CERT-In Advisory

Hacktivist Group campaign targeting Indian ICT Infrastructure (CIAD-2023-S3)

Original Issue Date: September 05, 2023

Severity Rating: Critical

Overview

Multiple Indonesian hacktivist groups including ‘Ganonsec’ and ‘Jambi Cyber Team’, have threatened to begin cyber-attack campaigns against websites and ICT infrastructure in India. The groups has solicited the support of other hacker groups around the world for this campaign.

The hacker groups have threatened via social media regarding future cyber-attacks in Indian cyber space as shown below:

Motivated campaigns like this could lead to a breach of sensitive information and disruption of services of organizations in Government and private sector.

Attack Vectors

According to observations, hacktivist groups have used DDoS (Distributed Denial of Service) to attack websites and ICT infrastructure in India and other countries. Hacktivist groups leverages various open-source, widely available utilities to conduct DDoS attacks at different network layers, including Layer 3, Layer 4, and Layer 7. The attacks include DDOS attacks directed at individual servers, as well as DNS-amplification attacks that direct a large volume of traffic toward a victim's network.

A similar attack campaign against Indian cyber space was carried out by hacker group called "Dragon Force Malaysia" against Indian websites in June 2022 under the attack campaign named “OpsPatuk”. The attacks were carried out by compromising servers used for shared hosting and then using web shells to maintain persistence on target organizations’ networks.

Another similar attack campaign against Indian cyber space was carried out by hacker groups named ‘Anonymous Sudan’, ‘Eagle Cyber Crew (Malaysia)’, ‘Mysterious Team’ in April 2023. The hacktivist group had employed DDoS (Distributed Denial of Service) for attacks on various universities, hospitals, and cybersecurity firms.

In the view of above attack campaigns, it is anticipated that the following server-side and client-side attacks could be employed in the attacks:

Server-Side Attacks

- Leveraging widely available tools for DDOS.
- Password spraying using compromised accounts on social media sites.
- Targeting hosting providers to gain unauthorized access to hosted websites.
- Local File Inclusion attacks on web applications.
- Compromising VPN credentials of vendors to conduct attack via supply chain

Client-Side Attacks

- Usage of Microsoft document exploits.
- Malware
- Phishing campaigns using SMS and WhatsApp messages with malicious files.

In light of these impending threats, it is important for Indian organizations to secure their websites, assets and endpoints to prevent further escalation of attacks. Any cyber security related incident observed be reported to CERT-In immediately. The measures

for prevention and mitigation of web intrusion attacks, DDoS attacks and malware attacks are provided below.

I. Measures for prevention of Web intrusion attacks/Web Defacement

i. Use latest version of Web server, Database Server, Hypertext Processor (PHP).

ii. Apply appropriate updates/patches on the OS and Application software

iii. Conduct complete security audit of web application, web server, database server periodically and after every major configuration change and plug the vulnerabilities found.

iv. 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.

v. 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.

vii. Search all the websites hosted on the web server or sharing the same DB server for the malicious web shells or any other artefact. viii. Periodically check the web server directories for any malicious/unknown web shell files and remove them as and when noticed.

ix. In order to identify Web shells, scan the server with Yara rules

x. 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.

xi. Use an application firewall to control input, output and/or access to the web application.

xii. 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.

xiii. Consider using File Integrity Monitoring (FIM) solution on web servers to identify unauthorized changes to files on the server.

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

i. Identify critical services and their priority. Have a Business Continuity Plan and Disaster Recovery Plan ready for activation in case of emergency.

ii. Understand your current environment, and have a baseline of the daily volume, type, and performance of network traffic.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. 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.

viii. Maintain and regularly examine logs of webservers to detect malformed requests/traffic.

ix. Preserve all logs indicating type of attack and attack sources.

x. Ensure that Intrusion/DDoS Prevention System contain signatures to detect the attacks launched from common DDoS tools.

xi. Maintain list of contacts of ISPs, vendors of network and security devices and contact them as appropriate.

xii. 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.

xiii. Implement Egress and Ingress filtering at router level.

xiv. Implement a bogon block list at the network boundary.

xv. In case your SLA with ISP includes DDoS mitigation services instruct your staff about the requirements to be sent to ISP.

xvi. Identify the attack sources. Block the attack sources at Router/Packet filtering device/DDoS prevention solutions. Disable non-essential ports/services. xvii. 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.

xvii. Allocate traffic to unaffected available network paths, if possible, to continue the service.

III. Measures for prevention of Malware Attacks

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

vii. Deploy Microsoft's Enhanced Mitigation Experienced Toolkit (EMET) which provides end node protection against zero-day vulnerabilities and blocks and prevents memory-based attack approaches.

viii. Enhance the Microsoft Office security by disabling ActiveX controls, Macros, Enabling protect View, File Protection Settings.

ix. Apply software Restriction policies appropriately. Disable running executables from unconventional paths.

x. Protect against drive-by-downloads through controls such as Browser JS Guard

xi. 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

xii. Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.

xiii. 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”

xiv. 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.

xv. 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.

xvi. 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.

xvii. 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.

xviii. Maintain up-to-date antivirus signatures and engines.

xix. Restrict users’ ability (permissions) to install and run unwanted software applications.

xx. Enforce a strong password policy and implement regular password changes.

xxi. Enable a personal firewall on workstations.

xxii. Disable unnecessary services on workstations and servers.

xxiii. Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).

xxiv. Scan all software downloaded from the Internet prior to executing.

xxv. Maintain situational awareness of the latest threats; implement appropriate ACLs.

Any cyber security related incident observed be reported to CERT-In immediately.