CONTROLLER GENERAL OF DEFENCE ACCOUNTS – IT&S
ULAN BATAR ROAD, PALAM, DELHI CANTT – 110010
Phone : 011-25665761-63 Fax : 011-25675030
Website : http://cgda.nic.in
Email : cgdanewdelhi@nic.in

No Mech/IT&S/810/Cyber Security Dated : 15/05/2017

To
All PCsDA / CsDA/ PCA (fys)

Subject : Security Measures : Out Break of Ransomware – WannaCry and Microsoft OS Vulnerability.

There is a global ransomware attack on the several countries. As per the message of CERTIN, following immediate measures are to be taken :

1. Blocking of Port 445 TCP / UDP
    a. On all UTMs – Action by security configuration team of Cyber Security Group.
    b. Blocking Port 445 TCP / UDP at internet gateway level : Action by Network group
2. Patching the vulnerability (Microsoft Security Bulletin MS17-010) On endpoints –
    a. It may be confirmed from Antivirus OEM, the availability of required signature for securing against the Ransomware. The signature s are available and the same are being ensured to be pushed to the respective antivirus management servers.
    b. For systems managed using the centrally managed patch management solution The control team will ensure that the patches are pushed to the endpoints on IMMEDIATE basis.
    c. The respective Network / Security Administrators should ensure that the patch is available for update by the endpoints.

Contd. . . .

NIC has suggested the Best practices to prevent ransomware attacks as follows:

- Maintain updated Antivirus software on all systems
- Check regularly for the integrity of the information stored in the databases.
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems
- Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Don.t open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization.s website directly through browser
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.
- Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
- Disable remote Desktop Connections, employ least-privileged accounts.
- If not required consider disabling, PowerShell /windows script hosting.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- 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
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empaneled auditors. Repeat audits at regular intervals.

- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies

Am I protected against this threat?

In order to prevent infection, users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010.

https://technet.microsoft.com/library/security/MS17-010

For any further detail on the same you can visit Indian Computer Emergency Response Team website at

http://cert-in.org.in/s2cMainServlet?pageid=PUBADV01&CACODE=CICA-2017-2509

A compliance report may please be forwarded to cgdanewdelhi@nic.in immediately.

Please accord "TOP PRIORITY"

Jt CGDA(IT) has approved.

(Vinay Khanna)
Sr. ACGDA(IT)