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

विकसित भारत अभियान

SECRET

No. Mech/ IT&S/810/Cyber Security/Advisory-A Dated: 08.10.2025

To,

The Dy. CISOs,
All PCsDA/CsDA

Subject: Advisory on Chinese Intelligence Operatives (CIOs) and Suspected Chinese Entities (SCEs) based threat actors.

Input from reliable government agency indicates that they have received an alert vide the above regarding the act of some Chinese Intelligence Operatives (CIOs) and Suspected Chinese Entities (SCEs) which are actively engaged in collecting sensitive information pertaining to India's national security, defence establishment, critical infrastructure and government functioning etc.

2. **Modus Operandi**:

a. **Use of Job Portals:** The Hongkong based CIOs and other SCEs have been reported using LinkedIn, Naukri.com to identify and recruit candidates with relevant experience particularly in the journalism and defense sectors. The shortlisted candidates are screened by Indian intermediaries and then sent to SCEs for final selection and placement.

b. **Tasks assigned to the recruited candidates:** The selected candidates were assigned the task of writing source-based articles, covering strategic topics such as India-China relations, QUAD, SCO, G20, war experience, Indo-Pak conflict, Operation Sindoor, deployment of troops, weapon systems, latest defence procurement, joint military exercises such as Nomadic Elephant (Indo-Mongolia), Malabar Exercise (countries), war exercises (India-US) etc.

c. **Payment - Indian Intermediaries, Amount of Cybercrime and Indian Students Used:**
Initially $100 was paid for writing articles, which increased to $300-$400 depending on the quality of the report. Payments were usually made through Indian accounts or sometimes through overseas transfers. In one case, 1 lakh was paid by an Indian student studying in China. In another instance, an amount of 740,000 was paid to a journalist, which was received from a cryptocurrency fraud in which a person from Gujarat was duped of 8.5 lakh.

d. **Concealing Chinese Identity:** CIOs and SCEs describe itself as a representative of consulting firms based in Singapore, Hong kong and residents of Indonesia, Japan, Singapore, Macau, Malaysia, etc., to conceal their Chinese identity. The applicants recruited by Lee were paid and executed through Indian intermediaries. For example, two Indian entities, unaware of actual objectives were acting as local representatives of a Singapore-based consulting firm and found to be involved in screening and recruiting

P.T.O

applicants.

e. **Collecting data:** Documents such as PAN cards and Aadhaar cards of applicants with defence backgrounds were being collected through Indian intermediaries by a Singapore-based firm called 'Yonder Consulting', whose implications were unknown.

3. In view of above, it is requested to sensitize the personnel employed in your organisation regarding the modus of operandi being adopted by SCEs which is concern of national security.

4. For your kind consideration and necessary action please.

This issues with the approval of CISO, CGDA.

Shashi

Dy. CGDA (IT&S)

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

विकसित भारत अभियान

SECRET

No. Mech/ IT&S/810/Cyber Security/Advisory-A Dated: 08.10.2025

To,

The Dy. CISOs,
All PCsDA/CsDA

Subject: Advisory on Accountable Intelligence for Strengthened Threat Detection and Rapid Response and Circulation of Malicious PDF.

Input from reliable government agency indicates that they have received an alert in which it has come to notice that numerous domains and subdomains were registered by state-sponsored threat actors, to target government, Defence, and central investigation agencies Some of the domains observed are enclosed as Annexure-I and Annexure-II. Information pertaining to the same are also available on CERT-In's Threat Intel Exchange Platform. These domains are designed to steal email credentials or distribute malicious software via cloned websites.

2. Further, an ongoing phishing email being received on 18 September 2025 evening with a malicious attachment disguised as **CDS_Directions_for_Tri-Services_and_Civil Dept.**

a) Brief findings of the static & dynamic analysis across multiple sandboxes showed below observations:

i. Attachment was a malicious PowerPoint Add-In (ppam).
ii. Exhibited persistence (registry/task scheduler), process injection & clipboard monitoring.
iii. Ransomware-like behaviour via Volume Shadow Copy manipulation.
iv. Confirmed as a dropper capable of opening backdoor access (linked to ransomware in past).
v. C2 communication with suspicious domain: securestore.it.com (198.54.125.47).
vi. File hash: 38d05a1235766e5606409651565c732177adc17a42011be70422ffe74aebbcb.

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

a. ***Enforce blocking or filtering protocols to restrict access to the identified malicious domains. 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.***

P.T.O

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

5. For your kind consideration and necessary action please.

This issues with the approval of CISO, CGDA.

Encl.: As above.

Sharthi

Dy. CGDA (IT&S)

Advisor (cyber)/5(01)/IR/2025-/667 dt° 19/09/2025 ANNEXURE-I

SECRET

Annexure – I

Network indicators	e-mail Alert details (Date & ID)	Other Details
post-branch.in mail-branch.in post-sec.in	CMTX-I-100082025 dated 28/08/2025	Potential phishing/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. May consider sharing this domain with their email security partners to proactively monitor and block it against potential future spear-phishing campaigns
54.144.107.42 boss-servers.gov.in.indian bosssysterns.ddns.net indianbosssysterns.ddns.net In.indianbosssysterns.ddns.net gov.in.indianbosssysterns.ddns.net	CMTX-I-005092025 dated 01/09/2025	Command and control server of Linux variant malware used by Pakistan based threat actors to target government officials.May consider blocking and monitoring the DDNS domain: ***ddns.net.*** Please note that the parent domain is not malicious but PAK/CN based threat actor abuse its subdomain for cyber espionage campaigns. Additionally, kindly refer to previous alerts for **DDNS** domains: - CMTX-I-761082023 dated 31st August, 2023 - CMTX-I-119092023 dated 01st September, 2023 - CMTX-I-355092023 dated 07th September, 2023 - CMTX-I-512032024 dated 07th March, 2024 - CMTX-I-563122024 dated 16th December, 2024
cloudstore.carn 2ndline. cfd 5.178.0.29	CMTX-I-820092025 dated 02/09/2025	BeastRAT (Linux variant) is a new family of multi-platform malware compiled in the Go programming language. It includes binaries targeting both Windows- and Linux-based systems. The malware is deployed as the final payload in a multi-stage distribution campaign, using a decoy document as a lure.
seeconnectionalive.website	CMTX-I-866092025 dated 02/09/2025	BeastRAT (Linux variant) is a new family of multi-platform malware compiled in the Go programming language. It includes binaries targeting both Windows- and Linux-based systems. The malware is deployed as the final payload in a multi-stage distribution campaign, using a decoy document as a lure.

cases.airforce	CMTX-I-255092025 dated 03/09/2025	Potential phishing/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. May consider sharing this domain with security partners to proactively monitor and block it against potential future spear-phishing campaigns
www.email.gov.in.publications.it email.gov.in.publications.it www.sewa.gov.in.ansupport.store indianvisaonline.gov.in.statuswebsite.com cashkhelo.xyz *.publications.it *.in.ansupport.store *.in.statuswebsite.com	CMTX-I-265092025 dated 04/09/2025	Phishing/malicious domains created with the intent to harm, deceive, or exploit users. These domains are being used for spear-phishing, malware distribution, email-based fraud and command & control (C&C) server. May consider sharing this domain with security partners to proactively monitor and block it against potential future spear-phishing campaigns.
cbi.nicgov.cloud cbi.it.com nicgov.cloud	CMTX-I-268092025 dated 04/09/2025	Phishing/malicious domains created with the intent to harm, deceive, or exploit users. These domains are being used for spear-phishing, malware distribution and email-based fraud. May consider sharing this domain with security partners to proactively monitor and block it against potential future spear-phishing campaigns.
46.30.188.13 mha-gov.ink mea.nic-cloud.digital nic-cloud.digital **SHA1 Hashes** d30359284672d5f7f2d8f762fa918fe93cd34483 f28eba4919e56bf75de21710990978377347717l 18b635f0f231048aa3ca910690812c06f2f9e379 b8aa1f82be9f152a6fb3125513759ac2793e17c2	CMTX-I-821092025 dated 08/09/2025	SteganoRAT is a newfamilyof malware developed in .NET, featuring multiple layers of overlays. It is deployed using steganography techniques, with the malicious code hidden within a decoy file. SteganoRAT serves as the final payload in a multi-stage distribution campaign, designed to evade detection and facilitate persistent infection.
cgda.site defence.cgda.site	CMTX-1-335092025 dated 08/09/2025	Potential phishing/malicious domains created with the intent to harm, deceive, or exploit users. These domains can be used in various cyberattacks, including spearphishing, malware distribution, email-based fraud and command & control (C&C) server. May consider sharing this domain with security partners to proactively monitor and block it against potential future spear-phishing campaigns

Adv.Sor(cyber)|S(G1)|IR|2025|683 dt. 25/09/2025

Annexure -II

Network indicators	e-mail Alert details (Date & ID)	Other Details
award-data-portal.info www.award-data-portal.info	CMTX-I-975092025 Dated 09/09/2025	Potential phishing/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 this domain ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing campaigns.
83.147.38.102 milaostore.com	CMTX-I-765092025 Dated 09/09/2025	Command and control server of CrimsonRAT malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
dgqadefence.in finmin-in.org	CMTX-I-100092025 Dated 09/09/2025	Potential phishing/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 this domain ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing campaigns
pagamento.milaostore.com seguro.milaostore.com	CMTX-I-766092025 Dated 10/09/2025	Command and control server of CrimsonRAT malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
144.172.103.208	CMTX-I-806092025 Dated 10/09/2025	Command and control server of CrimsonRAT malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.

Annexure

104.21.55.41 atmaniirbhar.in cbwee8fhuj4jzjj.sansdesk.in download.igod.info fakehyperelax.igod.info files.igod.info helicopter.sansdesk.in hostmaster.igod.info igod.info kavach.igod.info keystone.igod.info ndc.atmaniirbhar.in rafalekiller.igod.info sansdesk.in shivani.igod.info uxthgtequkighv.igod.info www.igod.info	CMTX-I-892092025 Dated 12/09/2025	Command and control server of malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
d2i8rh3pkr4ltc.cloudfront.net ingov.myartsonline.com	CMTX-I-947092025 Dated 15/09/2025	Command and control server of GitRAT malware used by Pakistan based threat actors to target government officials. NIC may consider sharing this domain ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
newforsomething.rest setchartron.site winsoft.setchartron.site	CMTX-I-101092025 Dated 16/09/2025	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 ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
179.43.186.228	CMTX-I-253092025 Dated 16/09/2025	Command and control server of Poseidon malware associated Mythic Framework used by threat actors were identified. NIC may consider sharing this domain ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing and cyber espionage campaigns.
hciaccounts.in	CMTX-I-854092025 Dated 18/09/2025	Potential phishing/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 this domain ([redacted]) with their email security partners to proactively monitor and block it against potential future spear-phishing campaigns

[redacted] When should it be used? Sources may use [redacted] 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.