*cert*Tonga

Tonga National Computer
Emergency Response
Team

*Cert*Tonga Advisory: Wanna Cry Ransomeware

Dear Constituents,

A massive global ransomware attack dubbed as **WannaCrypt** or "**WannaCry**" (Ransom:Win32/WannaCrypt) exploiting a vulnerability in Microsoft's Windows operating system is currently in progress. The ransomware is a new variant of the **Ransom.CryptXXX** family and spreads aggressively across networks and holds files to ransom. The attack is spreading widely and impacting a large number of organisations across the world.

Affected Systems:

Windows Systems which do not have the latest security updates are at risk of infection.

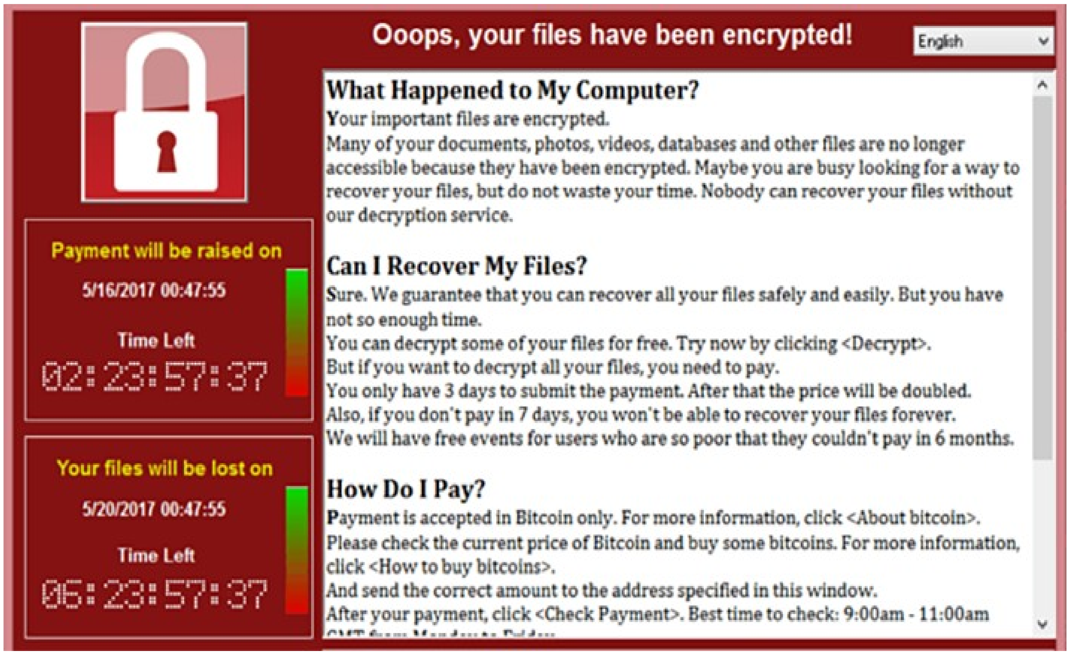
Methodology of Attack:

1. WannaCry propagates to other computers by exploiting a known SMB remote code execution vulnerability in Microsoft Windows computers. (MS17-010). The malware spreads itself within corporate networks, without user interaction, by exploiting the vulnerability. The payload gets loaded in C:\ProgramData\, in a hidden folder with random name.

2. The malware encrypts files with the extensions listed below and appends *.WCRY* to the end of the file name:

> *.123, .3dm, .3ds, .3g2, .3gp, .602, .7z, .ARC, .PAQ, .accdb, .aes, .ai, .asc, .asf, .asm, .asp, .avi, .backup, .bak, .bat, .bmp, .brd, .bz2, .cgm, .class, .cmd, .cpp, .crt, .cs, .csr, .csv, .db, .dbf, .dch, .der, .dif, .dip, .djvu, .doc, .docb, .docm, .docx, .dot, .dotm, .dotx, .dwg, .edb, .eml, .fla, .flv, .frm, .gif, .gpg, .gz, .hwp ,.ibd, .iso, .jar, .java, .jpeg, .jpg, .js, .jsp, .key, .lay, .lay6, .ldf, .m3u, .m4u, .max, .mdb, .mdf, .mid, .mkv, .mml, .mov, .mp3, .mp4, .mpeg, .mpg, .msg, .myd, .myi, .nef, .odb, .odg, .odp, .ods, .odt, .onetoc2, .ost, .otg, .otp, .ots, .ott, .p12, .pas, .pdf, .pem, .pfx, .php, .pl, .png, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .psd, .pst, .rar, .raw, .rb, .rtf, .sch, .sh, .sldm, .sldx, .slk, .sln, .snt, .sql, .sqlite3, .sqlitedb, .stc, .std, .sti, .stw, .suo, .svg, .swf, .sxc, .sxd, .sxi, .sxm, .sxw, .tar, .tbk, .tgz, .tif, .tiff, .txt, .uop, .uot, .vb, .vbs, .vcd, .vdi, .vmdk, .vmx, .vob, .vsd, .vsdx, .wav, .wb2, .wk1, .wks, .wma, .wmv, .xlc, .xlm, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xlw, .zip*

3. WannaCry encrypts data files and ask users to pay a US$300 ransom in bitcoins. The ransom note indicates that the payment amount will be doubled after three days. If payment is not made after seven days, the encrypted files will be deleted. The Ransom demand screen displayed by WannaCry . Trojan is shown below:



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

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.

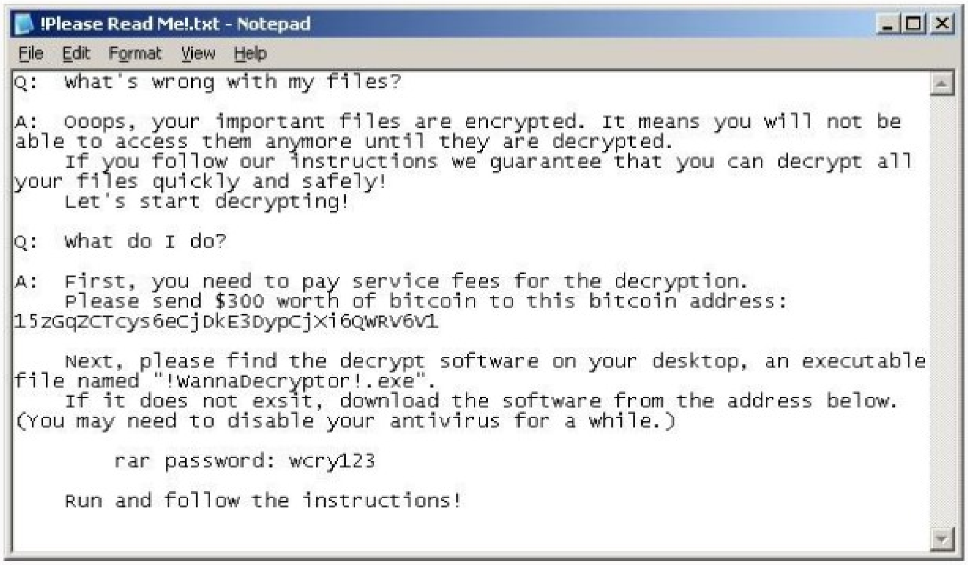
Can I Recover My Files?

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

4. It also drops a file named *!Please Read Me!.txt* which contains the ransom note. This is shown below for your reference:



!Please Read Me!.txt - Notepad

```
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!
```

How to detect the attack?

Microsoft Anti-Malware products detect the present version of this WannaCry ransomware as **Ransom:Win32.WannaCrypt** from definition version **1.243.291.0**

WHAT TO DO

- Aggressively **patch and update** Anti-Virus signatures with a priority on those in the last 60 days (including MS17-010).
- Warn users **not to open attachments/enable macros** on suspicious emails. This may be the entry vector so diligence is warranted
- If you suspect you may be a victim, install Windows Defender; and run to remove the malware on systems
- If you are experiencing major outage issues, contact your Microsoft Windows representative.
- If patching is not possible (i.e. if the machines cannot be updated with the March MS17-010), temporarily block SMB connections to limit the spread. This will likely impact your organization's services.

Please for more information you can contact us:

Tonga National CERT
Ministry of MEIDECC
OG Sanft Building Level 2
Nuku'alofa
Tel: 2378 (CERT)
email: cert@cert.to
web: www.cert.to