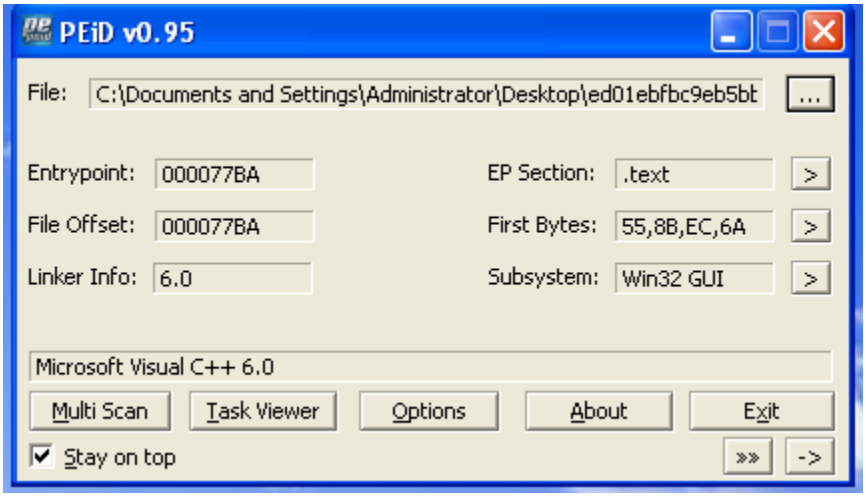
**Malware Analyst**: Mahmoud Morsy ElMenshawy

**Ransomware**: WannaCry

## Summary Of Ransomeware :

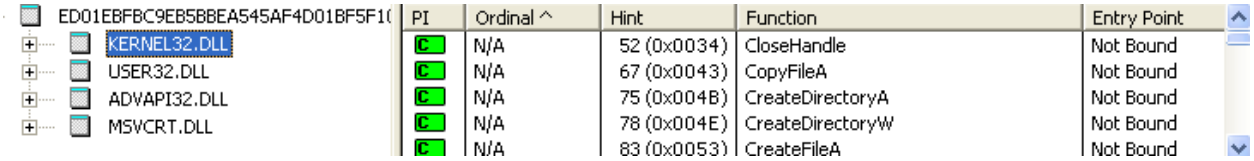
Wannacry is ransomware that spread quickly among several computer in the same network using vulnerability of SMB (MS17-010) it have huge files once for connecting to attacker ip and other for encryption files using AES And RSA Algorithm , creating services and need amount of Bit coins from 300$ - $600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

## Static analysis:




We load ransomeware in ollydbg 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 .



## Number Of connected Domains:

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

## Persistence:

Ransomware create process called tasksche and mssecsvc2 for persistence .

## Mutex:

MsWinZonesCacheCounterMutexA

## Dropped Files:

Mssecsvc ( connection to attacker ip )
b.wnry ( Ransomware Image )
c.wnry ( Configuration File ( Coonection To server And Download Tor browser ) )
r.wnry ( words of Ransomware in view When Run malware )
s.wnry ( Zip File Contain Tor Browser )
t.wnry ( Encryption Tool using AES algorithm )
taskdl ( used for delete Temporary Files )
taskse (support Decryption Tool )
u.wnry( Decryption Tool )

## Languages Files :

m_bulgarian.wnry
m_chinese (simplified).wnry
m_chinese (traditional).wnry
m_czech.wnry
m_danish.wnry
m_dutch.wnry
m_english.wnry
m_filipino.wnry
m_finnish.wnry
m_french.wnry
m_german.wnry
m_greek.wnry
m_indonesian.wnry

m_italian.wnry
m_japanese.wnry
m_korean.wnry
m_latvian.wnry
m_norwegian.wnry
m_polish.wnry
m_portuguese.wnry
m_romanian.wnry
m_russian.wnry
m_slovak.wnry
m_spanish.wnry
m_turkish.wnry
m_vietnamese.wnry

## Encryptor Files:

00000000.res
00000000.pky
00000000.eky

## Process Arguments:

icacls. /grant Everyone: F /T /C /Q
attrib +h
cmd.exe /c

## 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
```

**Servers:**

gx7ekbenv2ri ucmf .onion

57g7s pgrzlojinas.onion

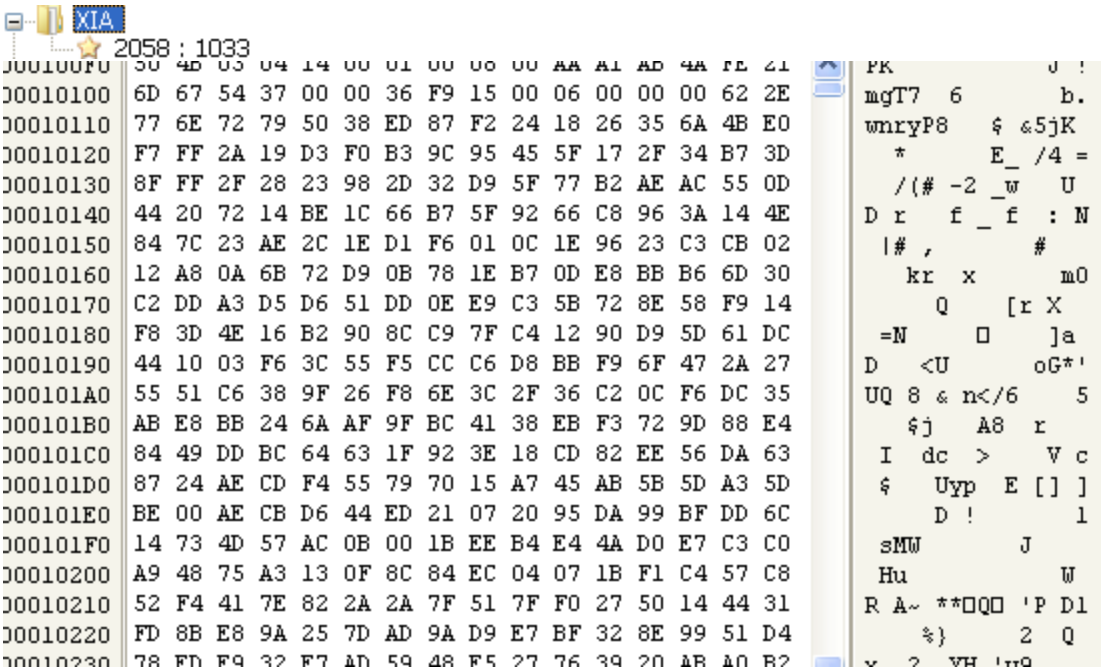
xxlvbrloxvriy2 c5.onion

76jdd2i r2embyv47.onion

cwwnhwhlz52maqm7 .onion

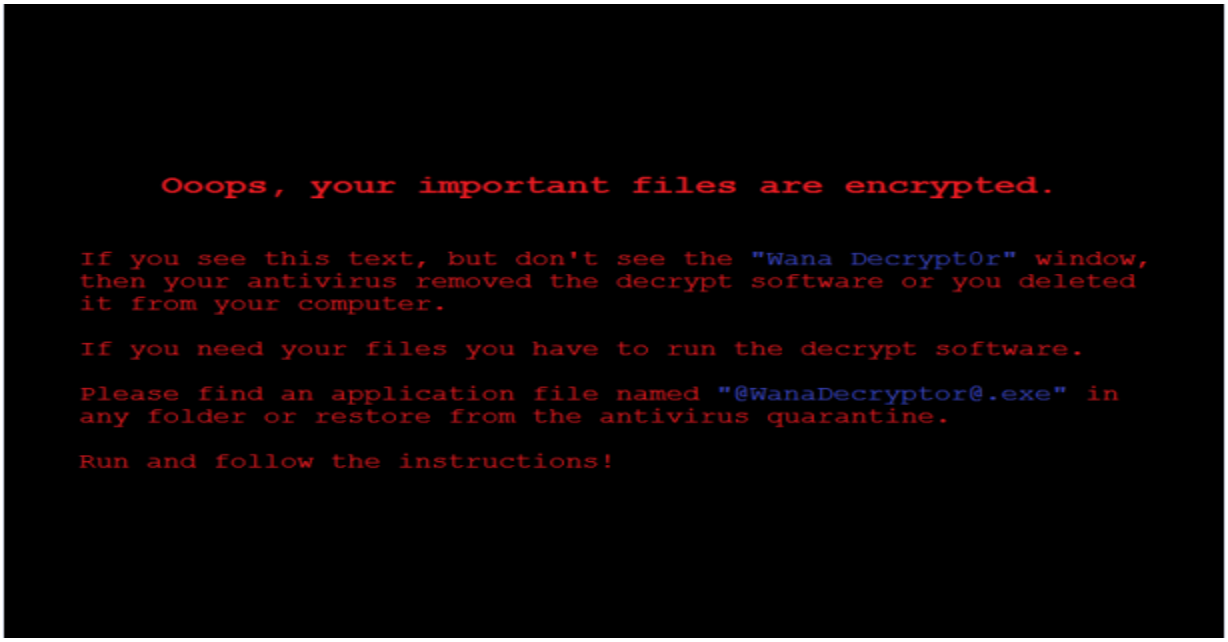
## Notes:

there is resource called “XIA” u have to convert it to bin then extract it WinRAR with password “WNcry@2ol7” then analysis each file .

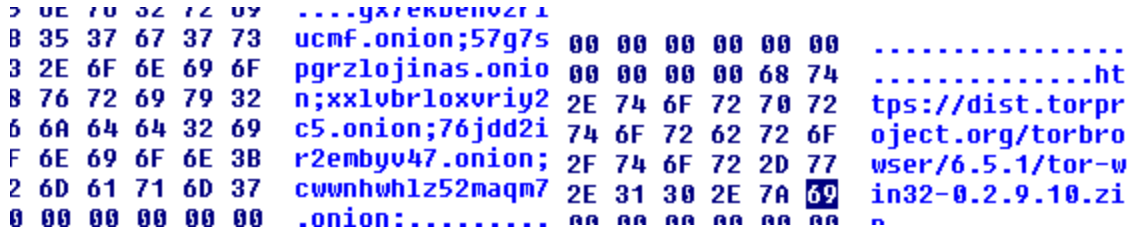



| | | | |
|---|---|---|---|
| m_bulgarian.wnry | 11/19/2010 11:16 ... | WNRY File | 47 KB |
| m_chinese (simplified).wnry | 11/19/2010 11:16 ... | WNRY File | 54 KB |
| m_chinese (traditional).wnry | 11/19/2010 11:16 ... | WNRY File | 78 KB |
| m_croatian.wnry | 11/19/2010 11:16 ... | WNRY File | 39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

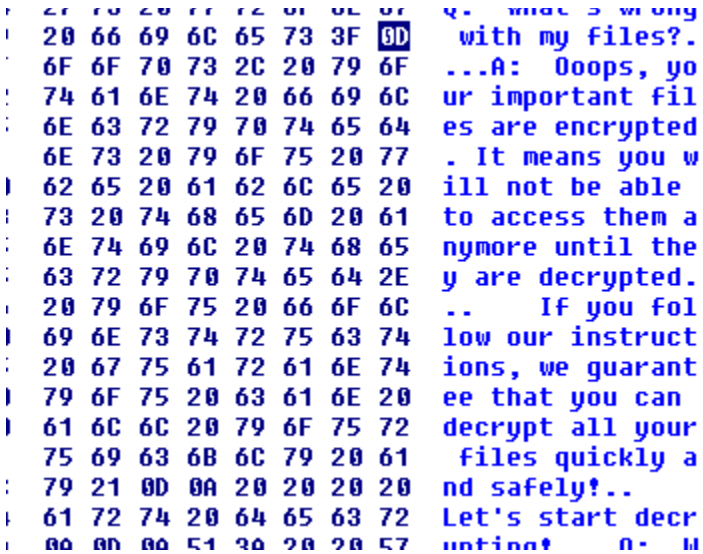
## Some screen shoots of Important Files:




b.wncry




c.wncry




r.wncry


t.wncry (tool for encryption)

**Md5:** db349b97c37d22f5ea1d1841e3c89eb4

ShA256s:

0345723a6bcd1b46b3c668aa3bed0eca89609a4252cd7473a01de1bebba27b65