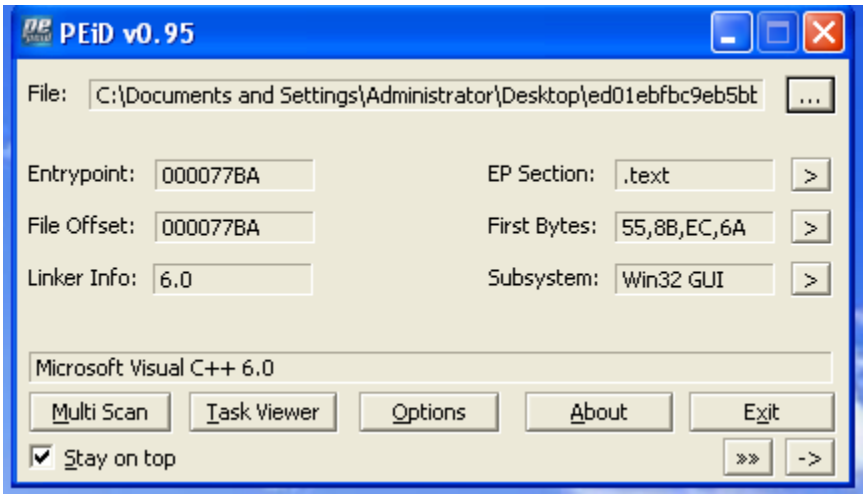
Malware Analyst: Mahmoud Morsy ElMenshawy

Ransomware: WannaCry

Summary Of Ransomeware:

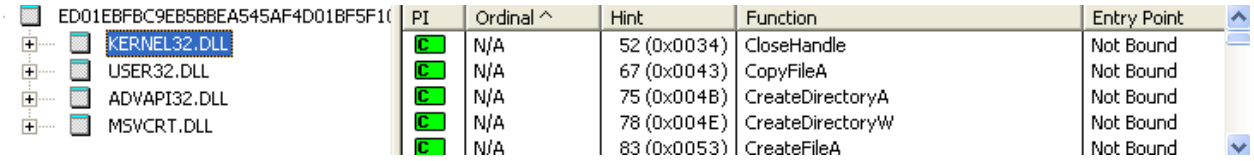
Wannacry is ransomware that spread quickly among several computer in the same network using vulnerability of SMB (MS17-010) it have huge files once for connecting to attacker ip and other for encryption files using AES And RSA Algorithm, creating services, encrypted files and add extension .WCRY and need amount of Bit coins from 300$ - $600 to decrypt files.

Static analysis:



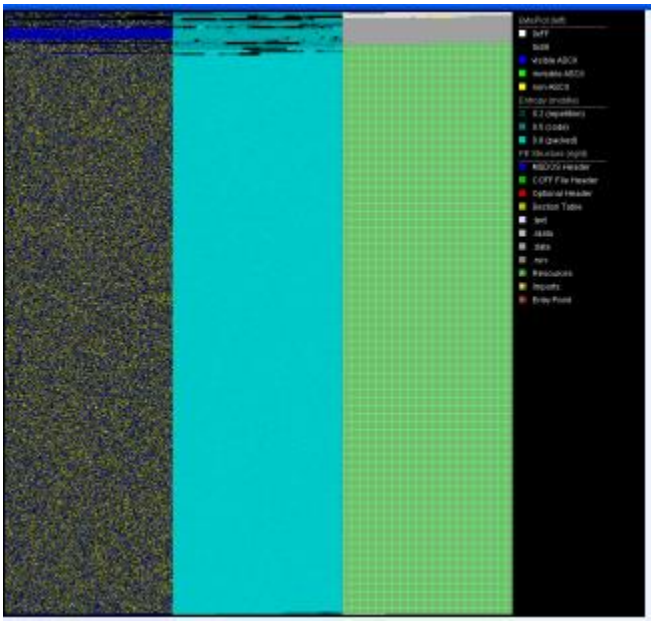
We load ransomeware in PEID we see that it is not packing and the file written with language called Microsoft visual c++. So we open malware using preview check the execution of compiled time we see it compiled in 2010/11/20.

We check for imports using dependency walker we see it import KERNEL32.DLL , USER32.DLL , ADVAPI32.DLL , MSVRT.DLL , if we go through of them we will notice that it create , open , close service , implement some technique of encryption like using windrows encryption .

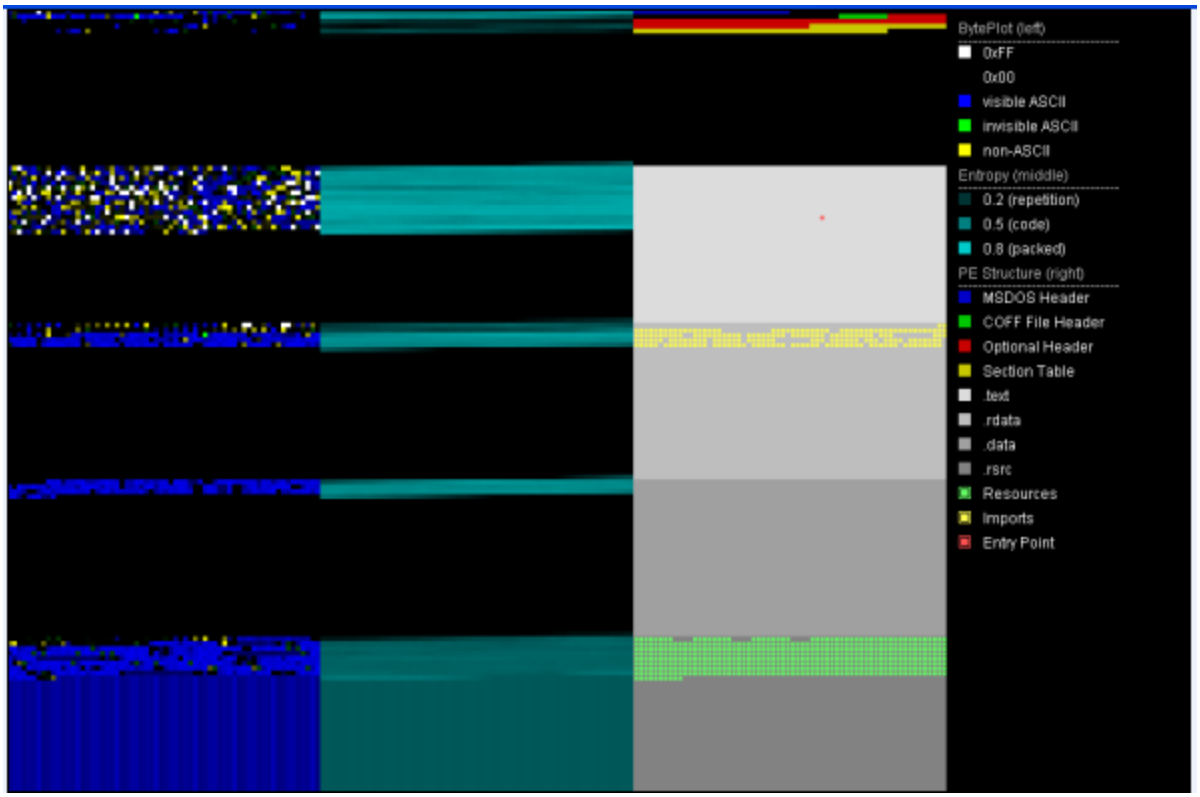


File characteristics:

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
Visualization:

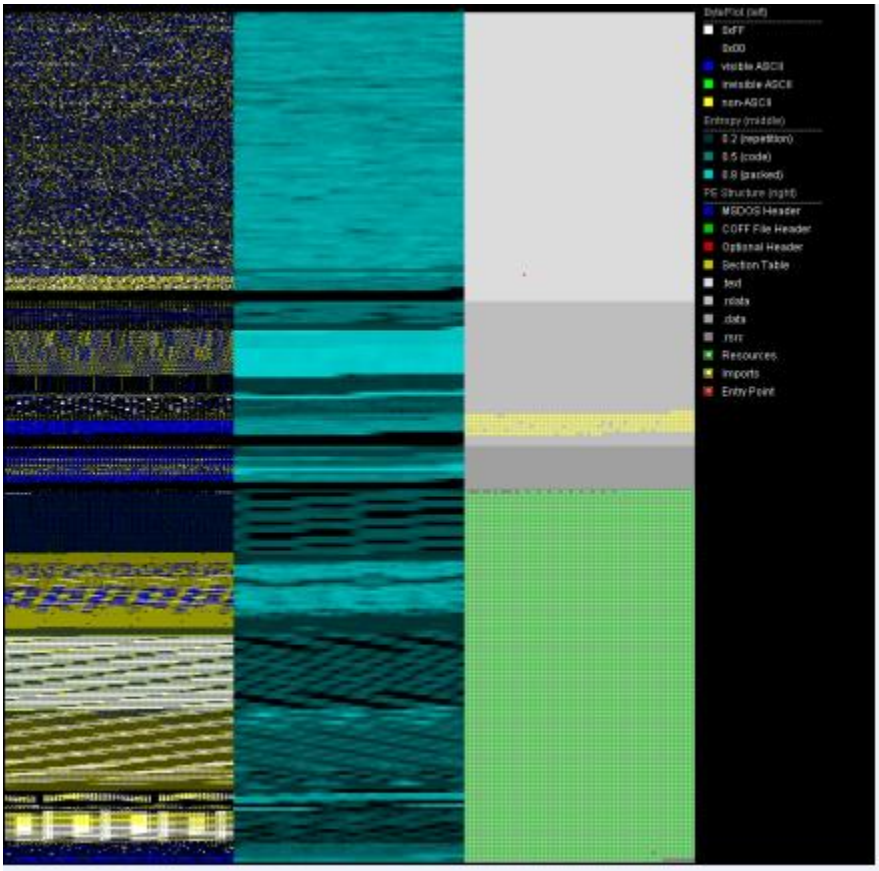


File Name: tasksche.
MD5: 84c82835a5d21bbcf75a61706d8ab549.
Size in bytes: 3514368.
Compiled time: 2010/11/20 sat 09:05:05 UTC
File Type: Executable.
Description: Loader + connection to attacker ip.
Visualization:



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.

Visualization:



Number Of connected Domains:

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

Persistence:

It creates process called tasksche and mssecsvc2 for persistence and the binary path of the 2 service is the actual path of current executable.

Mutex:

MsWinZonesCacheCounterMutexA.

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: 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

Dns Request (DEcryptor File):

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

Dns Request of File (Mssecsvc):

http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com

HTTP Request:

```
GET / HTTP/1.1
Host: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Date: Sat, 08 Jul 2017 13:23:17 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: close
Set-Cookie: __cfduid=d980260d16285e5643a7cd181aea4d1a61499520197; expires=Sun, 08-Jul-18
13:23:17 GMT; path=/; domain=.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com; HttpOnly
Server: cloudflare-nginx
CF-RAY: 37b35b7276a74173-CAI
```

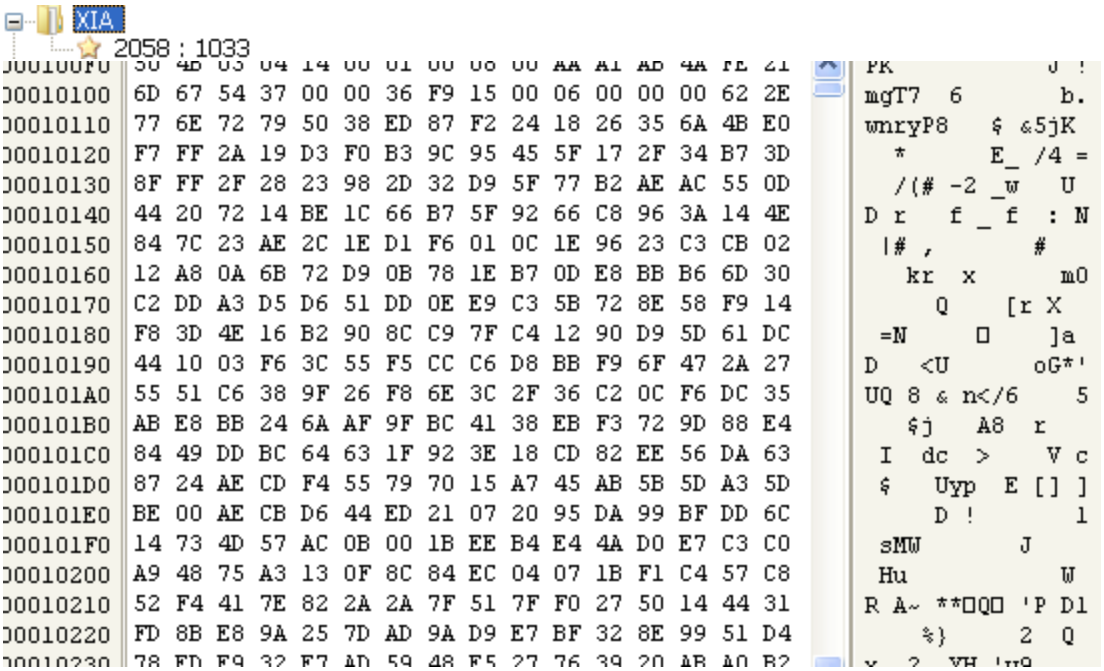
When ransomware executed it connect to domain www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com using InternetOpenURL.

Servers:

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

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.

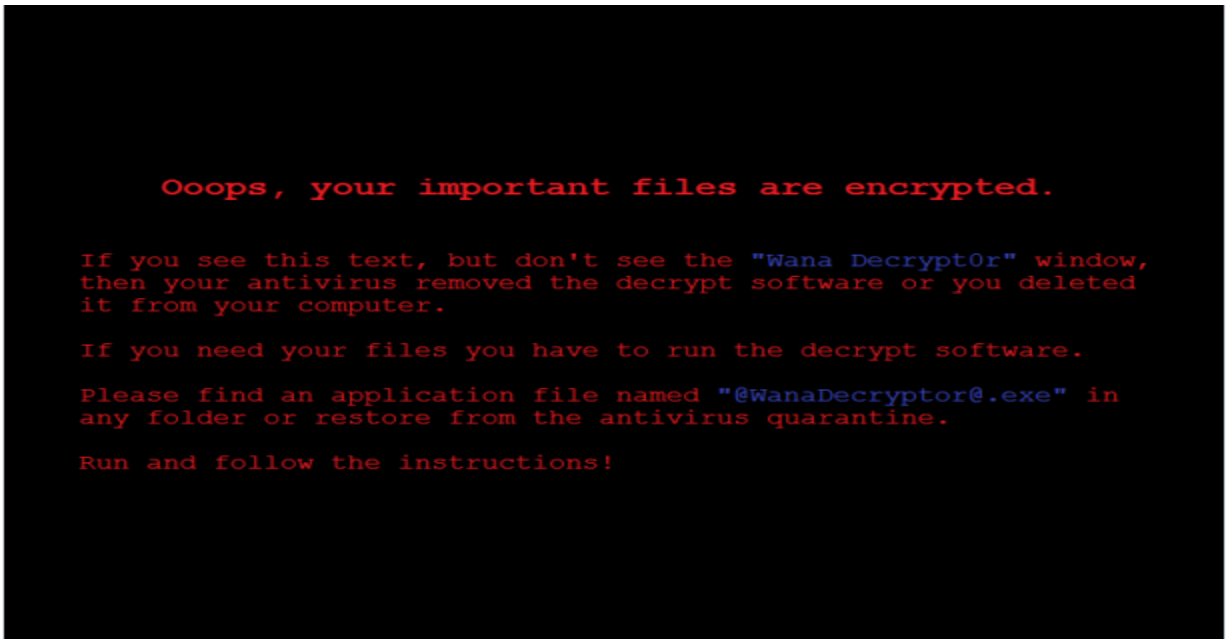


m_bulgarian.wnry	11/19/2010 11:16 ...	WNRY File	47 KB
m_chinese (simplified).wnry	11/19/2010 11:16 ...	WNRY File	54 KB
m_chinese (traditional).wnry	11/19/2010 11:16 ...	WNRY File	78 KB
m_croatian.wnry	11/19/2010 11:16 ...	WNRY File	39 KB
m_czech.wnry	11/19/2010 11:16 ...	WNRY File	40 KB
m_danish.wnry	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:

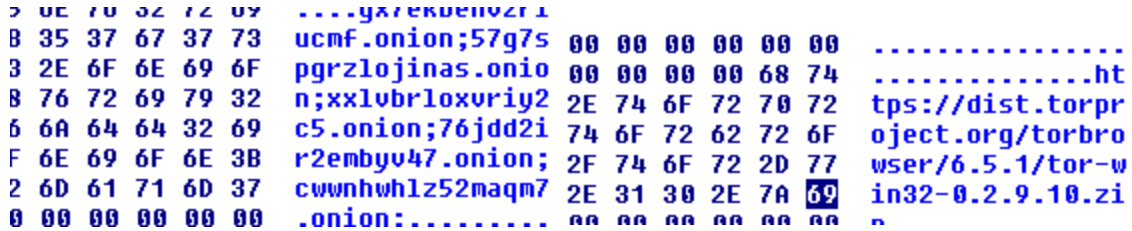
```
rule Ransomware_Wannacry {
        meta:
            filetype ="PE"
            author ="Mahmoud ElMenshawy"
            description = "Detect of Ransomware_Wannacry"
            date "5-8-2017"
            hash ="ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa"

        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
    }
```

Some screen shoots of Important Files:

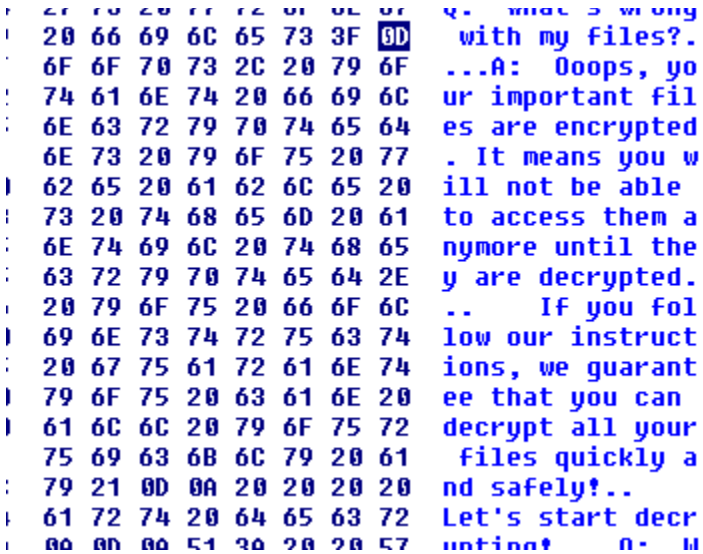

Ooops, your important files are encrypted.
If you see this text, but don't see the "Wana DecryptOr" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.
If you need your files you have to run the decrypt software.
Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.
Run and follow the instructions!

b.wncry


Wana DecryptOr 2.0
Ooops, your files have been encrypted!
English
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
Payment will be raised on
5/15/2017 17:23:59
Time Left
02:23:59:53
Your files will be lost on
5/19/2017 17:23:59
Time Left
06:23:59:53
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt



c.wncry



r.wncry

t.wncry (tool for encryption)

Md5: db349b97c37d22f5ea1d1841e3c89eb4

ShA256s:

0345723a6bcd1b46b3c668aa3bed0eca89609a4252cd7473a01de1bebba27b65