VAKRANGEE SECURITY ALERT!

Wannacry/ WannaCrypt Ransomware Malware

Issue Date: May 17, 2017

As you aware that a new malicious massive ransomware named as "Wannacry" has hit multiple countries, it has estimated more than 99 countries have been affected by it (locked up more than 100,000 computers) since last Friday 12th May 2017.

"WannaCry is a ransomware which infects systems when a user clicks on a link and downloads a malicious software."

One of the reason to spread this ransomware is through a malicious attachment to email; Opening emails and email attachments from people you don't know, or that you weren't expecting; visiting unsafe, suspicious, or fake websites; clicking on malicious or bad links in emails, Facebook, Twitter, and other social media posts, instant messenger chats, like Skype etc.

Warning - "Don't open attachment in unsolicited e-mail, 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."

If you're ever unsure – don't click it!

Wannacry encrypts the files on infected Windows systems. This ransomware **"WannaCrypt or WannaCry"** encrypts the computer's hard disk drive and then spreads laterally between computers on the same LAN.

Warning - "Do not open or 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"

This ransomware drops a file named **"!Please Read Me!.txt"** which contains the text explaining what has happened and how to pay the ransom. Ransomware is granting full access to all files.

Warning - "Do not pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to systems@vakrangee.in **or** ritut@varkrangee.in **we will work out with the help of CERT-In and Law Enforcement agencies."**

Ransomware is writing itself into a random character folder in the 'ProgramData folder with the file name of "tasksche.exe' or in C:\Windows\ folder with the file-name 'mssecsvc.exe' and 'tasksche.exe'.

Prevention

In order to prevent infection users are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010.
https://technet.microsoft.com/library/security/MS17-010

Best practices to prevent ransomware attacks:

1. Maintain updated Antivirus software on all systems
2. Check regularly for the integrity of the information stored as a data/information/Backup.
3. Regularly check the contents of backup files for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
4. Keep the operating system, third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
5. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process.
6. Keep your data on a separate device, and backups should be stored offline.
7. Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
8. Do not install and run unwanted software applications.
9. Enable personal firewalls on workstations.
10. Implement strict External Device (USB drive) usage policy.
11. Microsoft has already released a patch to protect against NSA exploit of windows system. Ensure that your systems are updated with this patch.
12. Microsoft has also released a patch for non-supporting older Windows operating system. If you have any such systems, immediately apply the patch on such systems.

Please Note: In case you have come in contact with any such instance please contact systems@vakrangee.in or ritut@vakrangee.in

Be Safe and Secure!!