Castellum Labs

MUSTANG PANDA

A THREAT GROUP OF CHINA

Threat Overview

Mustang Pandais a highly capable and active China-linked cyber espionage Advanced Persistent Threat (APT) group that has been operating since at least 2012.

They specialize in intelligence collection to support Beijing's geopolitical objectives, consistently targeting global government agencies, military entities, religious groups, and NGOs across Asia, Europe, and the Americas.

Profile Information

Metric	Value
Aliases	BASIN, Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, Hive0154, G0129, TA416, BASIN, BRONZE PRESIDENT, Earth Preta, HoneyMyte, LuminousMoth, Polaris, Red Lich, Stately Taurus, TANTALUM, TEMP.HEX, Twill Typhoon
First Seen	2012
Last Seen	2026-06-29
Associated Campaigns	Operation Diànxùn, RedDelta Modified PlugX Infection Chain Operations.
Country of Origin	China
Exploited CVEs	CVE-2017-0199, CVE-2021-1675, CVE-2021-34527, CVE-2021-40444, CVE-2017-11882, CVE-2022-47966
Associated Infrastructure	Microsoft OneDrive, Zoho Workdrive

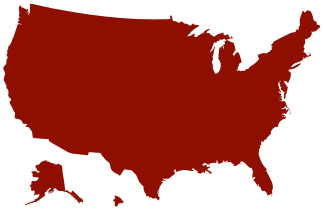
Castellum Labs

Targeted Geography

India

Taiwan

South Korea



United States

Pakistan

Germany

Mongolia

Myanmar

Targeted Sectors

Financial

Government

Critical Infrastructure

Energy

Military

Non - Government Organization

Telecommunication

Malware Used

Malware	Description
PlugX	A modular remote access trojan (RAT) extensively used by Mustang Panda for persistent access, command execution, file theft, and remote system control.
BOOKWORM	A custom Mustang Panda backdoor used to establish covert persistence and facilitate command-and-control (C2) communications.
CorKLOG	A keylogger deployed by Mustang Panda to capture user credentials, keystrokes, and other sensitive information from compromised systems.
CLAIMLOADER	A custom loader used to decrypt and execute Mustang Panda payloads while evading security detection.
DOPLUGS	A PlugX variant customized by Mustang Panda to provide remote administration, payload delivery, and post-compromise operations.
FDMTP	A lightweight backdoor used by Mustang Panda for remote command execution and maintaining access to compromised hosts.
Hodur	A stealthy loader used to deploy additional malware while bypassing endpoint security and analysis mechanisms.
HIUPAN	A Mustang Panda backdoor designed to establish persistence, execute attacker commands, and communicate with C2 infrastructure.
LOTUSLITE	A lightweight remote access trojan employed for espionage activities, enabling file collection and remote control.
MQsTTang	A malware family leveraging the MQTT protocol for covert command-and-control communications in Mustang Panda campaigns.
STATICPLUGIN	A modular PlugX plugin that extends malware capabilities through additional espionage and post-exploitation modules.
StarProxy	A proxy malware used to tunnel malicious traffic through compromised hosts, masking attacker infrastructure and activity.

Malware Used

Malware	Description
SplatCloak	An evasion component designed to disable or bypass endpoint security products before deploying additional payloads.
TONESHELL	A sophisticated backdoor used by Mustang Panda for long-term persistence, command execution, and intelligence collection.
SnakeDisk	A malware component used to stage, store, and deliver encrypted payloads while reducing forensic visibility.

Tools Used

Tool	Description
AdFind	Used by Mustang Panda for Active Directory reconnaissance, enabling enumeration of users, groups, computers, and domain trust relationships.
Cobalt Strike	A commercial post-exploitation framework abused by Mustang Panda for beaconing, privilege escalation, lateral movement, and command execution.
Impacket	A collection of Python tools leveraged for credential abuse, remote execution, SMB operations, and lateral movement across Windows environments.
NBTScan	A reconnaissance utility used to identify NetBIOS-enabled hosts and enumerate systems within targeted internal networks.

Initial Access & Infection Techniques

Spear-Phishing Emails (Primary Method)

- Sends highly targeted emails to government, diplomatic, NGO, military, and political targets.
- Uses themes relevant to the victim (meetings, policies, regional issues, events).
- Attachments commonly include:
  - Microsoft Office documents
  - PDFs
  - ZIP/RAR archives
  - Executables disguised as documents

Malicious Archives

- Delivers password-protected ZIP/RAR files.
- Archive contains:
  - Malware executable
  - Decoy document
  - DLL files for sideloading

DLL Sideloading (Signature Technique)

- Places a legitimate signed application alongside a malicious DLL.
- Victim runs the legitimate application.
- The application loads the malicious DLL automatically.
- Frequently used to deploy PlugX, ToneShell, and other payloads.

LNK Shortcut Files

- Uses malicious Windows shortcut (.LNK) files.
- Clicking the shortcut launches hidden commands that execute malware.
- Often embedded within compressed archives.

USB/Removable Media Propagation

- Some campaigns use USB drives to spread malware.
- Particularly observed in air-gapped or restricted environments.
- Associated with PlugX variants.

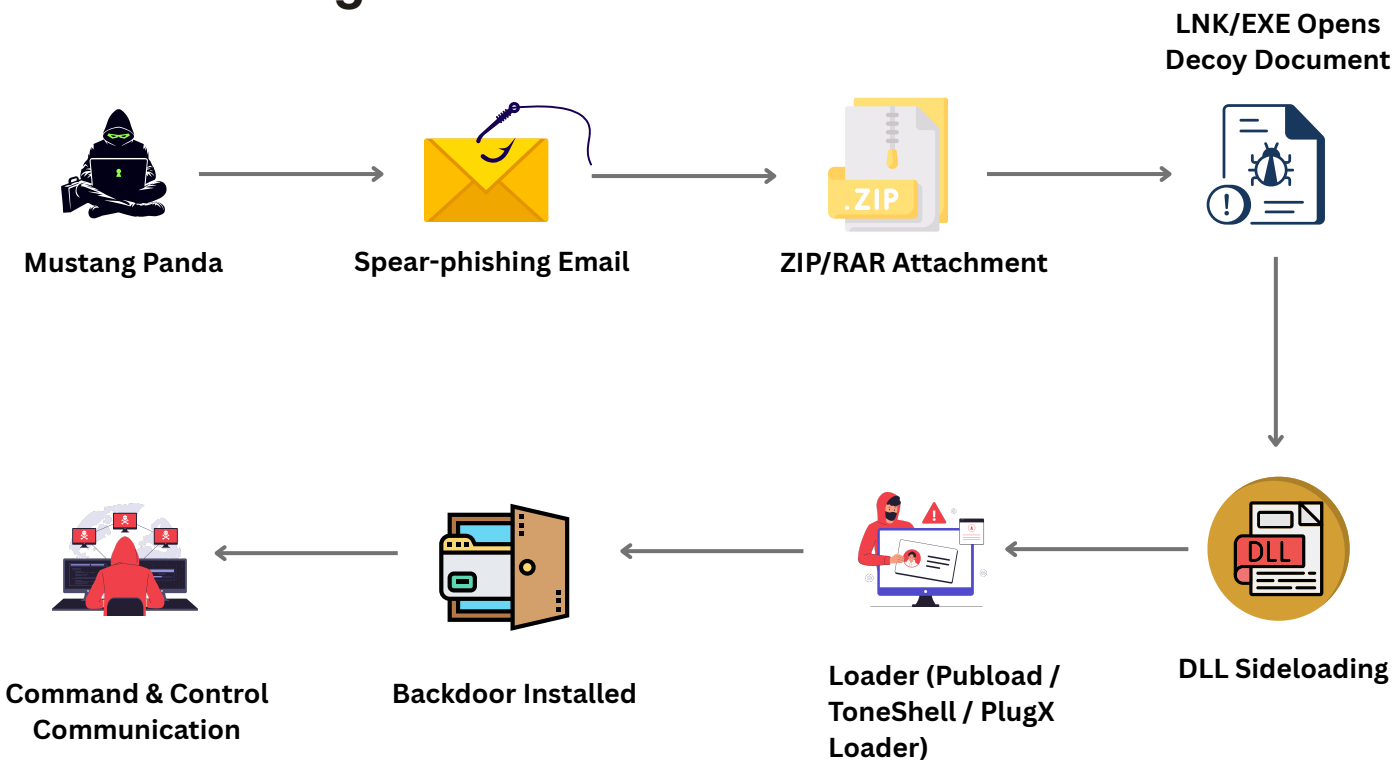
Event-Themed Lures

- Uses current geopolitical events as bait:
  - ASEAN meetings
  - South China Sea issues
  - Tibetan political events
  - Government policy documents

Legitimate Cloud Services

- Malware downloads additional payloads from trusted services:
  - Google Drive
  - Dropbox
  - OneDrive
  - Other cloud-hosted infrastructure
- Helps evade network security controls.

Multi-Stage Infection Chains



Indicators of Compromise (IoCs)

Hash Type	Hash Value
SHA256	ab9d8f1021f2a99c74aa66f8ddb52996ac2337da9de2676d090b87e19ce93033
SHA256	cf61b7a9bdde2a39156d88f309f230a7d44e9feaf0359947e1f96e069eca4e86
SHA256	5064b2a8fcfc58c18f53773411f41824b7f6c2675c1d531ffa109dc4f842119b
SHA256	fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81
SHA256	fa8853aaa156485855b77a16a2f613d9f58d82ef63505be8b19563827089bf52
SHA256	79af67ed343bc45b6a19e4836ebb83f1130243ff98f48465f9a7a807ba4bfa91
SHA256	106f46375d8497d353c22c98f72ab15a9bb87beba4585d5a492fd11edc288b0b
SHA256	8421e7995778faf1f2a902fb2c51d85ae39481f443b7b3186068d5c33c472d99
SHA256	4cd81d26289c4d8383a0ffa34397f0b03941554eac04f1b420269b831accf90e
SHA256	d4bc21e12360af2f2cb55872a90b62805150d498c452b2b1c6a05a806cbb3187
SHA256	b52c484a3cc383dd3b4dc79c207946b603a810edf74bff76dca7ad29d4de4167
SHA256	b9adc1433ef7c6fee4d36f73b79744ad611d51a8e039d4c384dd453e33452d0f
SHA256	e0fc2cf31a0fd7f4bfa1ba453fd8f272784330de2ecba80104455252a931789b
SHA256	cab5fa13c8239e97c15b04b27f9b70fb8b561d31935af7b0680bb80aec12c813
SHA256	1E629FE7C8911A9ADBDE2E35AF4F6F9E60EE538638C82EDBCBD7CCE5AD2FF4AB
SHA256	951b09c559fdc1c447f3dc63870b5244c2b715d728e1318a62db64bc17dcb85d

Hash Type	Hash Value
SHA256	9b7615b4c2c6ebdd283afb1dae4d951b7ef928939b98ffbe7dea49cc5c5eee02
SHA256	36AFA5B3133667F2577687B3E83D7F6C009DD65864C20A408D860B3C6678DF2A
SHA256	5009F65E7A8D84A9955D5ADBDB86107B15304B1061BDABA5DD2AC2293DD8E6CB
SHA256	2AEEF18ABF22B233DE5515A95CDCA5AA3CBC6C21E8D2F83A68214E7272F9D947
SHA256	377d65bdbf2b323ef9b497b1d3e2f93521a9ce57d4f2d6c296b048ee1390173e
SHA256	aec41c4f461cd08efe1390c8de513e54f766a5903c3c1f67ac4a9c93a3213c6b
SHA256	4743ccff0b5dbc34027165e177143018b9ee9e3232496ca5d4fa5cd56b5646f6
SHA256	033786a482641aa901a28a3e3c314dbe86723906cea15147629167d8364907f7
SHA256	f9e7b9e537cf6cfc88a6819f925fd2fed6404c5b58f7292ca66e3a00a02c7efa
SHA256	f7c68da91c4f52d4f5a565c4ed73b53caa8d34fe7dd0cf1cb1cb91361f94f103
SHA256	5a2e478f5a1fdb271f27595506b3cf93cf297b4ef588697c4f627690a778bfdb

Hash Type	Hash Value
MD5	08f25a641e8361495a415c763fbb9b71
MD5	01d74e6d9f77d5202e7218fa524226c4
MD5	5f094cb3b92524fced2731c57d305e78
URL	http://45[.]251[.]243[.]210/iis.jpg

Hash Type	Hash Value
SHA1	6856bb506a0858cc5597666d966b5b7499e38542
SHA1	7b90dcdf6ea88b1efa1cee36a0b1ab71e34c8d1d
SHA1	db999a5ecf4e1c87fae10983f6d23b26069cbba1
SHA1	2CF4BAFE062D38FAF4772A7D1067B80339C2CE82
SHA1	58B6B5FD3F2BFD182622F547A93222A4AFDF4E76
SHA1	69AB6B9906F8DCE03B43BEBB7A07189A69DC507B
SHA1	10AE4784D0FFBC9CD5FD85B150830AEA3334A1DE
SHA1	062473912692f7a3fab8485101d4fcf6d704ed23
SHA1	10ae4784d0ffbc9cd5fd85b150830aea3334a1de
SHA1	2b5d6bb5188895da4928dd310c7c897f51aaa050
SHA1	39863ceca1b0f54f5c063b3015b776cdb05971f3
SHA1	477a1ce31353e8c26a8f4e02c1d378295b302c9e
SHA1	4ebfc035179cd72d323f0ab357537c094a276e6d
SHA1	511da645a7282fb84ff18c33398e67d7661fd663
SHA1	52288c2cdb5926ecc970b2166943c9d4453f5e92
SHA1	59002e1a58065d7248cd9d7dd62c3f865813eee6
SHA1	69ab6b9906f8dce03b43bebb7a07189a69dc507b
SHA1	7992729769760ecab37f2aa32de4e61e77828547
SHA1	7e059258cf963b95bde479d1c374a4c300624986

Hash Type	Hash Value
SHA1	908f55d21ccc2e14d4ff65a7a38e26593a0d9a70
SHA1	97c92add7145cf9386abd5527a8bcd6fabf9a148
SHA1	ab01e099872a094dc779890171a11764de8b4360
SHA1	c13d0d669365dfaff9c472e615a611e058ebf596
SHA1	cbd875ee456c84f9e87ec392750d69a75fb6b23a
SHA1	cdb15b1ed97985d944f883af05483990e02a49f7
SHA1	f05e89d031d051159778a79d81685b62aff4e3f9
SHA1	f67c553678b7857d1bbc488040ea90e6c52946b3
SHA1	fdbb16b8ba7724659bab5b2e1385cfd476f10607

Hash Type	Hash Value
MD5	8f17a2ec3c13bed031e99cb57af220cf
MD5	b671ec37c4c59c8ccb28c22a2c8d5d5f
MD5	560110e4905c606d32d2f4164bc84dab
MD5	3c99e3522923b6ec94093e04b7e13fa5
MD5	80e1b35816a1231b9cf02983fc75a617
MD5	3c6173d8693510f6363b608c09feebb1
MD5	8fbad6e5aa15857f761e6a7a75967e85
MD5	7e05d4944026e5b2198563d0a6a0bd53

Hash Type	Hash Value
MD5	40876d28457f5efd3367f963542a8b8b
MD5	d7ac2c6987f31219b9e5c86d85e66bfa
MD5	12aa335ef324df213571a24ad38c3199
MD5	bd43933d60913e2f633bf029ff0120db
MD5	a23cc87cb713f5c4855babb841189b04
MD5	54d4fee3384c0595decb189b62712591
MD5	11045d9af0ec399b02c7cf8259e18548
MD5	d91655915849a6451b54a1c7a4aba8b4
MD5	01d8305b91524d83ccf2c26c1b3b7f1f
MD5	b17619b7f6e607e4ceea4139a08897b7
MD5	6a2b0d57bcc6dabd986e553dc1a892ef
MD5	8ff41ca8ff54542f43ad9648ad4f3286
MD5	6f207612d5d594e50cb1f624de3323aa
MD5	c649cb9f2cf6a39cb5c731277758e3bc

IOC Type	IOC Value
IP Address	65.21.111.255
IP Address	103.75.190.50
IP Address	95.217.1.81
IP Address	5.206.224.167
IP Address	45.121.146[.]113
IP Address	61.4.102[.]75
IP Address	45.154.24[.]14
IP Address	45.154.14[.]235
IP Address	92.118.188[.]78

IOC Type	IOC Value
Domain	wpstatic.microsoft.com
Domain	www.download.wndowsupdate.com
Domain	web.officeproduces[.]com
Domain	fruitbrat[.]com
Domain	president-office.gov[.]m
Domain	urmsec[.]com
Domain	zyber-i[.]com
Domain	locvnpt[.]com

Castellum Labs

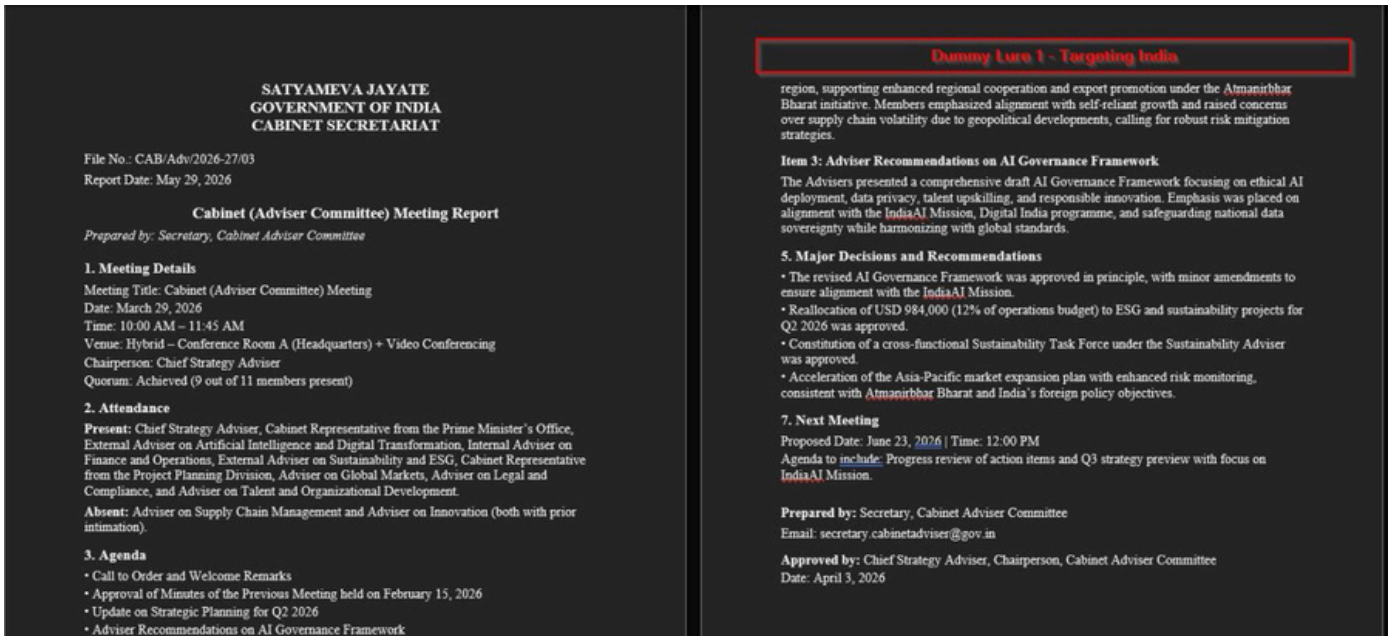
Key Timelines

Year	Key Event	Why It Matter
2012	Mustang Panda begins operations (earliest activity traced by multiple security firms).	Marks the emergence of what would become one of China's most active cyber-espionage groups.
2017–2018	Public identification by researchers after campaigns targeting Mongolia and Southeast Asia. CrowdStrike formally names the group "Mustang Panda" in 2018.	This is when the group became widely known in threat intelligence circles.
2019	Major espionage campaigns exposed against minority groups, governments, NGOs, and organizations across Asia.	Demonstrated that the group's mission extended beyond traditional government targets into broader intelligence collection.
2020	RedDelta operations linked to surveillance of entities connected to the Vatican and Catholic organizations.	One of the most politically sensitive campaigns attributed to the group.
2021	Expansion beyond Asia; campaigns increasingly target Europe, diplomatic organizations, and policy-related entities.	Showed the group's growing geographic reach and strategic ambitions.
2022	Shift to more advanced malware delivery chains; deployment of new PlugX variants (including "Hodur") and Ukraine-themed lures targeting European and Russian organizations.	Signaled a significant technical evolution and adaptation to current geopolitical events.
2023	Researchers report more than 200 victims across Asia, Africa, Europe, and the Middle East; targeting expands to immigration, border security, maritime, academia, finance, and energy sectors.	Demonstrated industrial-scale cyber-espionage operations.
2024–2025	Development and deployment of newer malware ecosystems such as ToneShell, CoolClient, StarProxy, PAKLOG, CorKLOG, and anti-detection tooling. Targeted the Tibetan community using Pubload malware and event-themed lures tied to Tibetan political activities.	Indicates a transition from reliance on older PlugX infrastructure to a broader custom toolset. Continued targeting aligned with Chinese strategic interests.
Jan–Feb 2026	New CoolClient-based espionage campaigns uncovered targeting government and diplomatic organizations across Asia and parts of Eastern Europe; use of cloud services for stealthy data exfiltration.	Represents the most recent known evolution of the group's espionage capabilities before June 2026.
June 2026	Mustang Panda targets Indian government and energy sectors using ZOHOMURK and MINIRECON.	Indicates sudden transition of targeting & focusing on India.

Recent Notable Event

June 28, 2026

- Mustang Panda orchestrated two concurrent campaigns targeting Indian Government entities such as **Hydropower sector & Government** with Lure MOUs**.**
- In this campaign, researchers uncovered new malware toolkit named as SHARDLOADER, MINIRECON and ZOHOMURK.
- **SHARDLOADER** variants demonstrate moderate sophistication, leveraging persistence and DLL sideloading to deploy two newly identified implants: **ZOHOMURK** and **MINIRECON**.
- **ZOHOMURK** is a newly identified implant that leverages Zoho WorkDrive for command-and-control, data exfiltration and remote task execution.
- **MINIRECON** is a newly identified implant derived from the **ToneShell** Malware familly.



SATYAMEVA JAYATE
GOVERNMENT OF INDIA
CABINET SECRETARIAT

File No.: CAB/Adv/2026-27/03
Report Date: May 29, 2026

Cabinet (Adviser Committee) Meeting Report

Prepared by: Secretary, Cabinet Adviser Committee

1. Meeting Details

Meeting Title: Cabinet (Adviser Committee) Meeting
Date: March 29, 2026
Time: 10:00 AM – 11:45 AM
Venue: Hybrid – Conference Room A (Headquarters) + Video Conferencing
Chairperson: Chief Strategy Adviser
Quorum: Achieved (9 out of 11 members present)

2. Attendance

Present: Chief Strategy Adviser, Cabinet Representative from the Prime Minister's Office, External Adviser on Artificial Intelligence and Digital Transformation, Internal Adviser on Finance and Operations, External Adviser on Sustainability and ESG, Cabinet Representative from the Project Planning Division, Adviser on Global Markets, Adviser on Legal and Compliance, and Adviser on Talent and Organizational Development.

Absent: Adviser on Supply Chain Management and Adviser on Innovation (both with prior intimation).

3. Agenda

- Call to Order and Welcome Remarks
- Approval of Minutes of the Previous Meeting held on February 15, 2026
- Update on Strategic Planning for Q2 2026
- Adviser Recommendations on AI Governance Framework

Dummy Lure 1 - Targeting India

region, supporting enhanced regional cooperation and export promotion under the Atmanirbhar Bharat initiative. Members emphasized alignment with self-reliant growth and raised concerns over supply chain volatility due to geopolitical developments, calling for robust risk mitigation strategies.

Item 3: Adviser Recommendations on AI Governance Framework

The Advisers presented a comprehensive draft AI Governance Framework focusing on ethical AI deployment, data privacy, talent upskilling, and responsible innovation. Emphasis was placed on alignment with the IndiaAI Mission, Digital India programme, and safeguarding national data sovereignty while harmonizing with global standards.

5. Major Decisions and Recommendations

- The revised AI Governance Framework was approved in principle, with minor amendments to ensure alignment with the IndiaAI Mission.
- Reallocation of USD 984,000 (12% of operations budget) to ESG and sustainability projects for Q2 2026 was approved.
- Constitution of a cross-functional Sustainability Task Force under the Sustainability Adviser was approved.
- Acceleration of the Asia-Pacific market expansion plan with enhanced risk monitoring, consistent with Atmanirbhar Bharat and India's foreign policy objectives.

7. Next Meeting

Proposed Date: June 23, 2026 | Time: 12:00 PM
Agenda to include: Progress review of action items and Q3 strategy preview with focus on IndiaAI Mission.

Prepared by: Secretary, Cabinet Adviser Committee
Email: secretary.cabinetadviser@gov.in

Approved by: Chief Strategy Adviser, Chairperson, Cabinet Adviser Committee
Date: April 3, 2026

IOC's of Recent Incident

IOC Type	Hash Value	File Name	File Size	File Type
SHA256	f53fd0626404a129dcddb8ee7589387dd7bda7999814e0df46c670af6b3da5f5	MOU USI-INDSR, TAIWAN.zip	3.15 MB	ZIP
SHA256	ebd533de7ca16daa70093b0b1084fb6136b6ba091d6ee0e4199762581e1b2e5a	SolidPDFCreator.dll	177.50 KB	Win32 DLL
SHA256	f2bed071676feb831ed460489643fd57f6c6c1e0d024a1ea447820276fb13828	Ctxmui.dll	2.28 MB	Win32 DLL
SHA256	cd9397797216fd4c08df324937509124e57258328c8e4c6d795c6a2cd25b69b0	Hydropower Cooperation Project Proposal.zip	850.66 KB	ZIP

MITRE ATT&CK Mapping:

Attack ID		Technique Name	Description
T1087	.002	Account Discovery: Domain Account	Mustang Panda has utilized AdFind to identify domain users.
T1583	.001	Acquire Infrastructure: Domains	Mustang Panda has acquired C2 domains prior to operations. Mustang Panda registered adversary-controlled domains during RedDelta Modified PlugX Infection Chain Operations that were re-registrations of expired domains.
	.006	Acquire Infrastructure: Web Services	Mustang Panda has set up Dropbox and Google Drive to host malicious downloads.
T1557		Adversary-in-the-Middle	Mustang Panda leveraged a captive portal hijack that redirected the victim to a webpage that prompted the victim to download a malicious payload.
T1071	.001	Application Layer Protocol: Web Protocols	Mustang Panda has communicated with its C2 via HTTP POST requests. Mustang Panda used HTTP POST messages for command and control from PlugX installations during RedDelta Modified PlugX Infection Chain Operations.
T1560	.001	Archive Collected Data: Archive via Utility	Mustang Panda has used RAR to create password-protected archives of collected documents prior to exfiltration.Mustang Panda has used WinRAR "Rar.exe" to archive stolen files before exfiltration.Mustang Panda has also used TONESHELL and post-exploitation tools such as RemCom and Impacket to execute WinRAR rar.exe to archive files for exfiltration.
	.003	Archive Collected Data: Archive via Custom Method	Mustang Panda has encrypted documents with RC4 prior to exfiltration.
T1119		Automated Collection	Mustang Panda used custom batch scripts to collect files automatically from a targeted system.

Attack ID		Technique Name	Description
T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Mustang Panda has created the registry key HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\AdobeImdyU to maintain persistence.Mustang Panda has also established persistence via the registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run. Mustang Panda used Run registry keys with names such as OneNote Update to execute legitimate executables that would load through search-order hijacking malicious DLLS to ensure persistence during RedDelta Modified PlugX Infection Chain Operations.
T1059		Command and Scripting Interpreter	Mustang Panda has utilized meterpreter shellcode.
	.001	PowerShell	Mustang Panda has used malicious PowerShell scripts to enable execution. Mustang Panda used LNK files to execute PowerShell commands leading to eventual PlugX installation during RedDelta Modified PlugX Infection Chain Operations.
	.003	Windows Command Shell	Mustang Panda has executed HTA files via cmd.exe, and used batch scripts for collection.Mustang Panda has also utilized cmd.exe to execute commands on an infected host such as cmd.exe /c ping.exe 8.8.8.8 -n 70&&"%temp%\FontEDL.exe".
	.005	Visual Basic	Mustang Panda has embedded VBScript components in LNK files to download additional files and automate collection. Mustang Panda has also used VBA macros in maldocs to execute malicious DLLs.Mustang Panda also utilized a VBS Script "autorun.vbs" that created persistence through saving the VBS Script in the startup directory which would cause it to run each time the machine was turned on.
	.007	JavaScript	Mustang Panda has executed a JavaScript payload utilizing wscript.exe on the endpoint.
T1586	.002	Compromise Accounts: Email Accounts	Mustang Panda has compromised legitimate email accounts to use in their spear-phishing operations.
T1001	.003	Data Obfuscation: Protocol or Service Impersonation	Mustang Panda has utilized TLS record headers in network packets to impersonate various versions of TLS protocols to blend in with legitimate network traffic. Mustang Panda has used FakeTLS to communicate with its C2 servers.
T1074	.001	Data Staged: Local Data Staging	Mustang Panda has stored collected credential files in c:\windows\temp prior to exfiltration. Mustang Panda has also stored documents for exfiltration in a hidden folder on USB drives.

Attack ID		Technique Name	Description
T1622		Debugger Evasion	Mustang Panda has embedded debug strings with messages to distract analysts.Mustang Panda has also made calls to Windows API CheckRemoteDebuggerPresent and exits if it detects a debugger.
T1678		Delay Execution	Mustang Panda has delayed the execution of payloads leveraging ping echo requests cmd /c ping 8.8.8.8 -n 70&&"%temp%\<legitimate executable>".
T1140		Deobfuscate/Decode Files or Information	Mustang Panda has the ability to decrypt its payload prior to execution.Mustang Panda has also utilized RC4 encryption for malicious payloads.
T1587	.001	Develop Capabilities: Malware	Mustang Panda has developed custom malware for use in their operations.
T1573	.001	Encrypted Channel: Symmetric Cryptography	Mustang Panda has encrypted C2 communications with RC4 Mustang Panda has also leveraged encryption and compression algorithms to obfuscate the traffic between the system and C2 server, methods observed included RC4, AES, XOR with 0x5a, and LZO.
T1585	.002	Establish Accounts: Email Accounts	Mustang Panda has leveraged the legitimate email marketing service SMTP2Go for phishing campaigns. Mustang Panda has also created fake Google accounts to distribute malware via spear-phishing emails.Mustang Panda has also created accounts for spearphishing operations including the use of services such as Proton Mail.
T1546	.003	Event Triggered Execution : Windows Management Instrumentation Event Subscription	Mustang Panda's custom ORat tool uses a WMI event consumer to maintain persistence.
T1480		Execution Guardrails	Mustang Panda included the use of Cloudflare geofencing mechanisms to limit payload download activity during RedDelta Modified PlugX Infection Chain Operations.
T1048	.003	Exfiltration Over Alternative Protocol: Exfiltration Over Unencrypted Non-C2 Protocol	Mustang Panda has used FTP to exfiltrate archive files.
T1041		Exfiltration Over C2 Channel	Mustang Panda has exfiltrated stolen data and files to its C2 server.
T1052	.001	Exfiltration Over Physical Medium: Exfiltration over USB	Mustang Panda has used a customized PlugX variant which could exfiltrate documents from air-gapped networks.
T1567	.002	Exfiltration Over Web Service: Exfiltration to Cloud Storage	Mustang Panda has also exfiltrated archived files to cloud services such as Dropbox using curl.

Attack ID		Technique Name	Description
T1203		Exploitation for Client Execution	Mustang Panda has exploited CVE-2017-0199 in Microsoft Word to execute code. Mustang Panda used the GrimResource exploitation technique via specially crafted MSC files for arbitrary code execution during RedDelta Modified PlugX Infection Chain Operations.
T1083		File and Directory Discovery	Mustang Panda has searched the entire target system for DOC, DOCX, PPT, PPTX, XLS, XLSX, and PDF files.
T1564	.001	Hide Artifacts: Hidden Files and Directories	Mustang Panda's PlugX variant has created a hidden folder on USB drives named RECYCLE.BIN to store malicious executables and collected data.[36] Mustang Panda has also modified file attributes to hidden and system. Mustang Panda stored encrypted payloads associated with PlugX installation in hidden directories during RedDelta Modified PlugX Infection Chain Operations.
T1574	.001	Hijack Execution Flow: DLL	Mustang Panda has used a legitimately signed executable to execute a malicious payload within a DLL file.Mustang Panda has abused legitimate executables to side-load malicious DLLs. Mustang Panda used DLL search order hijacking on vulnerable applications to install PlugX payloads during RedDelta Modified PlugX Infection Chain Operations.
	.005	Hijack Execution Flow: Executable Installer File Permissions Weakness	Mustang Panda has leveraged legitimate software installer executables such as Setup Factory "IRSetup.exe" to drop and execute their payload.
T1070		Indicator Removal	Mustang Panda has deleted registry keys that store data and maintained persistence.
	.004	File Deletion	Mustang Panda will delete their tools and files, and kill processes after their objectives are reached.
	.006	Timestomp	Mustang Panda has modified file timestamps from the export address table (EAT) in malware to make it difficult to identify creation times.
T1105		Ingress Tool Transfer	Mustang Panda has downloaded additional executables following the initial infection stage.Mustang Panda has also leveraged Visual Studio Code code.exe and Dev Tunnels using DevTunnel.exe to propagate additional tools and payloads.
T1654		Log Enumeration	Mustang Panda has used Wevtutil to gather Windows Security Event Logs.

Attack ID		Technique Name	Description
T1036	.004	Masquerading: Masquerade Task or Service	Mustang Panda masqueraded Registry run keys as legitimate-looking service names such as OneNote Update during RedDelta Modified PlugX Infection Chain Operations.
	.005	Masquerading: Match Legitimate Resource Name or Location	Mustang Panda has used names like adobeupdate.dat and PotPlayerDB.dat to disguise PlugX, and a file named OneDrive.exe to load a Cobalt Strike payload.Mustang Panda has also masqueraded legitimate browser plugin updates to include AdobePlugins.exe.
T1106		Native API	Mustang Panda has used various Windows API calls during execution and defense evasion.
T1046		Network Service Discovery	Mustang Panda has leveraged NBTscan to scan IP networks.
T1095		Non-Application Layer Protocol	Mustang Panda has utilized TCP-based reverse shells using cmd.exe. Mustang Panda communicated over TCP 5000 from adversary administrative servers to adversary command and control nodes during RedDelta Modified PlugX Infection Chain Operations.
T1027		Obfuscated Files or Information	Mustang Panda has delivered initial payloads hidden using archives and encoding measures.Mustang Panda has also utilized opaque predicates in payloads to hinder analysis.
	.007	Dynamic API Resolution	Mustang Panda has leveraged obfuscated Windows API function calls that were concealed as unique names, or hashes of the Windows API.
	.012	LNK Icon Smuggling	Mustang Panda has utilized LNK files to hide malicious scripts for execution.Mustang Panda has also leveraged LNK files that were programmed to display a PDF icon to entice the victim to click on the file to execute an office.exe binary.
	.013	Encrypted/Encoded File	Mustang Panda stored installation payloads as encrypted files in hidden folders during RedDelta Modified PlugX Infection Chain Operations.
	.016	Junk Code Insertion	Mustang Panda has used junk code within their DLL files to hinder analysis.
T1588	.002	Obtain Capabilities: Tool	Mustang Panda has obtained and leveraged publicly-available tools for intrusion activities.
	.003	Obtain Capabilities: Code Signing Certificates	Mustang Panda has used revoked code signing certificates for its malicious payloads.

Attack ID		Technique Name	Description
T1588	.004	Obtain Capabilities: Digital Certificates	Mustang Panda has obtained SSL certificates for their C2 domains. Mustang Panda acquired Cloudflare Origin CA TLS certificates during RedDelta Modified PlugX Infection Chain Operations.
T1003		OS Credential Dumping	Mustang Panda utilized "Hdump" to dump credentials from memory.
	.001	LSASS Memory	Mustang Panda has harvested credentials from memory of lssas.exe with Mimikatz.
	.003	NTDS	Mustang Panda has used vssadmin to create a volume shadow copy and retrieve the NTDS.dit file. Mustang Panda has also used reg save on the SYSTEM file Registry location to help extract the NTDS.dit file.
	.006	DCSync	Mustang Panda has leveraged Mimikatz DCSync feature to obtain user credentials.
T1069	.002	Permission Groups Discovery: Domain Groups	Mustang Panda has leveraged AdFind to enumerate domain groups.
T1566	.001	Phishing: Spearphishing Attachment	Mustang Panda has used spearphishing attachments to deliver initial access payloads. Mustang Panda has also delivered archive files such as RAR and ZIP files containing legitimate EXEs and malicious DLLs. Mustang Panda leveraged malicious attachments in spearphishing emails for initial access to victim environments in RedDelta Modified PlugX Infection Chain Operations.
	.002	Phishing: Spearphishing Link	Mustang Panda has delivered malicious links to their intended targets.Mustang Panda has distributed spear-phishing emails with embedded links that direct the victim to a malicious archive hosted on Google or Dropbox. Mustang Panda distributed malicious links in phishing emails leading to HTML files that would direct the victim to malicious MSC files if running Windows based on User Agent fingerprinting during RedDelta Modified PlugX Infection Chain Operations.
T1057		Protocol Tunneling	Mustang Panda has leveraged OpenSSH (sshd.exe) to execute commands, transfer files and spread across the environment communicating over SMB port 445.
T1090		Proxy	Mustang Panda proxied communication through the Cloudflare CDN service during RedDelta Modified PlugX Infection Chain Operations.
T1219	.001	Remote Access Tools: IDE Tunneling	Mustang Panda has utilized an established Github account to create a tunnel within the victim environment using Visual Studio Code through the code.exe tunnel command.[18]

Attack ID		Technique Name	Description
T1219	.002	Remote Access Tools: Remote Desktop Software	Mustang Panda has installed TeamViewer on targeted systems.
T1018		Replication Through Removable Media	Mustang Panda has used a customized PlugX variant which could spread through USB connections.
T1053	.005	Scheduled Task/Job: Scheduled Task	Mustang Panda has created a scheduled task to execute additional malicious software, as well as maintain persistence.Mustang Panda has also created a scheduled task that creates a reverse shell.
T1593		Search Open Websites/Domains	Mustang Panda has used open-source research to identify information about victims to use in targeting to include creating weaponized phishing lures and attachments.
T1505	.003	Server Software Component: Web Shell	Mustang Panda has used China Chopper web shells to maintain access to victims' environments.
T1129		Shared Modules	Mustang Panda has leveraged LoadLibrary to load DLLs.
T1072		Software Deployment Tools	Mustang Panda has leveraged legitimate software tools such as AntiVirus Agents, Security Services, and App Development tools to execute scripts and to side-load dlls.
T1518		Software Discovery	Mustang Panda has searched the victim system for the InstallUtil.exe program and its version.
T1176	.002	Software Extensions: IDE Extensions	Mustang Panda has leveraged Visual Studio Code's (VSCode) embedded reverse shell feature using the command code.exe tunnel to execute code and deliver additional payloads.
T1608		Stage Capabilities	Mustang Panda has used servers under their control to validate tracking pixels sent to phishing victims.
	.001	Upload Malware	Mustang Panda has hosted malicious payloads on DropBox including PlugX. Mustang Panda staged malware on adversary-controlled domains and cloud storage instances during RedDelta Modified PlugX Infection Chain Operations.
T1553	.002	Subvert Trust Controls: Code Signing	Mustang Panda has used valid legitimate digital signatures and certificates to evade detection. Mustang Panda used legitimate, signed binaries such as inkform.exe or ExcelRepairToolboxLauncher.exe for follow-on execution of malicious DLLs through DLL search order hijacking in RedDelta Modified PlugX Infection Chain Operations.

Attack ID		Technique Name	Description
T1218	.004	System Binary Proxy Execution: InstallUtil	Mustang Panda has used InstallUtil.exe to execute a malicious Beacon stager.
	.005	System Binary Proxy Execution: Mshta	Mustang Panda has used mshta.exe to launch collection scripts.
	.007	System Binary Proxy Execution: Msiexec	Mustang Panda initial payloads downloaded a Windows Installer MSI file that in turn dropped follow-on files leading to installation of PlugX during RedDelta Modified PlugX Infection Chain Operations.
	.014	System Information Discovery	Mustang Panda has gathered system information using systeminfo. Mustang Panda captured victim operating system type via User Agent analysis during RedDelta Modified PlugX Infection Chain Operations.
T1016		System Network Configuration Discovery	Mustang Panda has used ipconfig and arp to determine network configuration information.Mustang Panda has also utilized SharpNBTScan to scan the victim environment.
T1049		Traffic Signaling	Mustang Panda has utilized a magic value in C2 communications and only executes in memory when response packets match specific values of "17 03 03" or "46 77 4d".
T1204	.001	User Execution: Malicious Link	Mustang Panda has sent malicious links including links directing victims to a Google Drive folder.Mustang Panda has also utilized webpages with Javascript code that downloads malicious payloads to the victim device. Mustang Panda distributed hyperlinks that would result in an MSC file running a PowerShell command to download and install a remotely-hosted MSI file during RedDelta Modified PlugX Infection Chain Operations.
	.002	User Execution: Malicious File	Mustang Panda has sent malicious files requiring direct victim interaction to execute. Mustang Panda has also leveraged executable files that display decoy documents to the victim to provide a resemblance of legitimacy with customized themes related to the victim. Mustang Panda distributed malicious LNK objects for user execution during RedDelta Modified PlugX Infection Chain Operations.
T1102		Web Service	Mustang Panda has used DropBox URLs to deliver variants of PlugX.Mustang Panda has also used Google Drive to host malicious downloads.
T1047		Windows Management Instrumentation	Mustang Panda has executed PowerShell scripts via WMI

Recommendations

Advanced Email Filtering

- Use security tools that scan links (especially to cloud services like Google Drive/Azure) and utilize sandboxes to detonate and check attachments.

USB Device Control

- Implement strict policies to restrict removable media usage and monitor endpoints for unauthorized USB activity or the presence of the SnakeDisk worm.

Segment Your Network

- Isolate critical systems to ensure that if one zone is compromised, the attacker cannot easily pivot or reach sensitive information.

Patch and Harden Systems

- Regularly update operating systems, applications, and network devices to remediate known vulnerabilities. Prioritize critical systems, including government, defense, and telecommunications platforms.

Control Administrative Privileges

- Limit administrative rights and implement role-based access control to reduce the risk of credential misuse. Enforce multi-factor authentication (MFA) for all remote and privileged accounts.

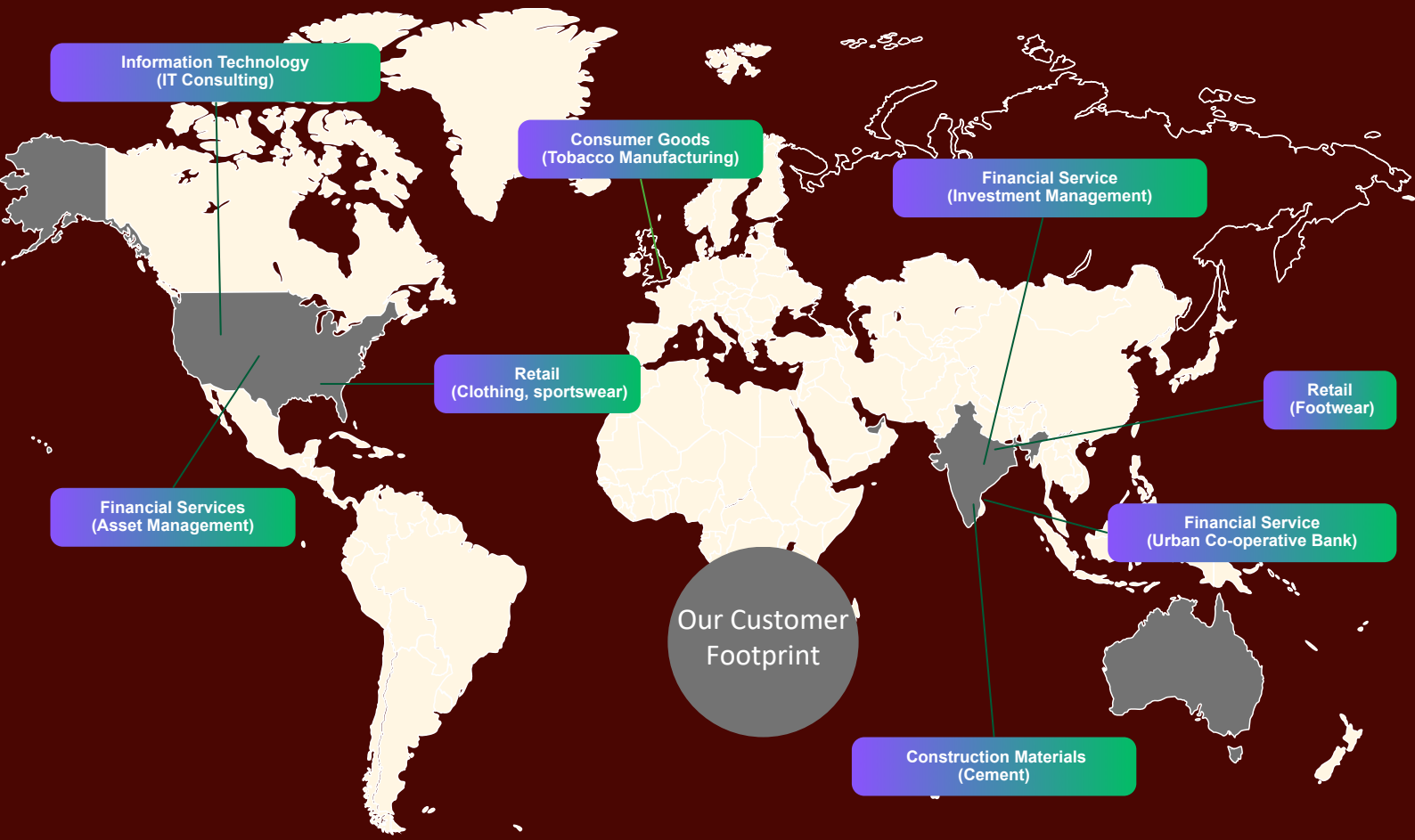
References

- https://attack.mitre.org/groups/G0129/
- https://cyble.com/threat-actor-profiles/mustang-panda/
- https://www.picussecurity.com/resource/blog/breaking-down-mustang-panda-windows-endpoint-campaign
- https://www.acronis.com/en/tru/posts/mustang-panda-targets-indias-government-and-energy-sectors/#3L5_YxHgSb
- https://www.linkedin.com/posts/smica83_mustangpanda-shardloader-minirecon-ugcPost-7477424316477992961-3eJ8/?utm_source=share&utm_medium=member_desktop&rcm=ACoAAD5j8xoBXAbLLUGwb1aPebVq9js1QihViEc

About Castellum Labs

- Services delivered by Global Cyber Capability Center using advance Platforms
- Based in Hyderabad, India with global customer base across India, US, Europe
- Strong Handpicked Team of 50+ with (best of security talent globally)
- Started by people with decades of product, services & deep tech experience
- Subscription & annual contract modeled services delivered globally
- Value + Impact from Day One, No Installation & No Deployment

100's of Satisfied Customers Across the Globe!



Cyber Security Portfolio

Secure Cloud WL

- Design Security for Cloud
- Cloud Security Posture
- DevOps Infra Security
- Container Security
- Kubernetes Security
- Integrated S/W Security
- Workload Hardening
- Security Automation
- Cloud Native Monitoring
- Cloud Governance

We create secure cloud environments, automate Cloud SecOps & manage it.

24x7 Monitoring

- MDR, 24x7 Monitoring
- SOC as a Service
- SIEM/SOC Design & Impl
- SOC Team on Hire
- Managed Incidents
- IR Process Designs
- IR Workshops
- SOC Assessments
- Threat Hunting Services
- Forensic Services

When it comes to SOC Monitoring & Response, we cover all aspects of it

Vuln Mgmt

- Application Security
- Network VAPT
- Cloud VAPT
- Controls & Config Audit
- Program Design for VAPT
- Managed Vuin Programs
- VAPT Automations
- Surface Assessments
- Threat Intel for VAPT
- DevSecOps

Program designed VAPT Engagement to enhance protection & reduce attack surface

Threat Intel

- Threat Intel Solutions
- Darkweb Hunting
- Deep Intel Reports
- Threat Intel Integrations
- Intelligence Automations
- Threat Intel Curation
- Vectored Searches
- Data Hunting
- Threat Intel Architecture
- Adversary Tracking

We take threat intel maintenance, keep, usage & application to next level.

Data & Privacy

- Data Security Design
- Data Sec Posture Assmnt
- Data Sec Posture Mgmt
- Encryption Design & Sol
- Data Exfiltration Assmnt
- Privacy Designing
- Privacy Gap Assessment
- Privacy Adoption Service
- Privacy Automations
- Privacy Compliances

Data and privacy are two considerations, we design, implement it & run compliances

Unified View of Security ...

#1 Orchestration & Automation

Automated governance
SecOps automation
Automated response

#2 Attack Surface Reduction

Inline AS detection
External AS validation
Continuous remediation

#3 Real Time Detection & Response

Real time detection
Active threat hunting
Proactive responses

#4 Zero Trust Micro Architecture

Zoning and isolations
Contextual runtime set
Transient access model

Castellum Labs

www.castellumlabs.com

Castellum Labs

reach@castellumlabs.com

+91 7842046995