CIS Governance Division
Cyber and Information Security Group,
National Informatics Centre,
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
csg-advisory@nic.in

NIC-CISG/2025-07/130
Dated: 30-07-2025
Severity: High

Special Advisory for Independence Day

A. Description:

It has been observed that a coordinated cyber threat campaign involving multiple Hacktivist groups is expected to launch attacks against Indian cyberspace on Independence Day. Historically, such groups have been active during national festivals and have typically executed three main types of attacks: Distributed Denial of Service (DDoS), website defacements, and data breaches, often followed by the publication of stolen data. In this regard all are advised to stay on high alert and ensure proper cyber security hygiene and best practices are followed both at Client level (i.e., desktop, laptop etc.) and at the Application, Database, Server, Data Centre & Network level..

These attackers commonly utilize a range of open-source and publicly available tools to carry out DDoS attacks across various network layers, including Layer 3 (Network), Layer 4 (Transport), and Layer 7 (Application). The tactics employed include direct DDoS attacks targeting individual servers, as well as DNS amplification attacks designed to overwhelm the victim's network with excessive traffic.

The Primary Attack Vectors used by these groups are: -

1. **Website Defacement:** Disruption of websites with political messages, propaganda, or symbolic imagery
2. **DDoS Attacks:** Targeted denial-of-service attacks causing website and service outages
3. **Data Exfiltration:** Theft of sensitive data from compromised systems

B. Mitigation measures against Website Defacement:

- Properly configure and secure internet-facing network devices, disable unused or unnecessary network ports and protocols on VPN servers/ Email servers and recommended to monitor any anomalous application behaviours [new user creation] and unknown connections in the network traffic. Enforce MFA for all users and on all VPN connections and regularly review, validate, or remove privileged accounts.
- SOC Team should be kept on alert to monitor all web facing interface for any suspicious activity.

- Keep the entire application stack up-to-date: This includes ensuring that the web server (e.g., Apache, Nginx, IIS), application server (e.g., Tomcat, Node.js), and content management system (CMS) (e.g., WordPress, Joomla, Drupal) are using the latest, secure versions. Apply security updates and patches promptly to the operating system, CMS, and application software as they become available. Always obtain patches from official and trusted channels to minimize the risk of malicious modifications.
- Secure plugins and third-party components: Vulnerable or outdated plugins (or extensions) can serve as entry points for attackers, leading to website defacement or other malicious activities. Regularly update or patch all active plugins and remove any unused or unnecessary ones. Ensure that plugins are sourced from reputable developers and avoid using plugins with known security flaws.
- Regularly conduct code reviews and use static analysis tools to identify weaknesses.
- Use a WAF to filter out malicious traffic and block attacks like SQL injection or cross-site scripting.
- Strict enforcement policies on popular Content Management systems (CMS) such as regular patching of CMS applications and its plug-ins such as file mangers, disabling of unused plugins, 2- Factor authentication, adequate ACLs, File type & size Upload limit etc.
- Disable public access to server admin interfaces (e.g., phpMyAdmin, Adminer) by implementing IP whitelisting or requiring VPN access or .htaccess restrictions.
- Limit internal VPN access to trusted personnel only, using strong authentication and role-based access control (RBAC) to limit user permissions to necessary functions.
- Use HTTPS with TLS 1.3 or higher to encrypt data in transit.
- Periodically check the web server directories for any malicious/unknown web shell files, remove it as and when noticed. If found/ observed any such malicious activity, report the incident to CERT-In Incident Response Help Desk immediately. (Email: incident@cert-in.org.in)
- Enforce strict control and monitoring of Windows Native applications such as command-line, PowerShell, WinRM, Windows Management Instrumentation (WMI), and Distributed Component Object Model (DCOM).
- Enable and maintain logs of different devices and servers [Webserver Access/Error logs, Application/DB/ Firewall/IDS/FTP logs] and maintain the same for all the levels. Preserving of these logs help in analyzing the incidents and known the TTP of actors.
- Check for unnecessary connectivity towards Content Delivery Networks, as malware are known to tunnel the connection towards these domains to hide their traffic and towards DDNS / free top level domains. Regular auditing of the failed connection attempts from DNS logs, proxy logs and to successful connection towards unknown domains. Some of the attacks use unconventional usage of DNS queries to exfiltrate interact with the attackers [DNS TXT Records].
- Backup Data Regularly: Schedule regular backups of your website and databases to ensure quick restoration in case of an attack.
- Conduct complete security audit of web application, web server, and database server periodically and after every major configuration change and plug vulnerabilities found. Services of CERT-In empanelled auditors may be availed. (Refer Cyber security Assurance section on website of CERT-In https://www.cert-in.org.in/).

C. Measures for Detection of Attacks:

- Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.
- Enable adequate logging mechanisms at perimeter level, server, and system level and review the logs at frequent intervals.
- 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.
- Preserve all logs indicating type of attack and attack sources.

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

- 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.
- Business Continuity Plan (BCP) and Disaster Recovery (DR) Plan should be ready for activation in case of emergency.
- Asset inventory of all the assets under your control need to be maintained along with their risk posture i.e. latest VA score, application audit status.
- Defence-in-depth strategies i.e. multiple, overlapping and mutually supportive defensive systems should be adopted to guard against single point failures in any specific technology and protection method.
- 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.
- Ensure the deployment and proper configuration of a Web Application Firewall (WAF) to safeguard applications against Layer 7 (application layer) attacks.
- CDN (Content Delivery Network) services may be utilized to efficiently manage anticipated spikes in traffic volume, in coordination with the CCC Division of NIC.
- Application owner need to ensure that threshold-based rules to limit traffic spikes by IP, protocol, or application are configured at relevant security/network devices i.e. on firewalls and load balancers.
- Ensure that the application is provisioned with sufficient resources to efficiently handle legitimate user traffic, including anticipated usage peaks and minor traffic surges.
- Use CAPTCHA or challenge-response mechanisms to filter out automated bots.
- Restrict access to non-essential services or ports during high-risk periods.
- Use VPNs or secure tunnels for administrative access to critical infrastructure.

- Disable unused APIs or services that could be exploited.
- Filter malicious traffic at firewalls or routers based on IPs, ports, or protocols.
- Implement geofencing (where applicable), to reduce the attack surface by restricting website access only to authorized or necessary geographic regions or countries.
- Application owners must ensure continuous monitoring of application logs and incoming traffic for any unusual or suspicious activity. In addition, appropriate measures to be implemented for regular monitoring of the health and performance of all associated servers and infrastructure components under their control. This includes tracking key server metrics such as CPU usage, memory utilization, and storage capacity. Any detected anomalies or irregular patterns should be promptly reported to the security team at incident@nic-cert.nic.in

E. Protection Mechanisms against data breach:

- Conduct regular vulnerability assessments to identify potential weaknesses in your systems and networks that could be exploited by hacktivists.
- Isolating sensitive data into separate network segments limits access and reduces the scope of exfiltration risks. Use VLANs and firewalls to create secure zones for critical data.
- Implement RBAC (Role-Based Access Control) to limit data access based on job roles. Ensure employees only have the minimum access they need, reducing internal threats and unauthorized data movement.
- Implement secure configuration settings on systems and applications to make it more difficult for hacktivists to penetrate them.
- Encrypt sensitive data both in transit and at rest to protect against data interception and theft.
- MFA strengthens security by requiring additional verification methods (e.g., OTPs, biometrics) to access sensitive systems. It protects against credential theft, reducing the likelihood of unauthorized access.
- Conduct frequent audits of data access and monitor logs for suspicious activity. Real-time alerts can notify security teams of potential exfiltration attempts, enabling quick intervention.
- Regularly educate employees on data protection practices and how to recognize phishing or social engineering tactics. This reduces human error and insider threats related to data exfiltration.
- Regularly backup important data to minimize the impact of a hack-and-breach attack.
- Limit the number of external-facing services to reduce the attack surface and make it more difficult for hacktivists to find vulnerabilities.
- Monitor social media channels for any threats or activity related to hacktivism.
- Develop and test an incident response plan to quickly detect and respond to data breaches. The plan should include steps for containing, mitigating, and investigating potential data exfiltration incidents.

F. Reference:

Indian Computer Emergency Response Team (CERT-In)

https://www.cert-in.org.in/