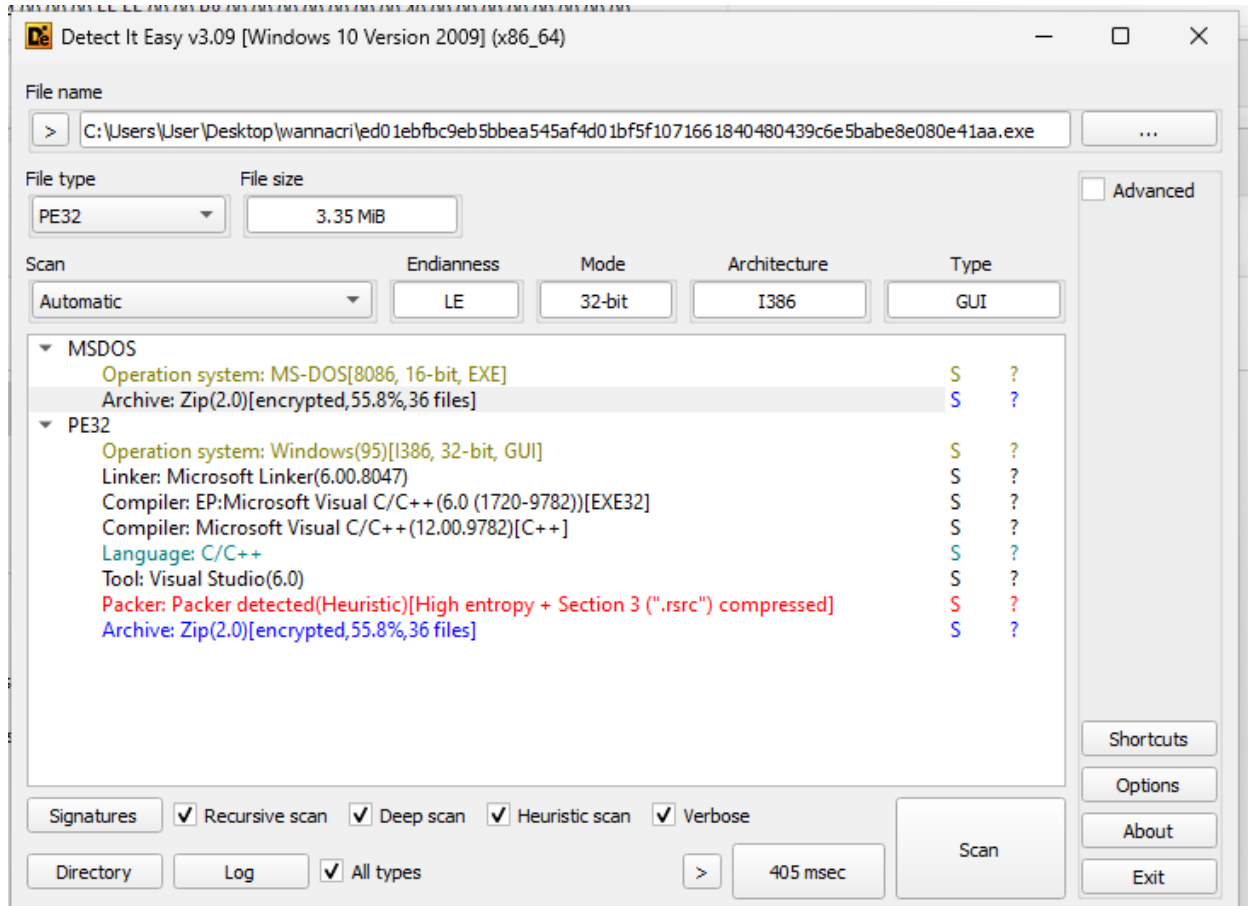
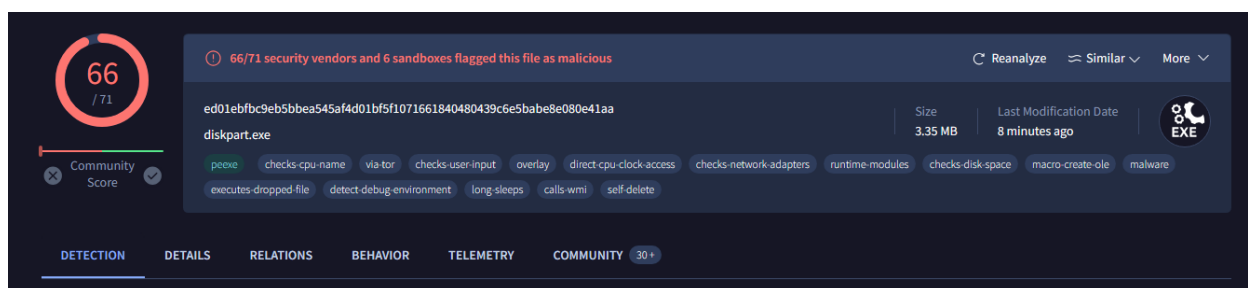


# lab1

- Hash ->  
**ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa**
- General info



- Virus Total data



- Sus strings

encoding (2)	size (bytes)	location	flag (28)	label (422)	group (11)	technique (16)	value (111594)
ascii	19	.data	x	-	reconnaissance	-	GetNativeSystemInfo
ascii	19	.rdata	x	import	cryptography	T1027   Obfuscated Files or Information	CryptReleaseContext
ascii	19	.data	x	-	cryptography	T1027   Obfuscated Files or Information	CryptAcquireContext
ascii	19	.rdata	x	import	-	-	SetCurrentDirectory
ascii	19	.rdata	x	import	-	-	SetCurrentDirectory
ascii	18	.rdata	x	import	execution	-	GetExitCodeProcess
ascii	17	.rdata	x	import	file	-	SetFileAttributes
ascii	16	.rdata	x	import	execution	-	TerminateProcess
ascii	15	.data	x	-	cryptography	T1027   Obfuscated Files or Information	CryptDestroyKey
ascii	14	.rdata	x	import	memory	T1055   Process Injection	VirtualProtect
ascii	14	.data	x	-	cryptography	T1027   Obfuscated Files or Information	CryptImportKey
ascii	13	.rdata	x	import	services	T1543   Create or Modify System Proc...	CreateService
ascii	13	.rdata	x	import	registry	T1112   Modify Registry	RegSetValueEx
ascii	13	.rdata	x	import	execution	T1106   Execution through API	CreateProcess
ascii	12	.rdata	x	import	registry	T1112   Modify Registry	RegCreateKey
ascii	12	.data	x	-	cryptography	T1027   Obfuscated Files or Information	CryptDecrypt
ascii	12	.data	x	-	cryptography	T1027   Obfuscated Files or Information	CryptEncrypt
ascii	11	.data	x	-	cryptography	T1027   Obfuscated Files or Information	CryptGenKey
ascii	10	.data	x	-	file	T1485   Data Destruction	DeleteFile
ascii	10	.data	x	-	file	T1105   Remote File Copy	MoveFileEx
ascii	9	.rdata	x	import	file	-	WriteFile
ascii	9	.data	x	import	file	-	WriteFile
ascii	8	.data	x	-	file	T1105   Remote File Copy	MoveFile
ascii	5	.rdata	x	-	cryptography	T1027   Obfuscated Files or Information	srand
ascii	4	.rdata	x	-	cryptography	T1027   Obfuscated Files or Information	rand
ascii	3	.rsrc	x	-	-	-	xmR
ascii	3	.rsrc	x	-	-	-	xMR
ascii	3	.rsrc	x	-	-	-	xMr

- Libraries used

library (4)	duplicate (0)	flag (0)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (114)	group	description
KERNEL32.dll	-	-	-	0x0000D638	0x0000802C	implicit	54	-	Windows NT BASE API Client
USER32.dll	-	-	-	0x0000D7DC	0x000081D0	implicit	1	-	Multi-User Windows USER API Client Library
ADVAPI32.dll	-	-	-	0x0000D60C	0x00008000	implicit	10	-	Advanced Windows 32 Base API
MSVCRT.dll	-	-	-	0x0000D714	0x00008108	implicit	49	-	Microsoft C Runtime Library

- Sus imports

imports (114)	flag (14)	callback (0)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (10)	technique (11)	type (1)	ordinal (0)	library (4)
srand	x	-	0x0000DCE6	0x0000DCE6	678 (0x02A6)	cryptography	T1027   Obfuscated Files or Information	implicit	-	MSVCRT.dll
srand	x	-	0x0000DCEE	0x0000DCEE	692 (0x02B4)	cryptography	T1027   Obfuscated Files or Information	implicit	-	MSVCRT.dll
VirtualProtect	x	-	0x0000D836	0x0000D836	902 (0x0386)	memory	T1055   Process Injection	implicit	-	KERNEL32.dll
WriteFile	x	-	0x0000D97E	0x0000D97E	932 (0x03A4)	file	-	implicit	-	KERNEL32.dll
SetFileAttributesW	x	-	0x0000D9BA	0x0000D9BA	794 (0x031A)	file	-	implicit	-	KERNEL32.dll
CreateProcessA	x	-	0x0000D832	0x0000D832	102 (0x0066)	execution	T1106   Execution through API	implicit	-	KERNEL32.dll
TerminateProcess	x	-	0x0000D808	0x0000D808	862 (0x035E)	execution	-	implicit	-	KERNEL32.dll
GetExitCodeProcess	x	-	0x0000D7F2	0x0000D7F2	346 (0x015A)	execution	-	implicit	-	KERNEL32.dll
SetCurrentDirectoryW	x	-	0x0000D9D0	0x0000D9D0	779 (0x030B)	-	-	implicit	-	KERNEL32.dll
SetCurrentDirectoryA	x	-	0x0000D882	0x0000D882	778 (0x030A)	-	-	implicit	-	KERNEL32.dll
CreateServiceA	x	-	0x0000DC2A	0x0000DC2A	100 (0x0064)	services	T1543   Create or Modify System Process	implicit	-	ADVAPI32.dll
RegCreateKeyW	x	-	0x0000DC04	0x0000DC04	467 (0x01D3)	registry	T1112   Modify Registry	implicit	-	ADVAPI32.dll
RegSetValueExA	x	-	0x0000D8F2	0x0000D8F2	518 (0x0204)	registry	T1112   Modify Registry	implicit	-	ADVAPI32.dll
CryptReleaseContext	x	-	0x0000DC14	0x0000DC14	160 (0x00A0)	cryptography	T1027   Obfuscated Files or Information	implicit	-	ADVAPI32.dll

- HTTP request and DNS resolutions

### HTTP Requests

http://192.168.122.1:9200/\_bulk

HTTP Method

POST

### DNS Resolutions

129.214.248.87.in-addr.arpa

147.251.123.92.in-addr.arpa

152.251.123.92.in-addr.arpa

82.250.63.168.in-addr.arpa

crt.sectigo.com

- Files

Files Opened

%ALLUSERSPROFILE%\application data\microsoft\office\data\opa12.bak

%ALLUSERSPROFILE%\application data\microsoft\user account pictures\default pictures\airplane.bmp

%ALLUSERSPROFILE%\application data\microsoft\user account pictures\default pictures\astronaut.bmp

%ALLUSERSPROFILE%\application data\microsoft\user account pictures\default pictures\ball.bmp

%ALLUSERSPROFILE%\application data\microsoft\user account pictures\default pictures\beach.bmp

%ALLUSERSPROFILE%\application data\microsoft\user account pictures\default pictures\butterfly.bmp

%ALLUSERSPROFILE%\application data\microsoft\user account pictures\default pictures\car.bmp

%ALLUSERSPROFILE%\application data\microsoft\user account pictures\default pictures\cat.bmp

%ALLUSERSPROFILE%\application data\microsoft\user account pictures\default pictures\chess.bmp

%ALLUSERSPROFILE%\application data\microsoft\user account pictures\default pictures\dirt bike.bmp

Files Written

%ALLUSERSPROFILE%\Documents\My Music\Sample Music\Beethoven's Symphony No. 9 (Scherzo).wma

%ALLUSERSPROFILE%\Documents\My Music\Sample Music\New Stories (Highway Blues).wma

%ALLUSERSPROFILE%\Documents\My Pictures\Sample Pictures\Blue hills.jpg

%ALLUSERSPROFILE%\Documents\My Pictures\Sample Pictures\Sunset.jpg

%ALLUSERSPROFILE%\Documents\My Pictures\Sample Pictures\Water lilies.jpg

%ALLUSERSPROFILE%\Documents\My Pictures\Sample Pictures\Winter.jpg

%ALLUSERSPROFILE%\documents\my music\sample music\@please\_read\_me@.txt

%ALLUSERSPROFILE%\documents\my music\sample music\@wanadecryptor@.exe.lnk

%ALLUSERSPROFILE%\documents\my music\sample music\beethoven's symphony no. 9 (scherzo).wma.wncryt

%ALLUSERSPROFILE%\documents\my music\sample music\new stories (highway blues).wma.wncryt

- Shell commands

Shell Commands

"%SAMPLEPATH%\diskpart.exe"

"%SAMPLEPATH%\ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe"

"%SAMPLEPATH%\file001\_tasksche.exe"

"C:\Program Files (x86)\Google\1496\_1906822985\bin\updater.exe" --update --system --enable-logging --vmodule="/chrome/updater/\*=2 /sessionId [F212D80D-137E-4DA7-BC54-DD3D939E8CF3] --enable-logging --vmodule="/components/winhttp/\*=1,/components/update\_client/\*=2,/chrome/updater/\*=2

"C:\Program Files (x86)\Google\1496\_1906822985\bin\updater.exe" --crash-handler --enable-logging --vmodule="/components/winhttp/\*=1,/components/update\_client/\*=2,/chrome/updater/\*=2 --system "-database=C:\Program Files (x86)\Google\GoogleUpdater\119.0.6042.0\Crashpad" --url=https://clients2.google.com/cr/report --annotation=prod=Update4 --annotation=ver=119.0.6042.0 --attachment=C:\Program Files (x86)\Google\GoogleUpdater\updater.log" --initial-client-data=0x254,0x258,0x25c,0x230,0x260,0x7dac08,0x7dac18,0x7dac24

"C:\Program Files (x86)\Google\2508\_1380917538\bin\updater.exe" --update --system --enable-logging --vmodule="/chrome/updater/\*=2 /sessionId [CD1578F8-6C83-4468-AC05-592A842805B5] --enable-logging --vmodule="/components/winhttp/\*=1,/components/update\_client/\*=2,/chrome/updater/\*=2

"C:\Program Files (x86)\Google\2508\_1380917538\bin\updater.exe" --crash-handler --enable-logging --vmodule="/components/winhttp/\*=1,/components/update\_client/\*=2,/chrome/updater/\*=2 --system "-database=C:\Program Files (x86)\Google\GoogleUpdater\117.0.5934.0\Crashpad" --url=https://clients2.google.com/cr/report --annotation=prod=Update4 --annotation=ver=117.0.5934.0 --initial-client-data=0x254,0x258,0x25c,0x230,0x260,0x16fab90,0x16fab0,0x16fabac

"C:\Program Files (x86)\Google\3756\_1517631155\bin\updater.exe" --update --system --enable-logging --vmodule="/chrome/updater/\*=2 /sessionId [9665AC88-A289-46CB-BDC7-BAABE67F4D53] --enable-logging --vmodule="/components/winhttp/\*=1,/components/update\_client/\*=2,/chrome/updater/\*=2

"C:\Program Files (x86)\Google\3756\_1517631155\bin\updater.exe" --crash-handler --enable-logging --vmodule="/components/winhttp/\*=1,/components/update\_client/\*=2,/chrome/updater/\*=2 --system "-database=C:\Program Files (x86)\Google\GoogleUpdater\121.0.6116.0\Crashpad" --url=https://clients2.google.com/cr/report --annotation=prod=Update4 --annotation=ver=121.0.6116.0 --attachment=C:\Program Files (x86)\Google\GoogleUpdater\updater.log" --initial-client-data=0x254,0x258,0x25c,0x230,0x260,0x1661bec,0x1661bf8,0x1661c04

- Cryptographical algorithms

encoding (2)	size (bytes)	location	flag (28)	label (422)	group (11)	technique (16)	value (111594)
ascii	1430	version	-	size	-	-	<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">\n <trustInfo xmlns="urn:schemas-micro...
ascii	53	.pdata	-	-	-	T1001   Data Obfuscation	Microsoft Enhanced RSA and AES Cryptographic Provider
ascii	45	.pdata	-	-	-	-	inflate 1.1.3 Copyright 1995-1998 Mark Adler
ascii	12	.pdata	x	-	cryptography	T1027   Obfuscated Files or Information	CryptDecrypt
ascii	12	.pdata	x	-	cryptography	T1027   Obfuscated Files or Information	CryptEncrypt

- Dynamic Analysis (process hacker)

Process Hacker [WINDEV2403EVAL\User]

Hacker View Tools Users Help

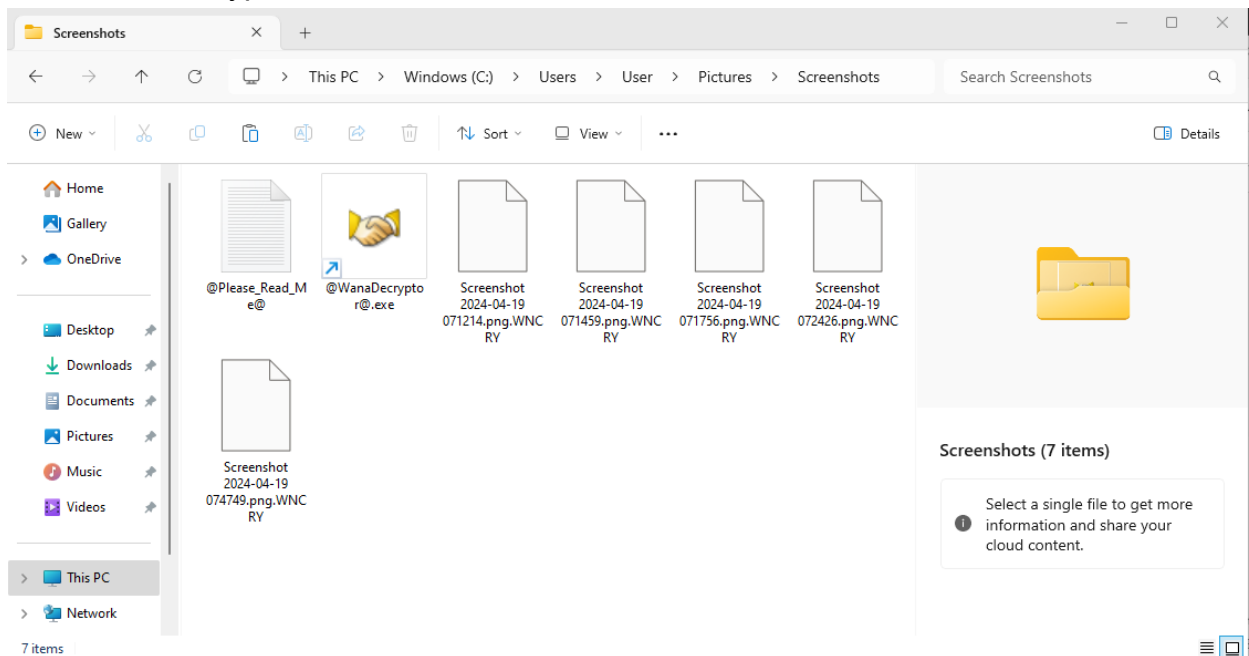
Refresh Options Find handles or DLLs System information Search Processes (Ctrl+K)

Processes Services Network Disk


Name	PID	CPU	I/O total ...	Private b...	User name	Description
> System Idle Process	0	72.28		60 kB	NT AUTHORITY\SYSTEM	
Secure System	76			184 kB		
Registry	116			9.21 MB		
csrss.exe	540			1.85 MB		Client Server Runtime Process
> wininit.exe	640			1.61 MB		Windows Start-Up Application
csrss.exe	660	0.09		2.18 MB		Client Server Runtime Process
> winlogon.exe	740			2.49 MB		Windows Logon Application
> explorer.exe	3996	0.36		132.55 MB	WINDEV2403EVAL\User	Windows Explorer
@WanaDecryptor@.exe	1376			1.85 MB	WINDEV2403EVAL\User	Load PerfMon Counters

CPU Usage: 27.72% Physical memory: 2.98 GB (37.21%) Processes: 151


- Files that are crypted and extension





▼ Today


 @Please\_Read\_Me@


▼ Last week


 chocolatey.2.2.2.nupkg


 PE-bear\_0.6.7.3\_qt4\_x86\_win\_vs10.zip.WNCRY


 die\_win64\_portable\_3.09\_x64.zip.WNCRY


 Ransomware.WannaCry.zip.WNCRY


 PView.zip.WNCRY


 cmdr\_mini.zip.WNCRY

 cmdr.zip.WNCRY


 7z2404-x64

 Wireshark-4.2.4-x64

 idafree84\_windows

 processhacker-2.39-setup

▼ A long time ago

 @WanaDecryptor@

• WannaCry GUY

Wana Decrypt0r 2.0



Payment will be raised on

4/26/2024 04:24:46

Time Left

02:23:51:28

Your files will be lost on

4/30/2024 04:24:46

Time Left

06:23:51:28

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

## Ooops, your files have been encrypted!

English

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 from Monday to Friday.  
Once the payment is checked, you can start decrypting your files immediately.

### Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

 **bitcoin**  
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:

13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Copy

Check Payment

Decrypt

- VirusTotal

<https://www.virustotal.com/gui/file/ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa/behavior>