

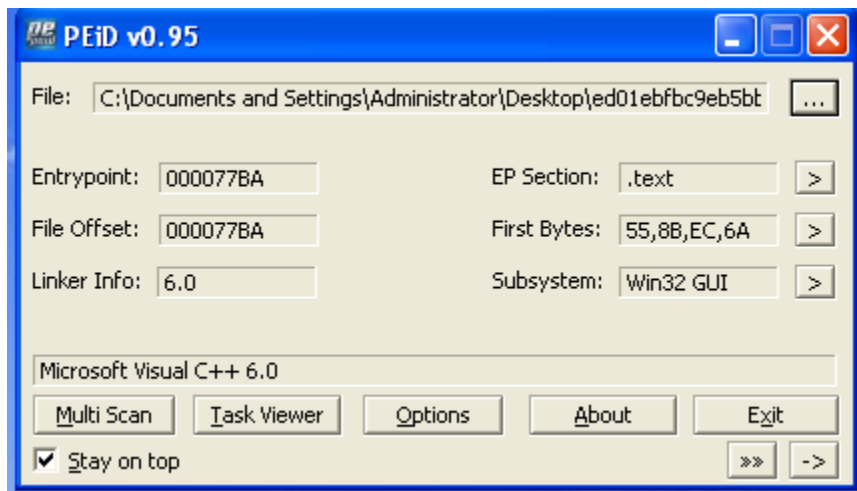
Malware Analyst: Mahmoud Morsy ElMenshawy

Ransomware: WannaCry

Summary Of Ransomware :

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 ransomware 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 .

0004	Number of Sections	
4CE78F41	Time Date Stamp	2010/11/20 Sat 09:05:05 UTC
00000000	File Signature	

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 .

	PI	Ordinal ^	Hint	Function	Entry Point
ED01EBFBC9EB5B8EA545AF4D01BF5F1(
KERNEL32.DLL	✓	N/A	52 (0x0034)	CloseHandle	Not Bound
USER32.DLL	✓	N/A	67 (0x0043)	CopyFileA	Not Bound
ADVAPI32.DLL	✓	N/A	75 (0x004B)	CreateDirectoryA	Not Bound
MSVCRT.DLL	✓	N/A	78 (0x004E)	CreateDirectoryW	Not Bound
	✓	N/A	83 (0x0053)	CreateFileA	Not Bound

Number Of connected Domains:

- (1) 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94.
- (2) 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw.
- (3) 115p7UMMngoj1pMvvpHijcRdfJNXj6LrLn.

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 (Coonnection 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:

icaccls. /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 pgrzlojinaz.onion

xxlvbrloxvriy2 c5.onion

76jdd2ir2embyv47.onion

cwwnhwhlz52maq7m7 .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 .



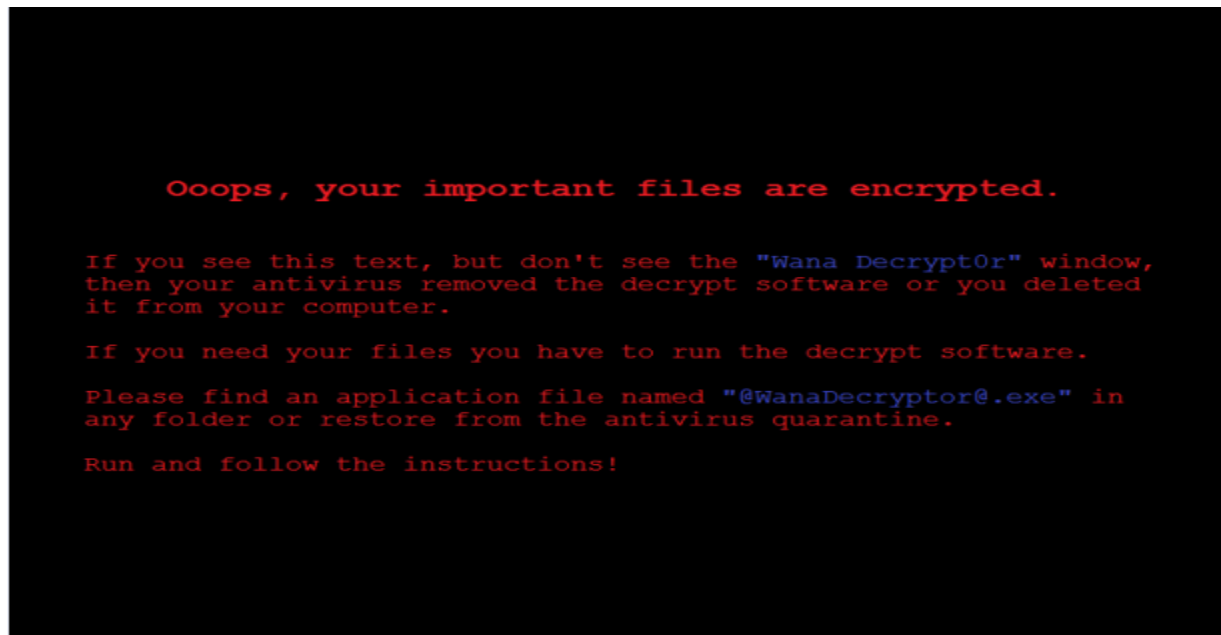
2058 : 1033

000100F0 50 4D 03 04 14 00 01 00 00 00 AA A1 AD 9A FE 41
00010100 6D 67 54 37 00 00 36 F9 15 00 06 00 00 00 62 2E
00010110 77 6E 72 79 50 38 ED 87 F2 24 18 26 35 6A 4B E0
00010120 F7 FF 2A 19 D3 F0 B3 9C 95 45 5F 17 2F 34 B7 3D
00010130 8F FF 2F 28 23 98 2D 32 D9 5F 77 B2 AE AC 55 0D
00010140 44 20 72 14 BE 1C 66 B7 5F 92 66 C8 96 3A 14 4E
00010150 84 7C 23 AE 2C 1E D1 F6 01 0C 1E 96 23 C3 CB 02
00010160 12 A8 0A 6B 72 D9 0B 78 1E B7 0D E8 BB B6 6D 30
00010170 C2 DD A3 D5 D6 51 DD 0E E9 C3 5B 72 8E 58 F9 14
00010180 F8 3D 4E 16 B2 90 8C C9 7F C4 12 90 D9 5D 61 DC
00010190 44 10 03 F6 3C 55 F5 CC C6 D8 BB F9 6F 47 2A 27
000101A0 55 51 C6 38 9F 26 F8 6E 3C 2F 36 C2 0C F6 DC 35
000101B0 AB E8 BB 24 6A AF 9F BC 41 38 EB F3 72 9D 88 E4
000101C0 84 49 DD BC 64 63 1F 92 3E 18 CD 82 EE 56 DA 63
000101D0 87 24 AE CD F4 55 79 70 15 A7 45 AB 5B 5D A3 5D
000101E0 BE 00 AE CB D6 44 ED 21 07 20 95 DA 99 BF DD 6C
000101F0 14 73 4D 57 AC 0B 00 1B EE B4 E4 4A D0 E7 C3 C0
00010200 A9 48 75 A3 13 0F 8C 84 EC 04 07 1B F1 C4 57 C8
00010210 52 F4 41 7E 82 2A 2A 7F 51 7F F0 27 50 14 44 31
00010220 FD 8B E8 9A 25 7D AD 9A D9 E7 BF 32 8E 99 51 D4
00010230 78 FD F9 32 F7 AD 59 48 F5 27 76 39 20 AB AD B2

PK 0 !
mgT7 6 b.
wnryP8 \$ &5jK
* E_ /4 =
/(# -2 _w U
D r f _ f : N
l# , #
kr x m0
Q [r X
=N □]a
D <U oG*'
UQ 8 & n</6 5
\$j A8 r
I dc > V c
\$ Uyp E []
D ! l
sMW J
Hu W
R A~ **□□ 'P D1
%} 2 Q
v 2 VH lrrg

	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
	taskse.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



```

> 0E 70 32 72 07 ....gx7ekdenozr1
B 35 37 67 37 73 ucmf.onion;57g7s 00 00 00 00 00 00 .....
3 2E 6F 6E 69 6F pgrzlojinas.onio 00 00 00 00 68 74 .....ht
B 76 72 69 79 32 n;xxlvbrloxvriy2 2E 74 6F 72 70 72 tps://dist.torpr
6 6A 64 64 32 69 c5.onion;76jdd2i 74 6F 72 62 72 6F oject.org/torbro
F 6E 69 6F 6E 3B r2embyv47.onion; 2F 74 6F 72 2D 77 wser/6.5.1/tor-w
2 6D 61 71 6D 37 cwwnhwhlz52maq7 2E 31 30 2E 7A 69 in32-0.2.9.10.zi
0 00 00 00 00 00 .onion:..... 00 00 00 00 00 00 n

```

c.wncry

```

: 2F 70 20 7F 72 07 0E 07 q. what's wrong
: 20 66 69 6C 65 73 3F 0D with my files?.
: 6F 6F 70 73 2C 20 79 6F ...A: Ooops, yo
: 74 61 6E 74 20 66 69 6C ur important fil
: 6E 63 72 79 70 74 65 64 es are encrypted
: 6E 73 20 79 6F 75 20 77 . It means you w
: 62 65 20 61 62 6C 65 20 ill not be able
: 73 20 74 68 65 6D 20 61 to access them a
: 6E 74 69 6C 20 74 68 65 nymore until the
: 63 72 79 70 74 65 64 2E y are decrypted.
: 20 79 6F 75 20 66 6F 6C .. If you fol
: 69 6E 73 74 72 75 63 74 low our instruct
: 20 67 75 61 72 61 6E 74 ions, we guarant
: 79 6F 75 20 63 61 6E 20 ee that you can
: 61 6C 6C 20 79 6F 75 72 decrypt all your
: 75 69 63 6B 6C 79 20 61 files quickly a
: 79 21 0D 0A 20 20 20 20 nd safely!..
: 61 72 74 20 64 65 63 72 Let's start decr
: 00 00 00 51 30 20 20 57 untinat! 0. M

```

r.wncry

```

3A 52 51 03 CB 7B 7B 8B E8 A3 3E 46 BC 9D 33 BF CE RQ.-{iFú>F+¥3++
7A 48 15 2B DC EF 38 53 69 01 64 8E F3 4E B3 59 4B H.+_n8Si.dâ=N!YK
3A 12 85 88 72 C3 9C 08 43 A3 10 3E 53 AF CA 97 D4 .âêr+£.Cú.>S»-û+
3A D4 D6 FD 16 BB 8C CD F9 02 CF 2B 9E 38 1C A2 50 ++^._î-.-+P8.óP
3A 7F 23 9E 31 9A 82 67 28 93 68 B5 E7 32 0A A2 FE ■#P1Ûég(ôh!t2.ó!
3A B7 F2 85 AB 3D 40 61 78 92 9C 75 E0 C9 B8 56 71 +=à%=@axæua++Uq
3A 6A 5D A1 5D 32 5B B3 6F F8 82 56 31 54 BE 58 66 j]]i]2[!o°éU1T+Xf
3A 37 C5 D3 25 9C 35 8E BA 94 B5 9A 6B 43 1E 32 38 7++%£5â!ô!ÛkC.28
3A 4E 8D 20 8C 77 44 3E AC D5 33 68 45 0E B6 14 DB Nî îwD>%+3hE.!.!
3A DF 68 08 3A 22 4E CA 3C 82 06 31 8E 1A 57 7F 4C _h.: "N-<é.1Ã.W■L
3A 4D E1 25 DC 4F CD AD C9 22 15 6E 2F 4B B4 81 29 M0%_0-;+"n/K!ü)
3A 93 57 C6 28 52 FA F2 0E FB 87 F0 02 5A C5 DB EA ôW!(R=-.vç=.Z+!0
3A B4 38 4A 4E E9 1A FA 99 19 16 92 50 D3 5C 16 4D !8JNT.-Ü...æP+\.M
3A 73 54 56 4A 25 90 78 FD 9D C5 28 F3 C1 DA 2B 6C sTUVJ%Êx²¥+(=-+1
3A 0D C3 18 06 9F 84 D0 14 4A 54 20 50 73 AB EE 26 .+...■ä-.JT Ps%e&
3A EF B5 7B 00 C5 61 13 4E 1A AC 0B AD 21 1A 56 18 n!{.+a.N.%.;!U.
3A D1 F1 2A B0 9E 40 92 F2 D5 D0 B3 16 20 9F 0C 46 -+*!P@æ=+!|. ■.F
3A C8 D2 06 4B 3A 28 27 F4 E7 5B E3 EC 2F 7B A0 09 +- .K:( '(t[p8/{á.
3A 00 00 54 20 97 60 9F 0F F7 F2 F2 00 07 F0 F7 4B 0.~!F5tUWU..F+

```

t.wncry (tool for encryption)

Md5: db349b97c37d22f5ea1d1841e3c89eb4

ShA256s:

0345723a6bcd1b46b3c668aa3bed0eca89609a4252cd7473a01de1bebbba27b65