Dear All,

This is to inform you about a new ransomware attack which is spreading across Europe (and expected to affect globally). Please find below the summary of the attack as well as preventive measures to be taken.

Summary of the new attack vector

A major cyber-attack has struck large multinational companies across Europe, with Ukraine's government, banks, state power utility and Kiev's airport and metro system. The virus is named "**Petya**" believed to be ransomware - a piece of malicious software that shuts down a computer system and then demands an extortionate sum of money to fix the problem.

Petya is a nasty piece of ransomware and works very differently from any other ransomware malware. Unlike other traditional ransomware, Petya does not encrypt files on a targeted system one by one. Instead, Petya reboots victim's computers and encrypts the hard drive's master file table (MFT) and rendering the master boot record (MBR) inoperable, restricting access to the full system by seizing information about file names, sizes, and location on the physical disk. Petya replaces the computer's MBR with its own malicious code that displays the ransom note and leaves computers unable to boot. So far, it is not yet confirmed that what's the reason behind the sudden rapid spreading of Petya, but security researchers on Twitter are arguing that like WannaCry, Petya is also exploiting SMBv1 EternalBlue exploit and taking advantage of unpatched Windows machines.

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, usually in bitcoin.

Source of information: Various websites from internet (E.g:https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe, http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/, http://www.wired.co.uk/article/petya-malware-ransomware-attack-outbreak-june-2017)

Preventive Measures to be taken

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

- Ensure that ports TCP/UDP 445 are blocked on all perimeter devices and internal access control devices.
- Ensure that ports TCP/UDP 445 are blocked on all clients & servers using host firewalls through host antiviruses and HIPS.
- Apply all patches of Microsoft Windows (client and server) for the vulnerability mentioned in the Microsoft Security Bulletin MS17-010.
- Secure mail server with antivirus and anti-spam ware solution.
- Maintain updated Antivirus software on all user client systems urgently ON PRIORITY.
- Update operating system, third party applications (MS office, browsers, browser Plugins) and antivirus software with the latest patches ON PRIORITY.

Action items for System Administrators

All system administrators to **ensure this is done in the organizations ASAP.**

- Alert all users in the organization of the attack. Hence the above step of updating software's on the computer needs to be ensured before the user accesses email or internet.
- Users should be alerted not to open attachments in unsolicited e-mails, even if they come from people in your 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.
- 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. *
- 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.
- 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.
- 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
- Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
- 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.
- Restrict access using firewalls and allow only to selected remote endpoints, VPN may also be used with dedicated pool for RDP access
- Use strong authentication protocol, such as Network Level Authentication (NLA) in Window

Warm Regards,

Computer Emergency Response Team-Kerala (CERT-K)
Kerala State IT Mission
ICT Campus, Vellayambalam,
Thiruvanathapuram, Kerala - 695033
Office : 0471-2726881, 0471-2318007
Fax : 0471-2314284