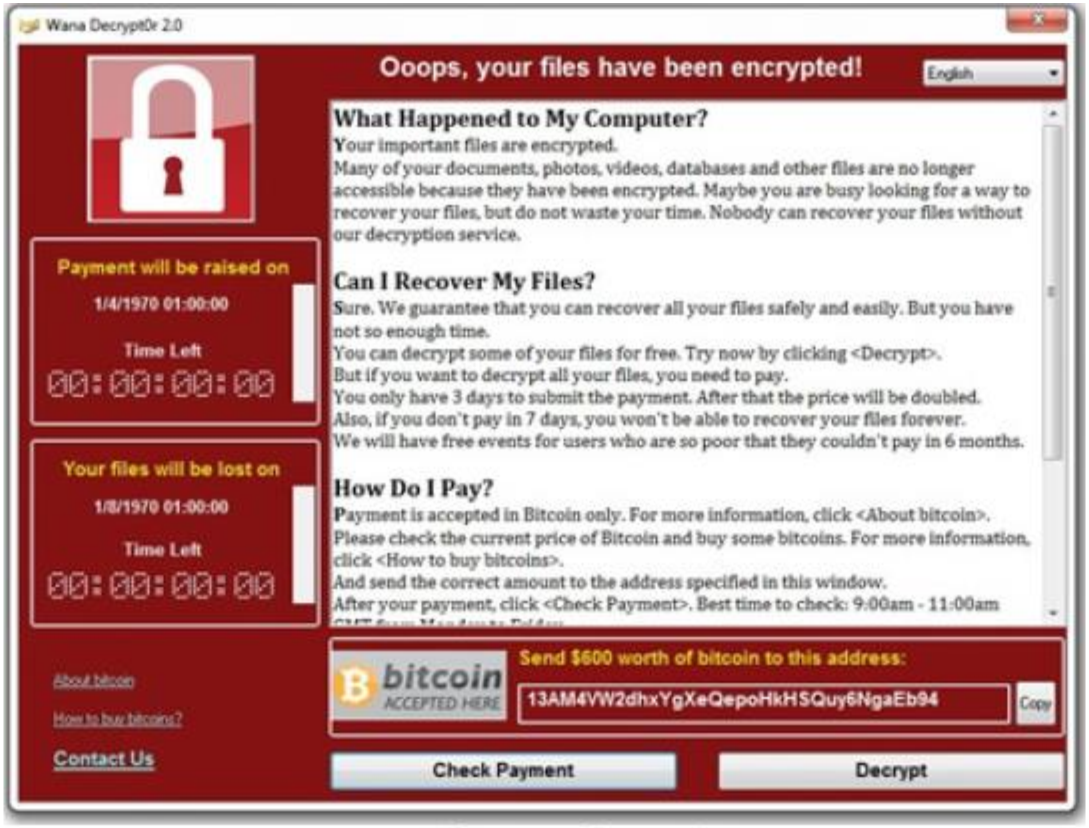
Advisory Note WannaCry Ransomware

Dear Customer,

A Major Cyber security attack throughout the world!

An exploit of Microsoft Windows called EternalBlue, is being used as one method for rapidly spreading a ransomware variant called "WannaCry" across the world which is caused by Microsoft vulnerability on Windows machines. The ransomware also spreads through malicious links or attachments to emails.
WannaCry Ransomware is a debilitating from the malware that breaks into a system and locks users by encrypting all their data and files.

The access to the data is withheld till the hacker's demands are met. WannaCry encrypts the computer's hard disk drive and then spreads laterally between computers on the same LAN.
This is believed to be by far the largest such ransomware attack in history. India was said to be among the countries worst affected in the attack.
After infecting, this Wannacry ransomware displays following screen on infected system:



Ooops, your files have been encrypted!

Payment will be raised on
1/4/1970 01:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 01:00:00
Time Left
00:00:00:00

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

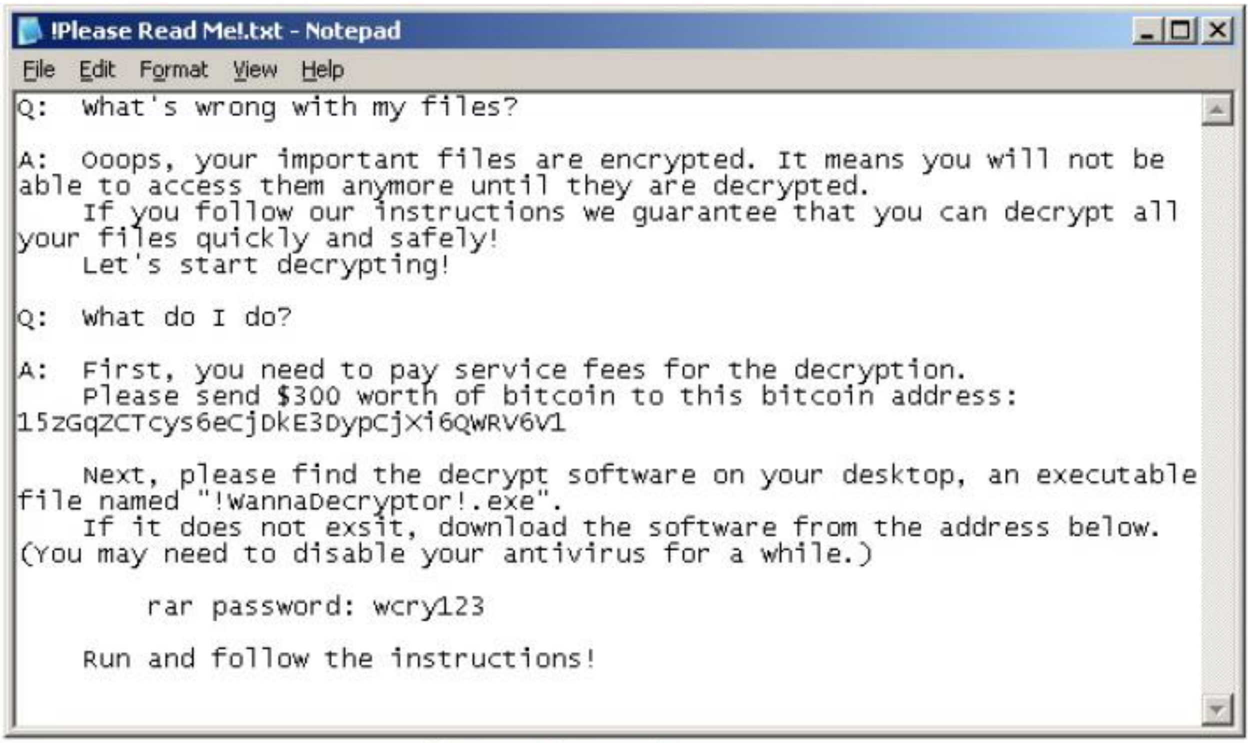
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday

Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Source: Symantec

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



```
Q:  What's wrong with my files?

A:  Ooops, your important files are encrypted. It means you will not be
able to access them anymore until they are decrypted.
    If you follow our instructions we guarantee that you can decrypt all
your files quickly and safely!
    Let's start decrypting!

Q:  What do I do?

A:  First, you need to pay service fees for the decryption.
    Please send $300 worth of bitcoin to this bitcoin address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

    Next, please find the decrypt software on your desktop, an executable
file named "!WannaDecryptor!.exe".
    If it does not exsit, download the software from the address below.
(You may need to disable your antivirus for a while.)

        rar password: wcry123

    Run and follow the instructions!
```

Source: Symantec

Software Affected:

Windows Vista Service Pack 2 and Windows Vista x64 Edition Service Pack 2
Windows 7 for 32bit
Service Pack 1 and Windows 7 for x64based
Systems Service Pack 1
Windows 8.1 for 32bit and 64bit systems
Windows RT 8.1
Windows 10 for 32 bit and 64bit systems
Windows Server 2012
Windows Server 2012 R2
Windows Server 2008 R2 for x64based

Systems Service Pack 1
Windows Server 2008 SP2 for 32bit and 64bit
systems (Server Core Installation)
Windows Server 2008 SP1 R2 for64bit Systems(Server Core Installation)
Windows Server 2008 R2 for Itaniumbased Systems Service Pack 1
Windows Server 2008 for Itaniumbased Systems Service Pack 2
Windows Server 2012 (Server Core Installation)
Windows Server 2012 R2(Server Core Installation)
Windows Server 2016 for 64bit
Systems(Server Core Installation)
Windows Server 2016 for 64bit Systems

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
.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:
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).

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) upto 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.

- 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 least privileged 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, 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 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. Report such instances of fraud to CERTIn and Law Enforcement agencies

References

https://securelist.com/blog/incidents/78351/wannacryransomwareusedinwidespreadattacksallovertheworld/
https://securingtomorrow.mcafee.com/executiveperspectives/analysiswannacryransomwareoutbreak/
https://www.symantec.com/connect/blogs/whatyouneedknowaboutwannacryransomware
https://www.uscert.gov/ncas/currentactivity/2017/05/12/MultipleRansomwareInfectionsReported
https://technet.microsoft.com/library/security/MS17010
CERT-In advisory - CERT-In Vulnerabilty Note CIVN-2017-0032_15March 2017 and CERT-IN Advisory_wannacrypt_ransomeware

Disclaimer: *The information provided herein is on "as is" basis, without warranty of any kind.*