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

विकसित भारत अभियान 1947 TO 2047

Important Circular
02/2026

No. Mech/ IT&S/810/Cyber Security/Circular Dated: 06.03.2026

To,
The Dy. CISOs,
All PCDA/CDA Offices

Subject: Cyber Security related instructions.

For effective monitoring and strengthening of cyber security framework of our organisation, numerous advisories have been issued from time to time by HQrs office. This circular highlights the Cyber Security incidents reported by the various investigating agencies and suggestions to prevent the incidents in the recent past.

2. Various nature of incidents reported are given below:
   i. **Phishing Domains:** Numerous domains and subdomains were registered by state-sponsored threat actors to target government, defence, and central agencies.
   ii. **Spurious/ suspicious phone calls**: There have been attempts through phone claiming to be Under Secretary from National Cyber Security.

3. Necessary advisories issued by HQrs Office regarding prevention of the above incidents are given in the table below:

Sl. No.	ADVISORY	DATE
1.	Advisory regarding spurious/ suspicious calls	18.02.2026
2.	Actionable Intelligence for Strengthened Threat Detection and Rapid Response.	18.02.2026

4. **Latest Update**:

a. Inputs indicate that the multiple hacktivist groups are carrying out cyber-attack campaign against Indian websites and ICT infrastructure in India. In this regards, detailed advisory is placed at **Annexure-'A'** to this letter.

b. It was observed that some **phishing emails** were currently being circulated, bearing varying subject lines and containing password protected attachments or similar variants. An Advisory regarding this bearing letter no. Mech/IT&S/810/Cyber Security/ Advisory–A dated 20.02.2026 was circulated on CGDA website. Further, Cert-In has also issued advisory on phishing attack which is enclosed at **Annexure-'B'** to this letter.

5. In view of the above, it is requested that all the attached and subordinate offices under your administrative purview may be informed about the guidelines/advisories for necessary action.

6. This issues with the approval of the CISO, CGDA.

Encl: As above.

Sr. ACGDA (~~IT~~&S)
6/3/26

Annexure-

CERT-In Advisory

Cyber-attack campaigns against Indian websites and ICT infrastructure (CIAD-S-2025-10)

Original Issue Date: December 20, 2025

Severity Rating: Critical

It has been observed that multiple hacktivist groups are carrying out cyber-attack campaigns against Indian websites and ICT infrastructure in India.

The primary tactics of hacktivist group has been web-based DDoS, targeted attack and website hacking from public cloud servers, hiding attack sources behind and across thousands of unsecured HTTPS/SOCKS proxies. The attacks have been characterized by Web based DDoS attacks combined with alternative waves of UDP and SYN floods.

Organisations are requested to strictly monitor their ICT infrastructure and report any incident to CERT-In immediately.

Measures for prevention of Web intrusion attacks/Web Defacement

1. Use latest version of Web server, Database Server, Hypertext Processor (PHP).
2. Apply appropriate updates/patches on the OS and Application software
3. Conduct complete security audit of web application, web server, database server periodically and after every major configuration change and plug the vulnerabilities found.
4. Validate and sanitize all user input, and present error messages that reveal little or no useful information to the user to prevent SQL injection attacks.
5. Enable and maintain logs of different devices and servers and maintain the same for all the levels. vi. Use Web Application Firewall (WAF), Security Information and Event Management (SIEM) and/or Database Activity Monitoring (DAM) solutions.
6. Search all the websites hosted on the web server or sharing the same DB server for the malicious web shells or any other artefact.
7. Periodically check the web server directories for any malicious/unknown web shell files and remove them as and when noticed.
8. In order to identify Web shells, scan the server with Yara rules
9. Change database passwords of all the accounts available in the compromised database Server. Also change the passwords/credentials stored in the databases present on the database server.
10. Use an application firewall to control input, output and/or access to the web application.
11. Limit the file types allowed to be uploaded to the web server by using a list of predetermined file types. Define permissions on the directory the files are uploaded into, to prevent attackers from executing the files after upload.
12. Consider using File Integrity Monitoring (FIM) solution on web servers to identify unauthorized changes to files on the server.

Measures for prevention of Denial of Service (DoS/DDoS) attacks

1. Identify critical services and their priority. Have a Business Continuity Plan and Disaster Recovery Plan ready for activation in case of emergency.
2. Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.

3. Employ defence-in-depth strategies: emphasize multiple, overlapping and mutually supportive defensive systems to guard against single point failures in any specific technology and protection method.
4. Enable adequate logging mechanisms at perimeter level, server and system level and review the logs at frequent intervals. Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks.
5. Thoroughly scan the network and online applications and plug any existing vulnerability in the network devices, Operating Systems, Server software and application software and apply latest patches/updates as applicable.
6. Deploy appropriate Intrusion/DDoS Prevention System capable of detecting and mitigating DDoS attacks. Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common attack tools.
7. Continuously monitor the network activities; server logs to detect and mitigate suspicious and malicious activities in your network. Review the traffic patterns and logs of perimeter devices to detect anomalies in traffic, network level floods (TCP, UDP, SYN, etc.) and application floods (HTTP GET) etc.
8. Maintain and regularly examine logs of webservers to detect malformed requests/traffic.
9. Preserve all logs indicating type of attack and attack sources.
10. Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common DDoS tools.
11. Maintain list of contacts of ISPs, vendors of network and security devices and contact them as appropriate.
12. Sudden surge in inbound traffic to any critical server or services, such as ICMP floods, UDP/TCP flood etc. could be due to Distributed Denial of Service (DDoS) attacks. If such attacks are observed, implement appropriate response measures in coordination with Internet Service Provider (ISP). In case of high volume of DDoS, consult your ISP to block attack sources and apply appropriate rate limiting strategies.
13. Implement Egress and Ingress filtering at router level.
14. Implement a bogon block list at the network boundary.
15. In case your SLA with ISP includes DDoS mitigation services instruct your staff about the requirements to be sent to ISP.
16. Identify the attack sources. Block the attack sources at Router/Packet filtering device/DDoS prevention solutions. Disable non-essential ports/services.
17. To counter attacks on applications, check the integrity of critical application files periodically and in case of suspicion of attack restore applications and content from trusted backups.
18. Allocate traffic to unaffected available network paths, if possible, to continue the service.

Measures for prevention of Malware Attacks

1. Block/restrict connectivity to the malicious domains/IPs shared by CERT-In from time to time. If any of the machines are found contacting them, take volatile evidence, isolate the machine, start necessary mitigation and containment procedures. Take forensic image of the machine for root-cause analysis. It is recommended to restore the system from a known good back up or proceed to a fresh installation.
2. Keep up-to-date patches and fixes on the operating system and application software such as client-side software, including Adobe Products (Reader, Flash player), Microsoft Office suite, browsers, JAVA applications.
3. Restrict execution of PowerShell/WSCRIPT in enterprise environment. Ensure installation and use of the latest version of PowerShell, with enhanced logging

enabled, script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

4. Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.
5. Control outbound DNS access. Permit internal enterprise systems to only initiate requests to, and receive responses from, approved enterprise DNS caching name servers. Monitor DNS activity for potential indications of tunnelling and data exfiltration, including reviewing DNS traffic for anomalies in query request frequency and domain length, and activity to suspicious DNS servers. The dnscat2 tool alternates between CNAME, TXT, and MX records when it is operating. Investigate abnormal amounts of these records going to the same second level domain, or a group of second level domains.
6. Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
7. Enhance the Microsoft Office security by disabling ActiveX controls, Macros, Enabling protect View, File Protection Settings.
8. Apply software Restriction policies appropriately. Disable running executables from unconventional paths.
9. Protect against drive-by-downloads through controls such as Browser JS Guard.
10. Leverage Pretty Good Privacy (PGP) or GnuPG in mail communications. Additionally, advise the users to encrypt/protect the sensitive documents stored in the internet facing machines to avoid potential leakage.
11. Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
12. Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header). Block the attachments of file types (exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf)
13. Consider configuring mandatory 2 Factor authentication if using VPN services to access organizational networks. It is recommended to consider an additional form of authentication, prior to granting access to internal network resources.
14. Consider limiting users' access using VPN services to a single IP address at a time. No multiple simultaneous remote accesses by the same user should be allowed.
15. Consider Geo-limiting users access to known geographical locations. Use Geolocation analysis to identify impossible connections, such as a user calling from 2 points geographically remote in a short period of time.
16. Check if the VPN software writes session data to the remote workstations disk. If possible, use a connection method that keeps the data in memory only, preferably encrypted.
17. Maintain up-to-date antivirus signatures and engines.
18. Restrict users' ability (permissions) to install and run unwanted software applications.
19. Enforce a strong password policy and implement regular password changes.
20. Enable a personal firewall on workstations.
21. Disable unnecessary services on workstations and servers.
22. Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
23. Scan all software downloaded from the Internet prior to executing.
24. Maintain situational awareness of the latest threats; implement appropriate ACLs.

Mitigation and Recommendations for Infra/Server team:

1. Update and patch software: Ensure that all software, including the content management system (CMS), plugins, and themes, are updated to their latest versions. Apply any necessary patches to fix known vulnerabilities.
2. Change passwords: Reset passwords for all user accounts, especially those with administrative privileges. Use strong, unique passwords and enable two-factor authentication (2FA) where possible.
3. Clean and secure the database: Check for any unauthorized changes or injected content in the database. Repair any damage and implement security measures to protect the database from future attacks.
4. Implement security best practices: Follow website security best practices, such as proper file permissions, secure configuration, input validation, and output encoding.
5. Monitor website activity: Regularly monitor website activity and server logs to detect any unusual or suspicious behaviour.
6. Install a web application firewall (WAF): A WAF can help protect your website from various types of attacks by filtering and monitoring HTTP traffic between the web application and the Internet.
7. Perform regular backups: Ensure that regular backups of the website and database are taken and stored securely offsite. This will help in the recovery process if any issues arise in the future.
8. Conduct a security audit: Carry out a comprehensive security audit of the website to identify vulnerabilities and weaknesses that could be exploited by attackers. Address any issues found and implement necessary security measures.

Also, the "Guidelines on Information Security Practices for Government Entities" shall be followed for hardening of ICT infrastructure:

URL: https://cert-in.org.in/PDF/guidelinesgovtentities.pdf.