No. DIT-F(10)4/2015(SDC) -108
Government of Himachal Pradesh
Department of Information Technology
*****

From

Director,
Department of Information Technology,
Government of Himachal Pradesh

To

1. **All the Administrative Secretaries to the Government of Himachal Pradesh**
2. **All the Heads of the Departments in Himachal Pradesh**
3. **All the Managing Directors/ CEOs of Corporations/ Boards in Himachal Pradesh**
4. **All the Divisional Commissioners in Himachal Pradesh**
5. **All the Deputy Commissioners in Himachal Pradesh**

Dated: Shimla-171013, the 22nd May, 2017

Subject: Advisory regarding "Wannacry" Ransomware – Cyber Attack

Sir/ Madam,

As we all have heard of the global ransomware cyber-attacknamed as "Wannacry" which is spreading like wild fire infecting critical IT installations globally. This ransomware spreads by using vulnerability in implementations of Server Message Block (SMB) in Windows systems. Wannacry encrypts the files on infected Windows systems.It just not only locks down the files rather it encrypts the files which makes it really impossible to crack open the locked files. As a result the users do not have any other way to regain access to their locked files but to pay the money and get the decryption code.

The WannaCryransomware 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.The easiest way to get into someone's computer is through attachments of spam emails or by clicking the unknown link. Usually users turn off the file extensions, so they cannot know what kind of file they are clicking on. The virus file pretends like a "doc" file or any other text file. But if you turn on the file extension of your computer, you will see that the file extensions are different. As you click on the infected file, all your data start encrypting and eventually asking you for ransom.

The Department of Information Technology, HP has taken precautionary steps at HPSDC and HIMSWAN datacenter to secure from ransomware.However, some of the Servers likeHimBhoomi, Himris, Excise & Taxation, Electricity department etcare installed outside HPSDC domain and hence cannot be taken care of centrally by IT Department/ NIC. Also, PCs installed in field officesacross the State, especially those who are not accessing internet through HIMSWAN/ NICNET, are most vulnerable because of using unsecured internet connections.

It is, therefore, advised to use HIMSWAN/ NICNET connectivity to access internet and also remove such machines from the LAN on immediate basis where Windows Operating System is not updated/ upgraded recently and/ or Antivirus is not installed/ updated. An Advisory from IT Department to all Departments is also enclosed herewith at Annexure-I for reference with a request to kindly go through the same and take precautionary measures to protect IT Systems from cyber-attacks.

Yours faithfully,

(Manasi Sahay Thakur)
Director,
Department of Information Technology,
Shimla-13, Himachal Pradesh

Annexure-I

Advisory

What is Ransomware?

Ransomware is a malicious software that encrypts the files and locks device, such as a computer, tablet or smartphone and then demands a ransom to unlock it. Recently, a dangerous ransomware named 'Wannacry' has been affecting the computers worldwide creating the biggest ransomware attack the world has ever seen. This has affected computers in India also.

What is WannaCry Ransomware?

WannaCry ransomware attacks windows based machines. It also goes by the name WannaCrypt, WannaCry, WanaCrypt0r, WCrypt, WCRY.It leverages SMB exploit in Windows machines called EternalBlue to attack and inject the malware. All versions of windows before Windows 10 are vulnerable to this attack if not patched for MS-17-010. After a system is affected, it encrypts the files and shows a pop up with a countdown and instructions on how to pay the 300$ in bitcoins to decrypt and get back the original files. If the ransom is not paid in 3 days, the ransom amount increases to 600$ and threatens the user to wipe off all the data. It also installs DOUBLEPULSAR backdoor in the machine.

How it spreads?

It uses EternalBlue MS17-010 to propagate. The ransomware spreads by clicking on links and downloading malicious files over internet and email. It is also capable of automatically spreading itself in a network by means of a vulnerability in Windows SMB. It scans the network for specific ports, searches for the vulnerability and then exploits it to inject the malware in the new machine and thus it spreads widely across the network.

What can you do to prevent infection?

- There is a critical vulnerability in various versions of Microsoft Windows (client as well as server) which is being used to spread ransomware across the globe. Microsoft has released a Windows security patch MS17-010 for Windows machines. This needs to be applied immediately and urgently.
- Remove Windows NT4, Windows 2000 and Windows XP-2003 from production environments and upgrade the same with latest versions

- Block ports 139, 445 and 3389 in firewall, PCs and Servers. Ensure that ports TCP/UDP 445 are blocked on all perimeter devices and internal access control devices.
- Avoid clicking on links or opening attachments or emails from people you don't know or companies you don't do business with.
- Make sure your Operating System is up-to-date
- Install antivirus being provided by HIMSWAN/ NICNET and a good anti-ransomware product for better security
- SMB is enabled by default on Windows. Disable SMB service on the machine by going to Settings > uncheck the settings > OK
- Make sure your software is up-to-date.
- Have a pop-up blocker running on your web browser.
- Perform regular backups of critical information to limit the impact of data or systems loss;
- Check content of backup files of databases for any unauthorized encrypted contents of data records or external elements, such as backdoors/malicious scripts is critical;
- Ensure integrity of codes/scripts used in database, authentication and sensitive systems;
- Below is a consolidated list that we need to block on you firewall/antivirus

  IPs

  - 16.0.5.10:135
  - 16.0.5.10:49
  - 10.132.0.38:80
  - 1.127.169.36:445
  - 1.34.170.174:445
  - 74.192.131.209:445
  - 72.251.38.86:445
  - 154.52.114.185:445
  - 52.119.18.119:445
  - 203.232.172.210:445
  - 95.133.114.179:445
  - 111.21.235.164:445
  - 199.168.188.178:445
  - 102.51.52.149:445
  - 183.221.171.193:445

- 92.131.160.60:445
- 139.200.111.109:445
- 158.7.250.29:445
- 81.189.128.43:445
- 143.71.213.16:445
- 71.191.195.91:445
- 34.132.112.54:445
- 189.191.100.197:445
- 117.85.163.204:445
- 165.137.211.151:445
- 3.193.1.89:445
- 173.41.236.121:445
- 217.62.147.116:445
- 16.124.247.16:445
- 187.248.193.14:445
- 42.51.104.34:445
- 76.222.191.53:445
- 197.231.221.221:9001
- 128.31.0.39:9191
- 149.202.160.69:9001
- 46.101.166.19:9090
- 91.121.65.179:9001
- 2.3.69.209:9001
- 146.0.32.144:9001
- 50.7.161.218:9001
- 217.79.179.177:9001
- 213.61.66.116:9003
- 212.47.232.237:9001
- 81.30.158.223:9001
- 79.172.193.32:443
- 38.229.72.16:443

Domains

- iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com
- Rphjmrpwmfv6v2e[dot]onion
- Gx7ekbenv2riucmf[dot]onion
- 57g7spgrzlojinas[dot]onion

- xxlvbrloxvriy2c5[dot]onion
- 76jdd2ir2embyv47[dot]onion
- cwwnhwhlz52maqm7[dot]onion

File Names:

- @Please_Read_Me@.txt
- @WanaDecryptor@.exe
- @WanaDecryptor@.exe.lnk
- Please Read Me!.txt (Older variant)
- C:\WINDOWS\tasksche.exe
- C:\WINDOWS\qeriuwjhrf
- 131181494299235.bat
- 176641494574290.bat
- 217201494590800.bat
- [0-9]{15}.bat #regex
- !WannaDecryptor!.exe.lnk
- 00000000.pky
- 00000000.eky
- 00000000.res
- C:\WINDOWS\system32\taskdl.exe

- 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).
    - **Indicators of compromise:**

      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".

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

- **hashes for WANNACRY ransomware:**

  5bef35496fcbdbe841c82f4d1ab8b7c2

  775a0631fb8229b2aa3d7621427085ad

  7bf2b57f2a205768755c07f238fb32cc

  7f7ccaa16fb15eb1c7399d422f8363e8

  8495400f199ac77853c53b5a3f278f3e

  84c82835a5d21bbcf75a61706d8ab549

  86721e64ffbd69aa6944b9672bcabb6d

  8dd63adb68ef053e044a5a2f46e0d2cd

  b0ad5902366f860f85b892867e5b1e87

  d6114ba5f10ad67a4131ab72531f02da

  db349b97c37d22f5ea1d1841e3c89eb4

  e372d07207b4da75b3434584cd9f3450

  f529f4556a5126bba499c26d67892240