



रक्षा लेखा नियंत्रक का कार्यालय, गुवाहाटी उदयन विहार, नारंगी, गुवाहाटी-781171

OFFICE OF THE CONTROLLER OF DEFENCE ACCOUNTS
UDAYAN VIHAR, NARANGI, GUWAHATI: 781171.

ई-मेल/e-mail:cda-guw@.nic.in फ़ैक्स/FAX:0361-2640204 फोन/Ph: 0361-2640394, 2641142.



Circular No - 35

No. CDAGUW/IT&SW/11/WAN/2023

Date: 22/03/2023

To,

All the Section of MO CDA, Guwahati

All the Sub Offices under CDA, Guwahati


Subject:- Responding to Ransomware attack.

Reference:- HQrs Office letter No Mech/IT&S/810/Cyber Security Dated 16/03/2023

Please find the HQrs Office Circular under reference regarding direction to curtail Ransomware attack in vulnerable sections/terminals to avoid any unauthorized access of sensitive information through malware.

In this regard, it is advised to ensure compliance of guidelines issued by HQrs office strictly..

Encl: As mentioned above


(Dhiman Biswas)
AO (IT&SW)

“ हर काम देश के नाम ”

रक्षा लेखा महानियंत्रक

उलान बटाररोड, पालम, दिल्ली छावनी-110010

Controller General of Defence Accounts

Ulan Batar Road, Palam, Delhi Cantt.- 110010

(IT&S Wing)



Phone: 011-25665588, 2566589, 25665763 Fax: 011-25675030 email:cgdanewdelhi@nic.in

No. Mech/ IT&S/810/Cyber Security

Circular

Date: 16/03/2023

To

All PCsDA/CsDA/PCA(Fy)/PrIFA/IFA

Subject: Responding to Ransomware attacks.

Ministry of Defence (MoD Cyber cell) has issued directions in order to curtail the ransomware attacks. Ransomware is a category of malware that gains access to systems and makes them unusable to its legitimate users, either by encrypting different files on targeted systems or locking out the system unless a ransom is paid.

2. In order to sensitise everyone with respect to the measures to be taken in case of a Ransomware attack, following advisory is being issued. These are the prescribed steps to be followed in case of Ransomware attack:

A. Identify & Isolate :

- a) Identify systems which are affected or appear to be affected and isolate the identified systems from the network at the switch level.
- b) If it is not feasible to isolate the systems at the switch/network level, isolate the systems by making them offline.
- c) Unplug all the external storage and turn off any wireless functionality from the systems.

B. Contain:

- a) Identify and secure critical systems by temporarily restricting their access and isolation them from the network as an interim measure.
- b) Secure network backups by taking them offline immediately and temporarily disable all remote access to the network.
- c) Identify and eliminate all forms and sources of threats and disrupt threat actor activities like suspected IPs and domains and terminate malicious processes and stop malicious files , scheduled tasks etc. from being executed.

C. Hardening:

- a) Reset credentials of all the privileged local, VPN and domain accounts
- b) Implement multi-factor authentication wherever possible. Also force domain users to change credentials on every next login.
- c) Perform user access review and ensure access to only legitimate users.
- d) Close SMB, RDP and other unused ports in the network.
- e) Ensure deployment of latest patches on all systems.
- f) Deploy custom signatures to endpoint protection and network security tools based on discovered Indicators of compromises (IOCs) and ensure endpoint protection is up-to-date and enabled on all systems.

D. Preserve Artefacts & Sanitise systems:

- a) Record basic information like “Ransomware Note” text or image, encrypted file extensions etc.
- b) Obtain forensic image and capture memory of affected devices for further analysis and also collect relevant logs.
- c) Backup of the infected systems be kept so that in case a decryptor is made available in future, encrypted files could be decrypted.
- d) Use updated endpoint protection solutions (AV, EDR, XDR etc.) to sanitise systems. Systems should be only connected to network after ensuring they are infection free.

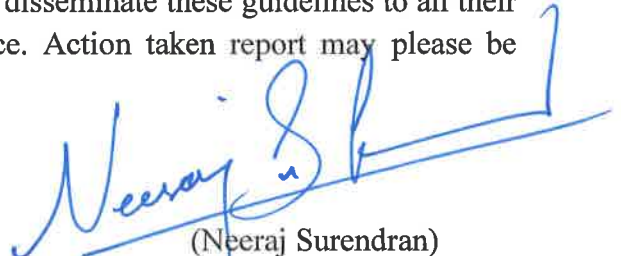
E. Securely Recover & Resume :

- a) Ensure that all the previous vulnerabilities and threats are eliminated and the systems are hardened.
- b) Affected systems may be recovered by:-
 - Restoring from a secure backup
 - Restoring from a previous secure restore point.
 - Rebuilding & re-installing from scratch
- c) When secure backups and restore points are not available, and rebuilding of the systems from scratch is the only available option, backups of encrypted critical system data should be taken.
- d) After restoration, scan with updated endpoint protection solutions to ensure no residual infections like backdoors etc. and review firewall configurations.
- e) Implement proper network segmentation to ensure isolation of various systems, segments & zones.

F. Monitor :

- a) Test each system, application and other components.
- b) Monitor the alerts from Security Information & Event Management (SIEM) solution, if available.
- c) Periodically analyze relevant logs and check for abnormal system behavior.
- d) Before fully resuming the systems to their pre-incident level, systems should be thoroughly tested to ensure they are functioning correctly and cyber threat has been neutralized.

3. In view of the above, all the Controllers are advised to ensure strict compliance of the guidelines given above and disseminate these guidelines to all their sections and sub offices for strict compliance. Action taken report may please be forwarded to this office at the earliest.



(Neeraj Surendran)
Sr. ACGDA (IT&S)