7220604/5744
29/05/2017

HARYANA GOVERNMENT / हरियाणा सरकार

Haryana State

Information Security Management Office

Society for IT Initiative Fund for e-Governance,
Department of Electronics & Information Technology, Haryana

हरियाणा

INFORMATION SECURITY

From: Addl. Dir. 26.5.17

Chief Information Security Officer (CISO),
Electronics & Information Technology Department, Haryana

To: DIR, Secondary Edn

1. All Administrative Secretaries
2. All Head of Departments
3. All Boards, Corporations and Institutions,
4. Registrar, Punjab & Haryana High Court, Chandigarh
5. State Information Office, NIC
6. Head - SeMT
7. PM- CT
8. AGM (C&C), Hartron

Commissioner & Director General Secondary Education Haryana
Diary No PA/DSE 17390
PANCHKULA

HRY-ISMO/2017/CISO/: 4768 All programmers 26/5

Dated: 15th May 2017

Dear Sir/Madam,

Subject:- Information Security Advisory on "Wannacry" ransomware - Rated CRITICAL.

Your attention in sought to the attached InfoSec Advisory, rated CRITICAL.

The advisory pertains to the latest ransomware named "Wannacry" which spreads infections in several countries around the world. Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it.

How it spreads:

1. Ransomware spreads by clicking on links over internet & email and downloading malicious files; it is also capable of spreading itself automatically in a network by means of a vulnerability in Windows based Operating Systems (OS).
2. Ransomware spreads easily when it encounters unpatched or outdated software.

What "Wannacry" can do ?

The Wannacry ransomware attacks on windows based machines and start encrypting the files on the system and shows a popup with a countdown and instructions on how to pay the ransom amount. Say: 300$ in bitcoins to decrypt and get back the original files. If ransom is not paid in 3 days, the ransom amount increases to 600$ and threatens the user to wipe off/ erase all the data in the windows based computer/ tab/ mobile, etc.

Countermeasures to prevent:

In order to prevent this infection, the users and organisations are advised to apply

Bays 73-76, Hartron Bhawan, Sector 2, Panchkula - 134151
Chairman, E.C.: 2740009, MSEC.: 2741547, Sr. Ad.O: 2748142, Fax:0172-2749985
CISO: 0172-2703479 www.haryanait.gov.in

patches to Windows systems as mentioned in Microsoft Security Bulletin MS17-010. (Link: https://technet.microsoft.com/library/security/MS17-010). The generic Do's and Don'ts are enclosed in **Annexure-'A'**.

Advisory to prevent ransomware attacks:

1. Maintain updated Antivirus software.
2. Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
3. Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
4. Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail.
5. Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
6. Enable personal firewalls on computers/ workstations, etc.
7. Prevent using unknown external devices (USB drive/ CDs etc).

Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee release/ decrypting of files. Report such instances immediately to CERT-In/ Haryana ISMO. The detailed Technical Advisory which may be followed is enclosed in Annexure-'B'.

You are requested to review your department/organization(s) IT/Computer Infrastructure for the critical threat of the ransomware and take necessary/corrective actions to prevent the same. An advisory issued by NIC is also enclosed for reference at **Annexure-'C'**

This may please be circulated within your organizations for prompt action by all the concerned. For more Information and any further assistance, the Haryana State Information Security Management Office (ISMO) may be contacted.

Yours truly,

15/5/2017

Chief Information Security Officer (CISO)/PH ISMO

A copy is forwarded to the following:
1. PS to Principal Secretary E&IT for kind information of Principal Secretary E&IT.
2. PA to Secretary E&IT for kind information of Secretary E&IT.

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) munish.chandan@semt.gov.in
b) pardeep@haryanaismo.gov.in
c) amitbeniwal@haryanaismo.gov.in

NIC Advisory on Ransomware Attacks.

A. What is a ransomware attack?

Attacks involve malware delivered through spear phishing emails that lock up valuable data assets and demand a ransom to release them.

Hackers now check a victim's social media accounts, and create a fake email address pretending to be a friend or contact in order to get them to click on an infected link or attachment.

"It's much more targeted, and will exploit a particular vulnerability in a device, application, server or software,

The Health / Education / social sector is highly targeted by hacker attacks, due to antiquated or misconfigured computer security systems and the amount of sensitive data they hold.

B. How to Prevent Ransomware Attacks ?

1. Do not click hyper links from un-known sources, and without establishing authenticity of link even from known sources.
2. Prepare a up-to-date inventory of all the "Digital Assets" at various locations/facilities being used by the various functionaries of the organization.
3. Make a trustworthy knowledgeable functionary (permanent Government employee) Administrator of the Digital Assets (ADA) of the organization at each location.
4. Let ADA keep all software (especially the system software) up to date, including operating systems and applications.
5. ADA has to ensure back-up of all digital content located in the digital assets under ADA jurisdiction every day, including information on employee devices, so ADA can restore encrypted data if attacked by ransomware.
6. Back up all digital content to a secure, offsite secret location(s) within organization.
7. Distribute Back-up : Divide the digital assets and distribute the back-up locations. Don't place all data on one back-up file and share it.
8. ADA in collaboration with NIC officials, to train all the staff using the digital assets including mobile devices connected to network, on cyber security practices, emphasizing not opening attachments or links from unknown sources.
9. Develop a communication channel and strategy to quickly inform all employees if a virus reaches the company network.
10. If every bit of data of the organization is safeguarded and back-up is kept secretly, even if hackers attack and demand ransom, Govt can launch an investigation rather than making payment.
11. Mandate security auditing by ICERT empanelled auditors for all the digital assets as per GoI policy.

12. ADAs in collaboration with information security teams of ITE&C Dept and NIC to perform penetration testing to detect the vulnerabilities.
13. Register all the devices and digital assets. Strictly avoid usage of un-registered and un-monitored devices.
14. Adopt and use standard security and data privacy policies as per advisories from ITE&C Dept, NIC/ Govt of India.
15. Ensure all devices and systems are protected well with latest firewalls and anti-virus systems.

C. Mitigating an attack

1. Remove the infected machines from the network, so the ransomware does not use the machine to spread throughout your network.
2. Report the attack and register all information related to attack.
3. Facilitate investigation of the attack.
4. Let one authorized spokesperson of the entire department only communicate with media the information related to attack.
5. A inventory of attacks and decryption kits / mitigation kits to be maintained.

Annexure-'A'

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):

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'.

Do's to prevent ransomware attacks

- Maintain updated Antivirus software on all systems
- Check regularly for the integrity of the information stored in the databases.

- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems
- Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.
- Enable personal firewalls on workstations.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empaneled auditors. Repeat audits at regular intervals.
- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies

Don'ts to prevent ransomware attacks:

- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser
- Don't allow ActiveX content in Microsoft Office applications such as Word, Excel, etc.
- Don't allow remote Desktop Connections, employ least-privileged accounts.

- Don't enable PowerShell /windows script hosting, until required genuinely.
- Don't permit users' to install and run unwanted software applications.

Generic Prevention Tools:

- Sophos: Hitman.Pro: https://www.hitmanpro.com/en-us/surfright/alert.aspx
- Bitdefender Anti-Crypto Vaccine and Anti-Ransomware (discontinued): https://labs.bitdefender.com/2016/03/combination-crypto-ransomware-vaccine-released/
- Malwarebytes Anti-Ransomware(formelyCryptoMonitor): https://blog.malwarebytes.com/malwarebytes-news/2016/01/introducing-the-malwarebytes-anti-ransomware-beta/
- Trendmicro Ransomware Screen Unlocker tool: https://esupport.trendmicro.com/en-us/home/pages/technical-support/1105975.aspx
- Microsoft Enhanced mitigation and experience toolkit(EMET): https://www.microsoft.com/en-us/download/details.aspx?id=50766

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