Advisory and Resource Facilitation
National Informatics Centre.
A-Block, CGO Complex, Lodhi Road,
New Delhi - 110003 India
IP No 5578
Csg-advisory@nic.in

NIC-CISG/2024-12/589
Dated: 23-12-2024

राष्ट्रीय सूचना विज्ञान केंद्र
National Informatics Centre

Special Advisory for Republic Day (Preventing DoS/DDoS Attacks)

Description:

The Republic Day Parade(RDP) and Beating The Retreat Ceremony(BTR)-2025 is schedule on 26 & 29 January 2025 at Kartavya Path and Vijay Chowk in New Delhi respectively. This is very prestigious and sensitive National event, which will attract the attention of malicious cyber threat actors with a view to impact the smooth conduct of the event thus causing harm to prestige of the Nation. The themes/programmes for Republic Day may be weaponized as threat vectors, well before the event as subjects of phishing emails etc. In view of the mentioned cyber threat, please find below:

Measures for prevention 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, e tc.) 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.