

Wannacry/ WannaCrypt Ransomware

It has been reported that 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.

Indicators of compromise:

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 etc.

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

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

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 filename '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 Batchfile (fefe6b30d0819f1a1775e14730a10e0e) `echo off echo SET ow =`

`WScript.CreateObject("WScript.Shell")> m.vbs`

`echo SET om = ow.CreateShortcut("C:\`

`WanaDecryptor`

`.exe.lnk")>> m.vbs .echo om.TargetPath = "C:\`

`WanaDecryptor`

`.exe">> m.vbs`

`echo om.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`

Prevention

In order to prevent infection, users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin MS17010.

Best practices 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) uptodate 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.
- Don't open attachments in unsolicited emails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited email, even if the link seems benign. In cases of genuine URLs close out the email and go to the organization's website directly through browser.
- 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.
- Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc. Disable remote Desktop Connections, employ leastprivileged accounts. If not required consider disabling, PowerShell /windows script hosting.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- Implement strict External Device (USB drive) usage policy.
- Employ dataatrest and dataintransit encryption. Consider installing Enhanced Mitigation Experience Toolkit, or similar hostlevel antiexploitation tools.
- Block the attachments of file types,
exelpifltmplurlvlvblvbelrcrlreglcr|pstlcmdlcomlbatldllldat|hlplhtaljs|wsf .
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERTIN 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.