowPad

PlugX and ShadowPad point to China-nexus cyberespionage groups on the basis of the tooling itself, since both are backdoors shared among multiple such groups. The victimology we observed for PlugX (between 27 February and 28 September 2024) and ShadowPad (between 3 August and 1 December 2024) reinforces this assessment.

Beyond Pakistani law enforcement, victimology for PlugX and ShadowPad includes government, foreign affairs, defense, nongovernmental, and research entities across South, Southeast, Central, and East Asia, the Arabian Peninsula, and Southeast Europe, consistent with China-aligned collection.

C2 Activity Cluster | Remcos

We attribute the Remcos C2 server 89.31.121[.]220 to a suspected India-nexus threat actor, which Recorded Future tracks as TAG-179. Its infrastructure, tooling, and TTPs overlap to varying degrees with those of the threat actors tracked by [Kaspersky](#) as Mysterious Elephant and by [Qihoo 360](#) as APT-C-08 (a.k.a. Bitter).

Our data shows that TAG-179 has been intensifying its activities and diversifying its TTPs since early 2025. This trend aligns with the prior research from Kaspersky and Qihoo 360, which documents in detail the tooling and infection chains used across 2025 and 2026.

Notably, Qihoo 360 describes a chain that delivers a Remcos backdoor configured with the same server that constitutes our Remcos C2 activity cluster (89.31.121[.]220). The IOC table of this report lists several lure files and backdoor components that we associate with TAG-179.

Among the lures is one with direct relevance to Pakistani law enforcement: it displays a decoy document posing as an operational plan for the repatriation of illegal foreigners, including Afghan Citizen Card (ACC) holders. These are Afghan nationals who have been granted temporary registration in Pakistan and are targeted for deportation under Pakistan's [Illegal Foreigners' Repatriation Plan](#).

The decoy document outlines coordination among district-level police forces, the National Database and Registration Authority (NADRA, an agency of the Pakistani Ministry of Interior), and Pakistani intelligence organizations. Its subject matter is consistent with the Pakistani law

enforcement victimology of TAG-179, making it an example of a plausible lure against this target class.

OPERATIONAL PLAN FOR REPATRIATION OF ILLEGAL FOREIGNERS –

The operational plan comprises of following major components:

1. District wise Identification / Mapping of ACC holders
2. Establishment of Transit / Holding Facilities
3. Holding of ACC holders at Transit Residential Facilities and Post Detention Management
4. Inter-Governmental (Provincial and Federal) and Inter-Agency Coordination & Monitoring Mechanism
5. Arrangements at International Border
6. Financial Implications

Sr.	Action	Responsibility
1.	DISTRICT WISE IDENTIFICATION / MAPPING OF ACC HOLDERS a. Mapping of all ACC holders and their families shall be carried out with Special Branch as the lead role. b. Real time data entry and sharing with all stake holders. c. Utilization of data available with FNSC Dashboard, SVAS and NADRA for the purpose of verification / identification. d. Constitution of ACC holders Identification Committees (ACCIC) at District level. e. The district level ACCIC may comprise of the following: i. Rep. of Spl. Br. ii. Rep. of CTD iii. Rep of ISI iv. Rep of MI v. Rep of IB vi. Reps of District Administration (Revenue + Local Government) vii. Rep of District Police viii. Rep of NADRA ix. Any other member deemed appropriate f. Provision of security cover to ACCIC. g. Preparation of lists of ACC holders to include information as mentioned in the prescribed format shared by Home Department.	DCs/DPOs/Special Branch District Intelligence Committees (DICs) Administrative & logistics support to be provided by DC & DPO
2.	ESTABLISHMENT OF TRANSIT / HOLDING FACILITIES a. Holding of ACC holders at Transit Facilities b. Transit / Holding facilities may include the following: i. A facility of School Education Department. ii. A facility of Higher Education Department. iii. A facility earlier used as Quarantine centers during COVID-19 pandemic. iv. Any under construction Government building which is nearing completion.	To be identified by respective DICs

Decoy document

Within our observation window for the Remcos C2 activity (from 20 November 2025 to 21 April 2026), the victimology outside Pakistani law enforcement includes government, defense,

foreign affairs, intelligence, research, and manufacturing entities across South and Southeast Asia, and the Middle East.

C2 Activity Cluster | Cobalt Strike

Although Cobalt Strike is a commodity tool that carries no inherent attribution, we attribute with medium confidence both servers in this C2 activity cluster to China-nexus threat actors.

The C2 traffic to 142.171.183[.]8, spanning 13 September 2024 to 5 December 2025, reveals victimology extending beyond Pakistani law enforcement to government, academic, telecommunications, and non-governmental entities across South, East, and Southeast Asia, the Middle East, and South America, in line with a China-aligned targeting profile. Among these entities are Tibetan Buddhist organizations in Taiwan, a long-standing Chinese cyberespionage interest.

For 193.42.25[.]65, we observed C2 communications only with Balochistan Police infrastructure, taking place between 7 November and 5 December 2024. 193.42.25[.]65 also served as next-stage infrastructure for one of two implants deployed on the Balochistan Police CMS web application. We trace these implants to a Chinese-speaking developer through related samples sharing the same development environment, a topic we discuss in greater detail in a later section.

Balochistan Police | Compromised Assets

Across the four C2 activity clusters, C2 communications involving the following Balochistan Police assets took place between 2 June 2024 and 9 April 2026:

- two network appliances;
- web servers hosting several Balochistan Police web applications;
- a Fortinet FortiMail appliance that had served as Balochistan Police's primary inbound email gateway.

At the time of this activity, the FortiMail appliance was no longer the designated inbound email gateway, but it remained operational on the network and may have continued to process outbound or internal mail relay traffic. Its compromise may therefore have additionally exposed email traffic it processed.

Many of the web applications hosted on the affected servers are part of the [Smart Police Station](#) initiative, an EU-supported effort to modernize Balochistan policing and improve how it serves the public through digitalization. Throughout the threat actor activities, the web servers hosted a mix of public-facing applications through which citizens and businesses access

policing services, alongside restricted police applications protected by firewalls against unauthorized external access.

The table below summarizes the application functions as described in publicly available documentation.

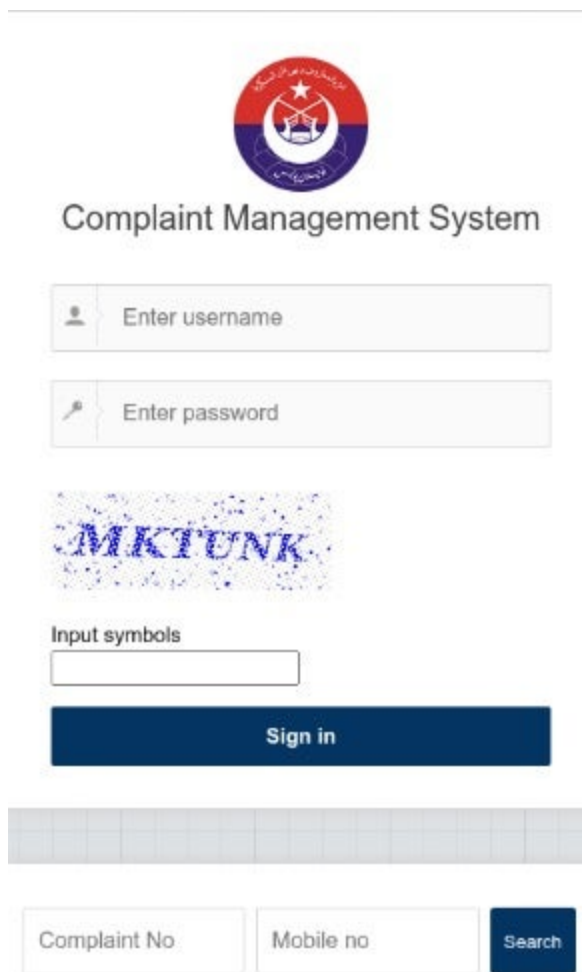
Application	Function
First Information Report (FIR)	Application for FIR registration and management. FIRs are documents prepared by police upon receiving information about the commission of a cognisable offence.
Human Resource Management Information System (HRMIS)	Personnel database managing officer service records, transfers, postings, payroll, and performance evaluations.
Anti-Vehicle Lifting System (AVLS)	Database for tracking stolen vehicles, their recovery, and investigation.
HotelEye	System for hotel guest check-in logging, integrated with NADRA identity records to notify police when individuals with criminal records check in.
Criminal Record Management System (CRMS)	Criminal records database with fingerprint-based biometric matching.
Tenant Registration System (TRS)	Landlord-tenant registration platform integrated with criminal records.
Complaint Management System (CMS)	Platform for registering, tracking, and resolving citizen complaints, from reports of crime and loss of documents to complaints about police misconduct.

If the threat actors could reach the data stores backing these applications from the compromised servers, the data they could obtain would span police personnel records, criminal case files, biometric records, stolen vehicle records, hotel guest check-in records, tenant registration records, and citizen complaints. Together, it would provide broad visibility into Balochistan Police's operational posture, capabilities, and intelligence activities.

Balochistan Police | CMS Compromise

The CMS web application, accessible at `cms.balochistanpolice[.]gov[.]pk` and hosted on one of the affected Balochistan Police web servers, was also compromised. Based on shared infrastructure and a common focus on Balochistan Police, we associate this intrusion with the threat actor operating `193.42.25[.]65`, a constituent of the Cobalt Strike C2 activity cluster.

The landing page at `cms.balochistanpolice[.]gov[.]pk` features a login interface and a separate search form.



Complaint Management System

Enter username

Enter password

MKTUNK

Input symbols

Sign in

Complaint No Mobile no Search

The CMS landing page

Access behind the login interface is highly likely restricted to law enforcement personnel. Stolen login credentials for the portal, which we retrieved from information stealer logs published on the dark web, reveal a consistent naming convention across the recovered usernames: a `ps-` prefix (most probably denoting “police station”) followed by a district or city within Balochistan, such as `ps-barkhan`.

In contrast, the search form, which posts to `/Complaint/PublicSearch` and accepts a complaint reference number and mobile number, is evidently intended to allow citizens to

check the status of a filed complaint.

We therefore assess with high confidence that the CMS application serves two distinct user groups: law enforcement personnel and citizens.

Based on VirusTotal data, two variants of an implant named `cms_plugin.exe` were uploaded to `cms.balochistanpolice[.]gov[.]pk/client%20scripts/` in late 2024, one written in the Rust programming language, the other compiled as a .NET executable. The Rust executable is a malware stager that downloads a payload from `193.42.25[.]65` and executes it. We could not retrieve the next stage at the time of analysis.

The .NET executable masquerades as `360Safe.exe`, a component of the endpoint security software 360 Safe Guard from the Chinese vendor Qihoo 360. It reflectively loads an assembly implementing an AsyncRAT client, which is configured to use `41.216.188[.]140` as its C2 server. The assembly has a PDB path of `D:\codedome\case\six\Client\Client2\obj\Debug\Client2.pdb`.

Pivoting on the `D:\codedome` prefix, we identified multiple additional samples highly likely built in the same development environment. Several are AsyncRAT clients that share implementation patterns with the one embedded in `cms_plugin.exe`, such as variable naming and string obfuscation, reinforcing a common origin beyond the shared PDB prefix. Some contain Chinese-language terms in pinyin in their PDB paths, such as `xinshi` (likely 新式, “new type” or “new variant”), and one includes log messages in simplified Chinese. These indicators point to a Chinese-speaking developer behind the samples linked by the `D:\codedome` prefix, including the one deployed on the Balochistan Police CMS application.

```
bool flag = stringBuilder.ToString().ToUpper() == text2;
if (flag)
{
    break;
}
Console.WriteLine(string.Format("第{0}次随机序列碰撞失败, 执行随机函数", num2));
RandomHelper.Instance.randomRun(5, 0, true);
Thread.Sleep(100);
}
Console.WriteLine("随机序列碰撞成功");
```

Log messages

Pivoting on the `cms_plugin.exe` filename, we identified a third malware stager functionally similar to the Rust variant, also downloading the next stage from `193.42.25[.]65`.

Both `cms_plugin.exe` samples downloading from `193.42.25[.]65` display the message Update Complete! Please refresh the page upon execution, mimicking an update for the CMS portal.

The fake update prompt, combined with the `cms_plugin.exe` filename and the hosting location in the portal's `/client scripts/` directory, indicates that the implants were targeted at users of the CMS platform: police staff, citizens checking complaint status, or both. Successful infection would grant the threat actor access to the victim's device. In the case of police personnel, this could provide a foothold into internal police networks and access to operational data beyond the CMS platform. In the case of citizens, it would enable surveillance of those who have filed complaints through the platform.

Conclusion

The intrusions we cover in this post show how domestic security institutions can become high-value intelligence targets when the threats they monitor overlap with foreign intelligence requirements. Balochistan Police sits at such an intersection, attracting cyberespionage activity from both a partner and an adversary of Pakistan. For China-nexus actors, access to its systems could support independent assessment of threats to Chinese nationals and interests in the country. For India-nexus actors, such access provides visibility into how Pakistan manages security in a province central to its adversarial relationship with India.

The compromise of the Complaint Management System web application adds a second dimension to the activity against Balochistan Police, extending the threat actor's reach beyond the initially compromised environment. By hosting implants in a portal used by both citizens and law enforcement personnel, the threat actor turned a tool built to make policing in Pakistan more accessible and accountable to the public into a malware delivery mechanism. This weaponization widened the collection surface from the application and its data to the users interacting with it.

The multi-actor convergence on Balochistan Police points to a structural consequence of digital policing. Systems built to centralize records, workflows, and public interaction can also centralize intelligence value by bringing together operational, institutional, and civilian data across connected environments. Law enforcement infrastructure in that setting is no longer just the digital backbone of policing but intelligence terrain, and it will be treated as such by any adversary who can reach it.

Indicators of Compromise

SHA-1 Hashes

Value	Note

000fad96a85dd6933c22d3dbec9aed47b7f1f066	Backdoor launcher (TAG-179)
08570471f39bb6725f07b8cddbca99ed48c22686	Backdoor launcher (TAG-179)
23f4766c011d193f076dfc735dc460e2a41ead79	Backdoor launcher (TAG-179)
23f6781919a50b118d8d4e6a7e9ae63b71ecc885	cms_plugin.exe
2bab40c55637398f0497cff9c8cbea564d595c7f	Lure file (TAG-179)
4039454c9189e64285e93fc075a30b93f814b5b5	cms_plugin.exe
47f8cb0c2dcf62702f58cfc1603d6325755f6820	Backdoor launcher (TAG-179)
539bd79fbb684edea94eb37518134b97e94b9dd8	Lure file (TAG-179)
58cb2d95063b9df807b7aa8dc106b74ce988a491	cms_plugin.exe
5d60ff36ff519c2e13e7f66cfa0bb46be79592a7	Backdoor (TAG-179)
63b88d00331de88af696dfb7a896935d830e485f	Backdoor (TAG-179)
6fe2e74d009abbd56de01fd7404a1245e9b47c79	Lure file (TAG-179)
71757adba833b46f961e840d0f055bcce0b529c4	Lure file (TAG-179)
8c329db96e093fa25268e078405a33c518dbb5c9	Backdoor (TAG-179)
c6c197e61079a0a33108c2c87b5e3c7056a138ec	Lure file (TAG-179)
d66ab0cd2e44dc8389c111b7ed34c7bcb0b35311	Backdoor (TAG-179)

IP Addresses

Value	Note
142.171.183[.]8	Cobalt Strike C2 server
172.111.233[.]105	PlugX C2 server
172.111.233[.]12	PlugX C2 server
172.111.233[.]26	PlugX C2 server

172.111.233[.]36	PlugX C2 server
172.111.233[.]96	PlugX C2 server
172.94.9[.]19	PlugX C2 server
172.94.9[.]43	PlugX C2 server
172.94.9[.]49	PlugX C2 server
193.42.25[.]65	Cobalt Strike C2 server
41.216.188[.]140	AsyncRAT C2 server
45.125.32[.]218	ShadowPad C2 server
45.74.6[.]17	PlugX C2 server
89.31.121[.]220	Remcos C2 server

URLs

Value	Note
https://cms.balochistanpolice[.]gov[.]pk/client%20scripts/cms_plugin.exe	Implant-hosting URL on the Balochistan Police CMS portal