VAKRANGEE CRITICAL ALERT
PETYA - Second World's Biggest Ransomware Attack
Issue Date: 30 June 2017

A massive cyberattack swept across systems worldwide this week on 27th Jun 2017 named as **"PETYA"**, speeding in Europe, Middle East, and United States and affecting a variety of companies, from banking institutions to airlines to hospitals. Petya has been designed for "speed", and is spreading around like crazy. Petya ransomware delivered via **phishing emails** pretending to provide a resume which is, in fact, a malicious dropper. After reaching to the system it locks the computer that are infected and encrypting files on them and ask for ransom.

This version of 'Petya' tries to **spread internally** within networks.

Warning 1- "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.

Warning 2 - "Do not open the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf"

Warning 3 - "Do not pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to systems@vakrangee.in or infosec@varkrangee.in

We will work out with the help of CERT-In and Law Enforcement agencies."

Best practices to prevent ransomware attacks:

1. **Do a complete back up.** Back up all of your machines immediately.
2. Keep your data on a separate device, and backups should be stored offline.
3. Always make sure your **anti-virus is up-to-date** to maximize the protection available to you.
4. **Don't click too quickly.** This attack may be spreading through phishing or spam emails.
5. **Apply system and application updates.** Make sure your operating system is up-to-date to help contain the spread of malware.
6. **Follow safe practices when browsing the web.** Ensure the web browsers are secured enough with appropriate content controls.
7. Do not install and run unwanted software applications.
8. Enable personal firewalls on workstations.
9. Implement strict External Device (USB drive) usage policy.

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

Be safe!!