Annexure-'B'

CRITICAL ALERT – Wannacry/ WannaCrypt Ransomware

About "Wannacry" Ransomware:

A new ransomware named as "Wannacry" is spreading widely.Wannacry encrypts the files on infected Windows systems. This ransomware spreads by using a vulnerability in implementations of Server Message Block (SMB) in Windows systems. This exploit is named as ETERNALBLUE.

The ransomware called WannaCrypt or WannaCry encrypts the computer's hard disk drive and then spreads laterally between computers on the same LAN. The ransomware also spreads through malicious attachments to emails. In order to prevent infection, users and organisations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010. https://technet.microsoft.com/library/security/MS17-010

It also drops a file named "!Please Read Me!.txt" which contains the text explaining what has happened and how to pay the ransom.

Indicators of compromise (IOC):

WannaCry encrypts files with the following extensions, appending .WCRY to the end of the file name:

- .lay6
- .sqlite3
- .sqlitedb
- .accdb
- .java
- .class
- .mpeg
- .djvu
- .tiff
- .backup
- .vmdk
- .sldm
- .sldx
- .potm
- .potx
- .ppam
- .ppsx
- .ppsm
- .pptm

- .xltm
- .xltx
- .xlsb
- .xlsm
- .dotx
- .dotm
- .docm
- .docb
- .jpeg
- .onetoc2
- .vsdx
- .pptx
- .xlsx
- .docx

The file extensions that the malware is targeting contain certain clusters of formats including:

- Commonly used office file extensions (.ppt, .doc, .docx, .xlsx, .sxi).
- Less common and nation-specific office formats (.sxw, .odt, .hwp).
- Archives, media files (.zip, .rar, .tar, .bz2, .mp4, .mkv)
- Emails and email databases (.eml, .msg, .ost, .pst, .edb).
- Database files (.sql, .accdb, .mdb, .dbf, .odb, .myd).
- Developers' sourcecode and project files (.php, .java, .cpp, .pas, .asm).
- Encryption keys and certificates (.key, .pfx, .pem, .p12, .csr, .gpg, .aes).
- Graphic designers, artists and photographers files (.vsd, .odg, .raw, .nef, .svg, .psd).
- Virtual machine files (.vmx, .vmdk, .vdi).

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

Ransomware is granting full access to all files by using the command:
Icacls . /grant Everyone:F /T /C /Q
Using a batch script for operations:
176641494574290.bat

Content of Batch-file (fefe6b30d0819f1a1775e14730a10e0e)

```
echo off
echo SET ow = WScript.CreateObject("WScript.Shell")> m.vbs
echo SET om = ow.CreateShortcut("C:\
WanaDecryptor
.exe.lnk")>> m.vbs
echoom.TargetPath = "C:\
WanaDecryptor
```

.exe”>> m.vbs
echoom.Save>> m.vbs
cscript.exe //nologo m.vbs
del m.vbs
del /a %0
Content of ‘M.vbs’
SET ow = WScript.CreateObject(“WScript.Shell”)
SET om = ow.CreateShortcut(“C:\
WanaDecryptor
.exe.lnk”)
om.TargetPath = “C:\
WanaDecryptor
om.Save

hashes for WANNACRY ransomware:

4fef5e34143e646dbf9907c4374276f5
5bef35496fcbdbe841c82f4d1ab8b7c2
775a0631fb8229b2aa3d7621427085ad
7bf2b57f2a205768755c07f238fb32cc
7f7ccaa16fb15eb1c7399d422f8363e8
8495400f199ac77853c53b5a3f278f3e
84c82835a5d21bbcf75a61706d8ab549
86721e64ffbd69aa6944b9672bcabb6d
8dd63adb68ef053e044a5a2f46e0d2cd
b0ad5902366f860f85b892867e5b1e87
d6114ba5f10ad67a4131ab72531f02da
db349b97c37d22f5ea1d1841e3c89eb4
e372d07207b4da75b3434584cd9f3450
f529f4556a5126bba499c26d67892240

- *Use endpoint protection/antivirus solutions to detect these files and remove the same*

The malware use TOR hidden services for command and control. The list of .onion domains inside is as following:

- gx7ekbenv2riucmf.onion
- 57g7spgrzlojinas.onion
- Xxlvbrloxvriy2c5.onion
- 76jdd2ir2embyv47.onion
- cwwnhwhlz52maqm7.onion
- sqjolphimrr7jqw6.onion

Specific Countermeasures to prevent Wannacry/WannaCrypt Ransomware:

Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection/ attacks:

- 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.

- **Apply following signatures/rules at IDS/IPS**

  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

(http://docs.emergingthreats.net/bin/view/Main/2024218)

alert smb any any -> $HOME_NET any (msg:"ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Request (set)"; flow:to_server,established; content:"|00 00 00 31 ff|SMB|2b 00 00 00 00 18 07 c0|"; depth:16; fast_pattern; content:"|4a 6c 4a 6d 49 68 43 6c 42 73 72 00|"; distance:0; flowbits:set,ETPRO.ETERNALBLUE; flowbits:noalert; classtype:trojan-activity; sid:2024220; 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; classtype:trojan-activity; sid:2024218; rev:1

- **Yara:**

```
rule wannacry_1 : ransom
{
meta:
author = "Joshua Cannell"
description = "WannaCry Ransomware strings"
weight = 100
date = "2017-05-12"
 Strings:
$s1 = "Ooops, your files have been encrypted!" wide asciinocase
```

$s2 = “WannaDecryptor” wide asciinocase
$s3 = “.wcry” wide asciinocase
$s4 = “WANNACRY” wide asciinocase
$s5 = “WANACRY!” wide asciinocase
$s7 = “icacls . /grant Everyone:F /T /C /Q” wide asciinocase

Condition:
any of them
}
rule wannacry_2{
meta:
author = “Harold Ogden”
description = “WannaCry Ransomware Strings”
date = “2017-05-12”
weight = 100
strings:
$string1 = “msg/m_bulgarian.wnry”
$string2 = “msg/m_chinese (simplified).wnry”
$string3 = “msg/m_chinese (traditional).wnry”
$string4 = “msg/m_croatian.wnry”
$string5 = “msg/m_czech.wnry”
$string6 = “msg/m_danish.wnry”
$string7 = “msg/m_dutch.wnry”
$string8 = “msg/m_english.wnry”
$string9 = “msg/m_filipino.wnry”
$string10 = “msg/m_finnish.wnry”
$string11 = “msg/m_french.wnry”
$string12 = “msg/m_german.wnry”
$string13 = “msg/m_greek.wnry”
$string14 = “msg/m_indonesian.wnry”
$string15 = “msg/m_italian.wnry”
$string16 = “msg/m_japanese.wnry”
$string17 = “msg/m_korean.wnry”
$string18 = “msg/m_latvian.wnry”

$string19 = “msg/m_norwegian.wnry”
$string20 = “msg/m_polish.wnry”
$string21 = “msg/m_portuguese.wnry”
$string22 = “msg/m_romanian.wnry”
$string23 = “msg/m_russian.wnry”
$string24 = “msg/m_slovak.wnry”
$string25 = “msg/m_spanish.wnry”
$string26 = “msg/m_swedish.wnry”
$string27 = “msg/m_turkish.wnry”
$string28 = “msg/m_vietnamese.wnry”
condition:
any of ($string*)
}

ISMO Contact Details:-

Information Security Management Office (ISMO),
Secretariat for Information Technology, Government of Haryana
HARTRON Bhawan, Bays No. 73-76, Sector-2, Panchkula – 134109
e-Mail address:-

a) CISO: munish.chandan@semt.gov.in
b) AM-IT: amitbeniwal@haryanaismo.gov.in
c) SA: pardeep@haryanaismo.gov.in