NASSCOM®

**NASSCOM-DSCI has alerted members on cyber outbreak – WannaCry Ransomware**

**15 May, 2017, Delhi:** NASSCOM & DSCI, acknowledging the global outbreak on a new Ransomware named 'WannaCry', has alerted the industry and issued a compilation of best practices to counter this challenge. DSCI has worked with leaders (CISOs/ CIOs) across industry and CERT-In, and shared important information and advisory to the organizations.

R Chandrashekhar, President, NASSCOM said, "The world is witnessing a massive cyber outbreaks in recent times. Thousands of organizations and institutions have been subjected to a series of ransomware attacks over the past two days. DSCI is constantly working with CERT-In and industry experts to ensure both domestic industry and global clients remain protected from this complex threat. This warrants the need for global collaboration and collective response."

Rama Vedashree, CEO, Data Security Council of India (DSCI), said, "While there is no significant impact on vital installations and networks in the country, it is important to continue to track the impact. Interestingly, we are witnessing unprecedented exchange of Information amongst Security professionals and communities across verticals to develop Best practices and SOPs (Standard Operating Procedures). We would like to emphasize the need for Industry, Government and Law Enforcement Agencies to collaborate to address and mitigate risk."

WannaCrypt or WannaCry is a recent ransomware that is affecting Windows based systems worldwide. It spreads by using a vulnerability in implementations of Server Message Block (SMB) in Windows systems. This exploit is named as ETERNALBLUE. The ransomware encrypts the computer's hard disk drive and then spreads laterally between computers on the same LAN. It also spreads through malicious attachments to emails.

Globally, critical sectors like Healthcare, Transport and Banking have been impacted and our IT Industry has stepped up its efforts to support their customers in India and across the globe.

Snapshot of NASSCOM-DSCI Best practices compilation on Wannacry/ WannaCrypt Ransomware is given below:

- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Any type of suspected behavior should be analysed and reported such instances of fraud to CERT-In and Law Enforcement agencies immediately:

  CERT-In is constantly updating its webpage, please refer for the latest update: http://www.cyberswachhtakendra.gov.in/alerts/wannacry_ransomware.html

· Windows OS Update: 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/

Given the impact of WannaCry, Microsoft has released SMB patch update for unsupported Windows Versions - XP, Vista, 8, Server 2003, 2008 etc. Patch has been released

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

· Endpoints: Switch off SMB traffic port (445) for the time being in the internal network, unless required by any particular application; enable personal firewalls on workstations; maintain updated Antivirus software on all systems; implement strict External Device (USB drive) usage policy;

· Server/ Network/ Gateway: Ensure IPS signatures are updated; ensure EMail Gateway solutions have all relevant updates for detecting possible mails that may bring the Trojan in the environment; ensure Proxy solution has updated database; block the known malware perpetrator IP addresses on Firewall; check regularly for the integrity of the information stored in databases among others.

(Detailed compilation can be found on DSCI website: https://www.dsci.in/taxonomypage/1466 )