Kerala State Information Technology Mission
Department of Electronics & Information Technology
Government of Kerala

ICT Campus, Vellayambalam Jn.,
Thiruvananthapuram 695 033, Kerala, India
Tel: +91 -471-2726881, 2314307, Telefax: +91-471-2314284
Email: admin.ksitm@kerala.gov.in

KSITM/CERT-K/2017
13th May 2017

Sir/Madam,

Sub : Threat of a possible Cyber Attack

This is to bring to your attention certain proactive measures to be taken to improve the security posture of the department/institution against the threat of possible "ransomware" cyber attacks happening in many places across the world. A massive ransomware attack shut down computer systems across several countries including some systems in India, last night. System Administrators have to be instructed to follow the steps mentioned in this letter and in the advisory enclosed to improve the cyber hygiene in the systems of the department.

The security researchers identified the ransomware as a new variant of "WannaCry" (also known as WanaCrypt0r and WCry) that has the ability to automatically spread across large networks by exploiting a known bug in Microsoft's Windows operating system (as per Microsoft bulletin MS17-010).

A ransomware attack infects individual computers (Windows OS) with a malware that blocks access to all data on the system. The malware encrypts all the data on a computer system and decrypts it only after the computer user/owner agrees to pay a ransom.

You are advised to kindly take the following preventive measures to protect your computer networks from ransomware infection/ attacks:

All system administrators have to ensure the following are done in the organization to improve endpoint security ASAP. They can brief staff on these measures to improve awareness on cyber security :-

1. Ensure that ports TCP/UDP 445 are blocked on all perimeter devices and internal access control devices.
2. Ensure that ports TCP/UDP 445 are blocked on all clients & servers using host firewalls through host antiviruses and HIPS (Host based Intrusion Prevention System).
3. Apply all patches of Microsoft Windows (client and server) for the vulnerability mentioned in the Microsoft Security Bulletin MS17-010.
4. Secure mail server with antivirus and anti spamware solution.
5. Maintain updated Antivirus software on all user client systems urgently ON PRIORITY.
6. Update operating system, third party applications (MS office, browsers, browser Plugins) and antivirus software with the latest patches ON PRIORITY.
7. Alert all users in the organization of the attack. Hence the above step of updating software on the computer needs to be ensured before the user accesses email or internet.

8. Users should be alerted not to open attachments in unsolicited e-mails, even if they come from people in their contact list; never click on a URL contained in an unsolicited e-mail unless you are sure it is genuine. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
9. 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.*
10. Check regularly for the integrity of the information stored in the databases.
11. Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
12. Ensure integrity of the codes/scripts being used in database, authentication and sensitive systems
13. 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.
14. Application white listing/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.
15. 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
16. Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
17. Disable remote Desktop Connections, employ least-privileged accounts. Limit users who can log in using Remote Desktop, set an account lockout policy. Ensure proper RDP logging and configuration.
18. Restrict access using firewalls and allow only to selected remote endpoints, VPN may also be used with dedicated pool for RDP access
19. Use strong authentication protocol, such as Network Level Authentication (NLA) in Windows.

For more information, Please refer the following links:

1. Official website of CERT-In:
   http://cert-in.org.in
   (refer CURRENT ACTIVITIES – Wannacry / WannaCrypt Ransomware – CRITICAL ALERT)

2. MS17 – 010 Security Bulletin:
   https://technet.microsoft.com/library/security/MS17-010

Thanking You,

Yours Sincerely,

Kerala State IT Mission ★ A Society under Govt. of Kerala ★

Director