1. Perform regular backup of workstations in order to limit the impact of loss of the critical data.

2. Do not open attachment in unsolicited emails, even if they come from people in your contact list because they may contain malware embedded in the attachment. In case of genuine URL please visit the organization's website directly from web browsers.

3. Disable remote Desktop connection, employ least-privileged accounts.

4. Use of personal system firewall on workstations.

5. Maintain updated Antivirus on workstations.

6. Install the latest version of the windows which are currently supported by Microsoft. Microsoft has issued patches for unsupported versions such Windows XP, Vista, Server 2003, server 2008 etc. you can visit below URL for downloading the patches.

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

7. Disable SMBv1 service on your system by following steps

For Windows 8.1 or Windows Server 2012 R2 and later users

(a) Open Control Panel, click Programs and then click Turn Windows feature on or off.

(b) In the windows Feature window, clear the SMB1.0/CIFS File Sharing Support checkbox, and then click OK to close the window.

(c) Restart the system.

for server operating systems:

(a) Open Server Manager and then click the Manage menu and select Remove Roles and Features.

(b) In the Features window, clear the SMB1.0/CIFS File Sharing Support check box, and then click OK to close the window.

(c) Restart the system.

8. Disable macros on Microsoft office product (Access, PowerPoint, Word, Excel, Outlook etc)

Administrators are requested to take following best practices need to be implemented for fighting with Wannacry/WannaCrypt ransomeware

1. Network security administrator

(a) kindly apply following three snort signature/rules at IPS and IDS level immediately.

alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response"; flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:1;)

alert smb $HOME_NET any -> any any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response";

flow:from_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; metadata: former_category EXPLOIT; classtype:trojan-activity; sid:2024218; rev:1;)

alert tcp $HOME_NET 445 -> any any (msg:”ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response”; flow:from_server,established; content:”|00 00 00 31 ff|SMB|2b 00 00 00 00 98 07 c0|”; depth:16; fast_pattern; content:”|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|”; distance:0; flowbits:isset,ETPRO.ETERNALBLUE; classtype:trojan-activity; sid:2024218; rev:2;)

(b) Block UDP port 137, 138 and TCP 139 and 445 on edge perimeter devices (IDS, IPS and Firewall).

2. Application administrator should implement Software Restriction Policies (SRP) to block the binaries running from

%APPDATA% , %PROGRAMDATA% and %TEMP% paths as ransomware sample drops and execute generally from these locations.

Wannacry/WannaCrypt Ransomware is writing itself into a random character folder in the ProgramData folder with the filename tasksche.exe

or in the C:\Windows\ folder with the filename mssecsvc.exe and tasksche.exe. Few examples are listed below for your reference

C:\ProgramData\lygekvkj256\tasksche.exe

C:\ProgramData\pepauehfflzjjtl340\tasksche.exe

C:\ProgramData\utehtftufqpkr106\tasksche.exe

3. Block the attachment of file types, exe|pif|tmp|url|vb|vbe|scr|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf.