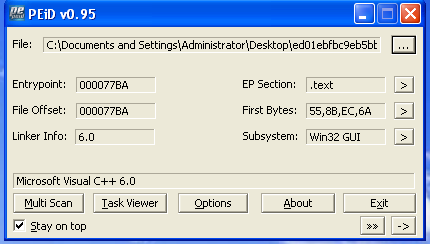
**Malware Analyst**: Mahmoud Morsy ElMenshawy

Ransomware: WannaCry

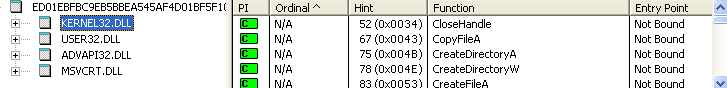
**Summary Of Ransomeware :**Wannacry is ransomware that spread quickly among serveral computer in the same network using vulnerability of SMB (MS17-010) it have huge files once for connecting to attacker ip and other for encryption files using AES And RSA Algorithm , creating services and need amount of Bitcoins 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 uing peview check the execution of compiled time we see it compiled in 2010/11/20   
C:\Users\Mahmoud_El_Menshawy\Desktop\4.PNG

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

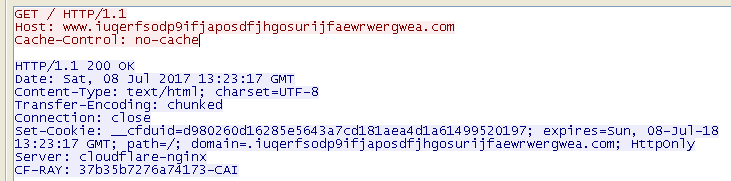
**Deopped Files:**Mssecsvc ( connection to attacker ip )  
b.wnry ( Ransomware Image )   
c.wnry ( Configuration File ( Coonection To server AndDownload Tor browser ) )  
r.wnry ( words of Ransomware in view When Run malware )   
s.wnry ( Zip File Contain Tor Browser )   
t.wnry ( Encryption Tool using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

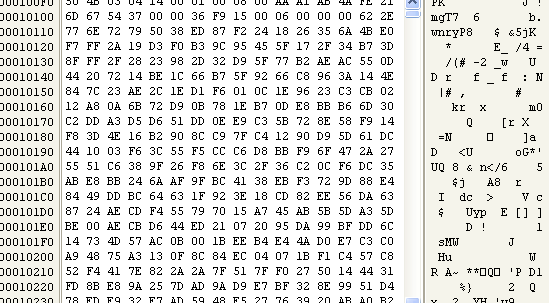
**Process Arguments:**   
icacls . /grant Everyone:F /T /C /Q  
attrib +h  
cmd.exe /c

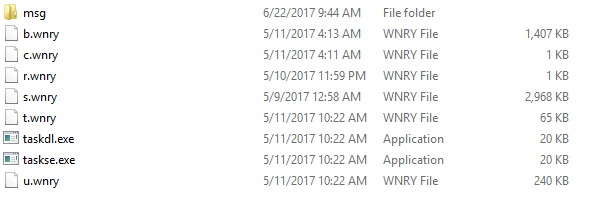
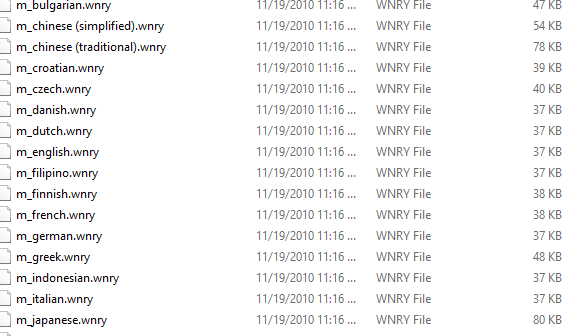
**Dns Request ( DEcryptor File ) :**<https://www.google.com/search?q=how+to+buy+bitcoin>  
<http://www.btcfrog.com/qr/bitcoinpng.php?address>   
https://en.wikipedia.org/wiki/Bitcoin

**Dns Request Of File (Mssecsvc) :**   
<http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com>

**HTTP Request:  
**

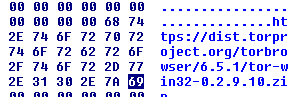
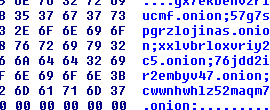
**Servers :**   
gx7ekbenv2ri ucmf .onion  
57g7s pgrzlojinas.onion  
xxlvbrloxvriy2 c5.onion  
76jdd2i r2embyv47.onion  
cwwnhwhlz52maqm7 .onion

**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 .  
C:\Users\Mahmoud_El_Menshawy\Desktop\Xia.PNG

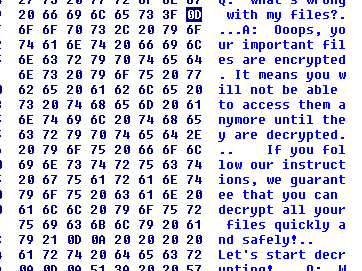
  
**Some screen shoots of Important Files:**



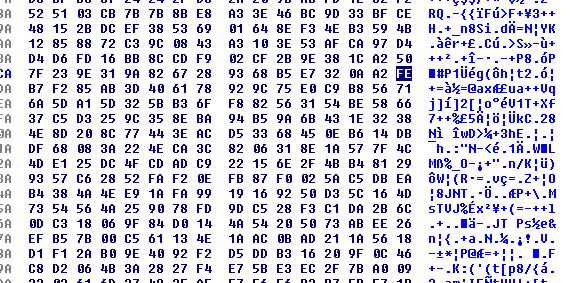
b.wncry



c.wncry



r.wncry



t.wncry (tool for encryption)

Md5 : db349b97c37d22f5ea1d1841e3c89eb4  
ShA256s : 0345723a6bcd1b46b3c668aa3bed0eca89609a4252cd7473a01de1bebba27b65