रक्षा लेखा महानियंत्रक
Controller General of Defence Accounts
उलान बटार रोड, पालम, दिल्ली छावनी-110010
Ulan Batar Road, Palam, Delhi Cantt – 110010
(सू.प्रौ.एवं प्र. विंग)/(IT&S Wing)
Phone- 011-25665588, 25665591
e-mail: cybercell.cgda@gov.in

विकसित भारत अभियान 1947 TO 2047

SECRET

No. Mech/ IT&S/810/Cyber Security/Advisory-A Dated: 30.12.2025

To,

The Dy. CISOs,
All PCsDA/CsDA

Subject: Accountable Intelligence for Strengthened Threat Detection and Rapid Response.

Input from reliable government agency indicates that they have received an alert in which it has come to notice that numerous domains, subdomains and IP addresses were registered by state-sponsored threat actors, to target government, Defence, and central investigation agencies through advanced cyber operations. Details are placed at Annexure-I.

2. The following actions are to be undertaken with immediate effect for improved detection and protection across the organisation:

a. ***Enforce proactive monitoring and blocking of the indicators or filtering protocols to restrict access to the identified malicious domains and IPs and protect against the potential future spear-phishing. Additionally, perform comprehensive examinations of network logs and security alerts to detect any potential indicators of compromise.***
b. ***Enhance employee awareness and training programs to educate staff about the risk associated with interacting with suspicious emails, links, or attachments.***
c. ***You are encouraged to disseminate this alert among pertinent stakeholders within your area of responsibility for early detection and swift response measures.***

3. Any additional information pertaining to the shared indicators of compromise/attack (IoCs/IoAs) observed may please be shared with this office to take up the matter with Advisor (Cyber) for strengthening of threat intelligence and analysis.

4. For your kind consideration and necessary action please.

Encl.: As above.

Shashi

Dy. CGDA (IT&S)

Annexure-I

Network indicators	e-mail Alert details (Date & ID)	Other Details
api.indiandefence.services dan.indiandefence.services de.indiandefence.services emv1.indiandefence.services ftp.indiandefence.services home.indiandefence.services mail.indiandefence.services mail1.indiandefence.services mea.gov.indiandefence.services mea.gov.in.indiandefence.services mobile.indiandefence.services mx0.indiandefence.services office.indiandefence.services pay.indiandefence.services store.indiandefence.services ups.indiandefence.services usps.indiandefence.services vpn.indiandefence.services vps.indiandefence.services web.indiandefence.services webmail.indiandefence.services www.emv1.indiandefence.services www.mea.gov.in.indiandefence.services	CMTX-I-654112025 Dated 17/11/2025	Malicious domains created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, email-based fraud and command & control (C&C) server. NIC may consider sharing the IOCs/IOAs (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing campaigns.
155.117.42.144 208.110.72.195 sharemaxme26.net sharemaxme66.net	CMTX-I-007112025 Dated 18/11/2025	Command and control server of **Crimson RAT** malware used by Pakistan based threat actors to target government officials. NIC may consider sharing the IOCs/IOAs (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
93.127.128.118	CMTX-I-982112025 Dated 19/11/2025	Command and control server of **Crimson RAT** malware used by Pakistan based threat actors to target government officials. NIC may consider sharing the IOCs/IOAs (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
45.155.54.253	CMTX-I-999112025 Dated 19/11/2025	Command and control server of **BeastRAT** (Linux variant) malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
lionsdenim.xyz (currently resolving to 67.223.118.206) 185.235.137.90	CMTX-I-886112025 Dated 20/11/2025	Command and control server of **AresRAT** malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
teamindia.quest chuchuchacha.shop	CMTX-I-021112025 Dated 21/11/2025	Command and control server of **BeastRAT** (Linux variant) malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.

209.200.246.43	CMTX-I-201112025 Dated 21/11/2025	Command and control server of **Crimson RAT** malware used by Pakistan based threat actors to target government officials. NIC may consider sharing the IOCs/IOAs (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
wmiprovider.com dns.wmiprovider.com update.wmiprovider.com aeroclubofindia.co.in (Compromised Domain)	CMTX-I-210112025 Dated 21/11/2025	Command and control server of **CurlBackRAT** malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
46.253.4.169 chuchuchachawin.bond	CMTX-I-003112025 Dated 21/11/2025	Command and control server of **BeastRAT** (Linux variant) malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
68.183.255.53 157.230.56.201 159.223.59.134 165.232.68.53 159.223.8.217 143.110.187.124 45.76.190.68 149.28.61.158 64.176.179.199 173.249.42.140 172.232.116.205 143.110.187.124	CMTX-I-300112025 Dated 21/11/2025	Command and control server of **Poseidon** malware associated Mythic Framework used by threat actors were identified. NIC may consider sharing this domain (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
csdindiagovin.site (currently resolving to 149.3.170.189)	CMTX-I-305112025 Dated 21/11/2025	Malicious domains created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spear-phishing, malware distribution, email-based fraud and command & control (C&C) server. NIC may consider sharing the IOCs/IOAs (TLP-RED) with their email security partners to proactively monitor and block it against potential future spear-phishing campaigns.

(TLP-RED) When should it be used? Sources may use (TLP-RED) when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further. How should it be shared? Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, LP: RED information is limited to those present at the meeting. In most circumstances, TLP: RED should be exchanged verbally or in person.