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/2024-12/587
Dated: 23-12-2024

राष्ट्रीय सूचना विज्ञान केंद्र
National Informatics Centre

Special Advisory for Republic Day (Preventing Malware 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 of Malware Attacks

1. Block/restrict connectivity to the malicious domains/IPs shared by various security agencies 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. 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.
8. Enhance the Microsoft Office security by disabling ActiveX controls, Macros, Enabling protect View, File Protection Settings.
9. Apply software Restriction policies appropriately. Disable running executables from unconventional paths.
10. Protect against drive-by-downloads through controls such as Browser JS Guard.
11. Leverage Pretty Good Privacy (PGP) or GnuPG in email communications.
12. Additionally, advise the users to encrypt/protect the sensitive documents stored in the Internet facing machines to avoid potential leakage.
13. Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
14. 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" Consider configuring mandatory two 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.
15. 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.
16. 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.
17. 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.
18. Maintain up-to-date antivirus signatures and engines.
19. Restrict users' ability (permissions) to install and run unwanted software applications.
20. Enforce a strong password policy and implement regular password changes.
21. Enable a personal firewall on workstations.
22. Disable unnecessary services on workstations and servers.
23. Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
24. Scan all software downloaded from the Internet prior to executing.
25. Maintain situational awareness of the latest threats; implement appropriate ACLs.