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