WannaCry Report

This sample is MALICIOUS.

Type of Report	Static and Sandbox Analysis / Dynamic Analysis
Date	4/3/2024
Analyst/Author	Mitchell Ross Burcheri
Reviewer	Srinivasa Kumar / Pradeep Ponnusamy

Verdict	Description
Malicious	During analysis, the sample in this report has exhibited malicious behaviour. It is confirmed as MALICIOUS

Summary

WannaCry is a ransomware that encrypts the users files and demands ransom of $300 to be paid to the bitcoin wallet address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw in order for the user to decrypt their files. After 6 days the ransom goes up to $600. The files are not deleted after 6 days.

WannaCry has a kill switch at the URL http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com which it checks upon execution. If the URL is found, the ransomware stops running.

The ransomware needs to be run as admin in order for it to begin encrypting the users files. When the files are executed they are given the file extension .WNCRY.

DiskPart is a new startup application that is registered and a fake microsoft security center service is started after WannaCry is successfully executed.

There were 3 bitcoin wallet addresses found and a list of file extensions of files that are encrypted by the ransomware.

Static Analysis

File Metas

Meta Name	Value
File Name:	invoice_greenanimals.pdf.exe
File Size:	3,723,264 bytes
File Type:	executable
MIME type:	application/x-dosexec
OS	windows
Format	pe
Arch	i386
CPU	32-bit
Subsystem	GUI
File Version:	6.1.7601.17514 (win7sp1_rtm.101119-1850)
Description:	Microsoft® Disk Defragmenter
Filename Version:	lhdfrgui.exe
File Signature	Microsoft Visual C++ v6.0
Compilation Language:	English-US
Compiler Stamp:	Sat Nov 20 09:03:08 2010 | UTC
MD5:	db349b97c37d22f5ea1d1841e3c89eb4
SHA1:	e889544aff85ffaf8b0d0da705105dee7c97fe26
SHA256:	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
ssdeep:	98304:wDqPoBhz1aRxcSUDk36SAEdhvxWa9P593R8yAVp2g3R:wDqPe1CxcxK3ZAEUadzR8yc4gB
Imphash:	9ecee117164e0b870a53dd187cdd7174 (74 x WannaCry, 1 x Worm.Virut)
First Bytes Hex:	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
First Bytes Text:	M Z .. .. @ .. ..

Resources file ratio	94.41%
Entry Point:	00009A16
Entropy:	6.13 (Not Packed) [PEiD] 7.964 [pestudio]

Static Analysis Observations

The malware sample creates services, enumerates the machine and uses the import CryptGenRandom which is commonly used in ransomware. The CAPA tool detected anti-behavioral features such as condition execution and runs as a service, anti-static analysis features such as executable code obfuscation for arguments and stack strings. The malware is able to send and receive data from a command and control centre, and installs additional programs.

Pestudio found two indicators of compromise

URL	http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Mutex	Global\MsWinZonesCacheCounterMutex
Bitcoin Wallet Addresses	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

URL

```
000313D0  http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
```

Bitcoin addresses

```
000414E4  115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
00041508  12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
0004152C  13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
```

Mutex

```
00041558  Global\MsWinZonesCacheCounterMutexA
```

Found a list of extensions of files that get encrypted

123, 3dm, 3ds, 7z, accdb, ARC, asf, asm, asp, avi, backup, bak, bat, bmp, class, cmd, cpp, crt, cs, csr, csv, db, dbf, der, dif, doc, docb, docm, docx, dot, dotm, dotx, dwg, eml, fla, flv, frm, gif, gz, hwp, iso, jar, java, jpeg, jpg, js, jsp, key, ldf, m3u, m4u, max, mdb, mdf, mid, mkv, mov, mp3,

mp4, mpeg, mpg, msg, myd, myi, odb, odp, ods, odt, ost, ots, p12, pas, pdf, pem, pfx, php, pl, png, pot, potm, potx, pps, ppsm, ppsx, ppt, pptm, pptx, ps1, psd, pst, rar, raw, rtf, sch, sldm, sldx, slk, sln, sql, stc, std, sti, stw, svg, swf, sxc, sxd, sxi, sxm, sxw, tar, tgz, tif, tiff, txt, vb, vbs, vdi, vmdk, vob, vsd, vsdx, wav, wb2, wk1, wks, wma, wmv, xlc, xlm, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xlw, zip

Strange string saying padding.

```
0038C454
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP
ADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADD
INGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDI
NGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGX
XPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA
DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD
DINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDIN
GXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDING
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP
ADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADD
INGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDI
NGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGX
XPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPA
DDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD
DINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDIN
GXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDING
PADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXPADDINGPADDINGXXP
```

Libraries and Imports

Import/API Key: Flagged (x), Ordinal (o)

Possible Usage definitions from: https://malapi.io/
Associated Attack definitions (https://malapi.io/):

- Evasion: Functions associated with evasive behaviour to evade security controls and solutions.
- Spying: Functions associated with spying on user actions (e.g. keylogger, screen capture).
- Internet: Functions associated with malicious internet connectivity (e.g. C&C, exfiltration, downloads).
- Anti-Debugging: Functions associated with anti-reverse engineering and debugging.
- Ransomware: Cryptographic functions used by ransomware.
- Helper: Functions that are not necessarily malicious, but can aid malware.

Detected with PEstudio

Library	Import/API	Group	Technique	Possible Usage
ADVAPI32.dll	ChangeServiceConfig2A (x)	services	T1569 | System	x

			Services	
	CreateServiceA (x)	services	T1543 | Create or Modify System Process	CreateServiceA is used to create a service object and adds it to the specified service control manager database. This function is commonly used by malware for persistence. Associated Attacks: Helper
	CryptAcquireContextA (x)	crypto | obfuscation	T1027 | Obfuscated Files or Information	CreateServiceA is used to create a service object and adds it to the specified service control manager database. This function is commonly used by malware for persistence. Associated Attacks: Helper
	CryptGenRandom (x)	crypto | obfuscation	T1027 | Obfuscated Files or Information	CryptGenRandom is used to fill a buffer with cryptographically random bytes. Associated Attacks: Ransomware
	StartServiceCtrlDispatcherA (x)	services	-	StartServiceCtrlDispatcherA is used by a service to connect the main thread of the process to the service control manager. Associated Attacks: Helper
	CloseServiceHandle	services	T1569 | System Services	-
	OpenSCManagerA	services	T1569 | System Services	OpenSCManagerA is used to open a handle to the service control manager. This function is commonly used when a malware intends to interact with a service. Associated Attacks: Helper
	OpenServiceA	services	T1543 | Create or Modify System Process	OpenServiceA is used to open an existing service. Associated Attacks: Helper
	RegisterServiceCtrlHandlerA	services	T1106 | Execution through API	-
	SetServiceStatus	services	T1543 | Create or	-

			Modify System Process	
	StartServiceA	services	T1569 | System Services	StartServiceA is used to start a service. Associated Attacks: Helper
iphlpapi.dll	GetAdaptersInfo (x)	network	-	GetAdaptersInfo is used to obtain information about the network adapters on the system. This function is commonly used by malware for enumeration purposes. Associated Attacks: Enumeration
KERNEL32.dll	GetCurrentThread (x)	execution	-	GetCurrentThread is used to retrieve a handle for the calling thread. Associated Attacks: Enumeration
	GetCurrentThreadId (x)	execution	T1057 | Process Discovery	GetCurrentThreadId is used to retrieve the thread identifier of the calling thread. Associated Attacks: Enumeration
	MoveFileExA (x)	file	T1105 | Remote File Copy	MoveFileExA is used to move an existing file or a directory, including its children. Associated Attacks: Helper
	QueryPerformanceFrequency (x)	reconnaissance	-	QueryPerformanceFrequency is used to retrieve the frequency of the performance counter. This function is commonly used by malware for anti-debugging purposes. The malware will measure the time before and after an operation, if the time exceeds taken expected time, the malware will terminate or activate a benign function. Associated Attacks: Anti-Debugging
	CreateFileA	file	-	CreateFileA is used to create a new file or opens an existing file. Associated Attacks: Helper
	FindResourceA	resource	-	FindResourceA is used to find a resource in an executable or loaded DLL. Malware sometimes uses

				resources to store strings, configuration information, or other malicious files. If you see this function used, check for a .rsrc section in the malware's PE header. Associated Attacks: Helper
	GetModuleFileNameA	dynamic-library	-	GetModuleFileNameA is used to return the filename of a module that is loaded in the current process. Malware can use this function to modify or copy files in the currently running process. Associated Attacks: Helper
	GetModuleHandleA	dynamic-library	-	GetModuleHandleW is used to retrieve a module handle for the specified module. The module must have been loaded by the calling process. This function is often used along with GetProcAddress to dynamically retrieve the address of a function for evasion purposes. Associated Attacks: Injection, Evasion
	GetProcAddress	dynamic-library	-	GetProcAddress is used to get the memory address of a function in a DLL. This is often used by malware for obfuscation and evasion purposes to avoid having to call the function directly. Associated Attacks: Injection, Evasion
	GetTickCount	reconnaissance	T1124 | System Time Discovery	GetTickCount is used to retrieve the number of milliseconds since bootup. This function is used by malware for anti-debugging purposes. Associated Attacks: Anti-Debugging
	GlobalAlloc	memory	-	GlobalAlloc is used to allocate the specified number of bytes from the heap. Associated Attacks: Injection
	LoadResource	resource	-	LoadResource is used to load a resource from a PE file into memory. Malware sometimes uses resources to store strings, configuration information, or other malicious files.

				Associated Attacks: Evasion
	LocalAlloc	memory	-	LocalAlloc is used for heap allocation and manipulation. Associated Attacks: Injection
	LockResource	resource	-	LockResource is used with FindResource(), LoadResource() and SizeOfResource() usually to work with embedded executables into the .rsrc section (droppers) Associated Attacks: Evasion, Helper
	QueryPerformanceCounter	reconnaissance	-	QueryPerformanceCounter is used to retrieve the frequency of the performance counter. This function is commonly used by malware for anti-debugging purposes. The malware will measure the time before and after an operation, if the time exceeds the expected time, the malware will terminate or activate a benign function. Associated Attacks: Anti-Debugging
	ReadFile	file	-	ReadFile is used to read data from the specified file or input/output (I/O) device. Associated Attacks: Enumeration
	SizeofResource	resource	-	SizeOfResource checks and retrieves the size of a given resource. Usually found in droppers Associated Attacks: Evasion, Helper
	Sleep	execution	T1497 | Sandbox Evasion	Sleep is used to suspend the execution of the current thread for a set time. This function is commonly used for time-based evasion by adding delays in the code. Associated Attacks: Evasion, Anti-Debugging
	TerminateThread	execution	-	TerminateThread is used to terminate a thread. Associated Attacks: Helper

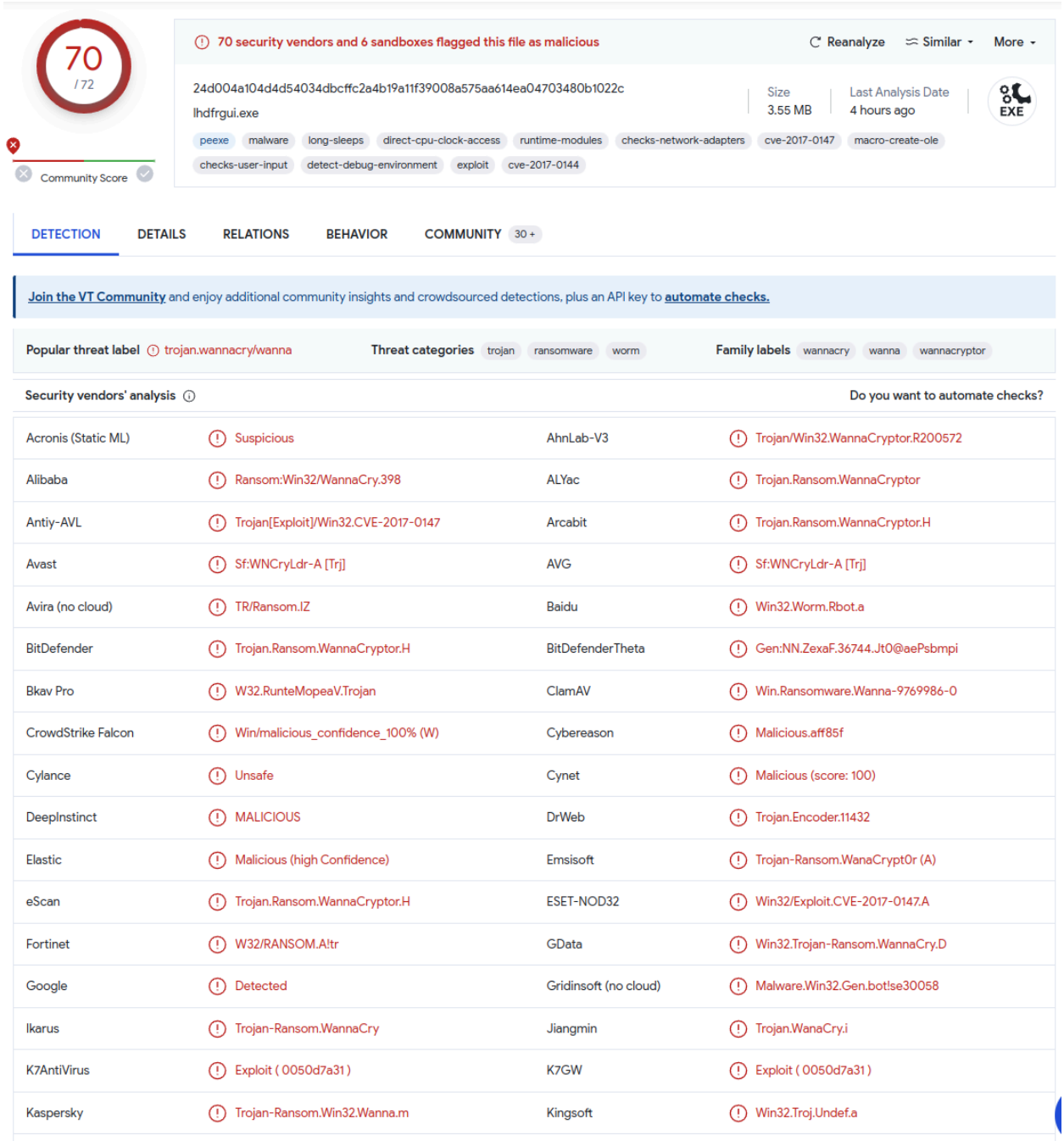
MSVCRT.dll	rand (x)	crypto | obfuscation	T1027 | Obfuscated Files or Information	x
	srand (x)	crypto | obfuscation	T1027 | Obfuscated Files or Information	x
WININET.dll	InternetCloseHandle (x)	network	-	InternetCloseHandle is used to close an internet handle. Associated Attacks: Internet
	InternetOpenA (x)	network	-	InternetOpenA is used to initialize the use of WinINet functions. Associated Attacks: Internet
	InternetOpenUrlA (x)	network	-	InternetOpenUrlA is used to open a resource specified by a complete FTP or HTTP URL. Associated Attacks: Internet
WS2_32.dll	10 (ioctlsocket) (x)(o)	network	-	ioctlsocket takes control of the I/O mode of a socket in any state Associated Attacks: Internet
	11 (inet_addr) (x)(o)	network	-	inet_addr is used to convert a string containing an IPv4 dotted-decimal address into a proper address for the IN_ADDR structure. Associated Attacks: Internet
	115 (WSAStartup) (x)(o)	network	-	WSAStartup is used to initiate use of the Winsock DLL by a process. Associated Attacks: Internet
	16 (recv) (x)(o)	network	-	Recv is used to receive data from a connected socket or a bound connectionless socket. Associated Attacks: Internet
	18 (select) (x)(o)	network	-	Select is used to determine the status of one or more sockets, waiting if necessary, to perform synchronous I/O. This function is used by malware for time-based evasion by setting a large timeout number.

				Associated Attacks: Evasion
	19 (send) (x)(o)	network	-	Send is used to send data on a connected socket. Associated Attacks: Internet
	23 (socket) (x)(o)	network	-	socket is used to create a socket that is bound to a specific transport service provider. Associated Attacks: Internet
	3 (closesocket) (x)(o)	network	-	Closesocket is used to close an existing socket. Associated Attacks: Internet
	4 (connect) (x)(o)	network	-	Connect is used to establish a connection to a specified socket. Associated Attacks: Internet

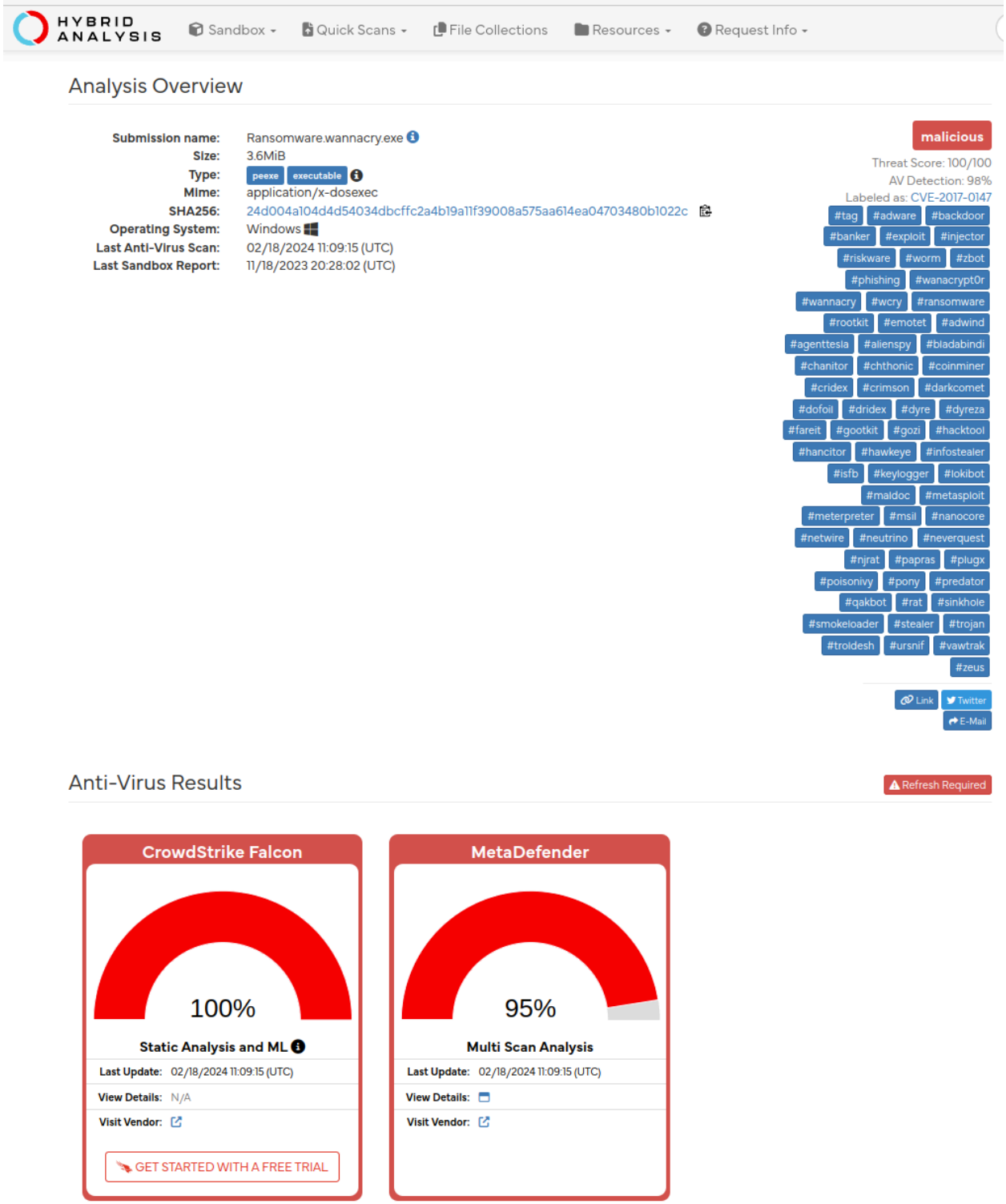
Sandbox Analysis

MalwareBazaar:
https://bazaar.abuse.ch/sample/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c/

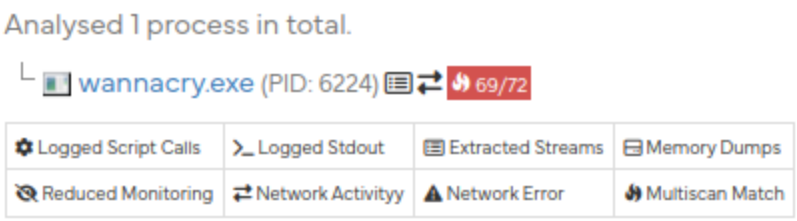
VirusTotal:
https://www.virustotal.com/gui/file/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c



Hybrid Analysis:
https://www.hybrid-analysis.com/sample/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c



Hybrid Analysis (Windows 10):
https://www.hybrid-analysis.com/sample/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c/635b01eb2e98705a9b6d9e64



Contacted Hosts

Login to Download Contacted Hosts (CSV)

IP Address	Port/Protocol	Associated Process	Details
104.16.173.80 OSINT	49732 TCP	wannacry.exe PID: 6224	United States

Memory Forensics

String	Context	Stream UID
http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	Domain/IP reference	00000000-00006224-62189-2-00408140

Dynamic Analysis

Host OS: Linux Mint 21.2. VirtualBox used as the Hypervisor.
Victim Virtual Machine: Flare VM on Windows 10 Home 22H2.
Lab Network Topology: Fake-NG

Dynamic Analysis Observations

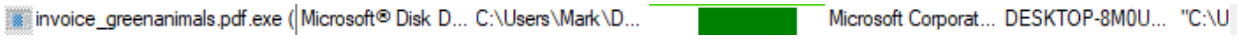
Fake-NG receives the dns query for the URL which activates the kill switch.

```
03/06/24 12:51:02 AM [       DNS Server] Received A request for domain 'www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com'.
```

This is the reverse engineered code in Ghidra of the kill switch. If there is a response from this URL program is closed.

```
int wWinMain(HINSTANCE hInstance,HINSTANCE hPrevInstance,PWSTR pCmdLine,int nCmdShow)

{
  HINTERNET hInternet;
  HINTERNET hInternet_return;
  int i;
  undefined4 *strange_url;
  undefined4 *strange_url_copy;
  undefined4 strange_url_buffer [14];
  undefined4 local_17;
  undefined4 local_13;
  undefined4 local_f;
  undefined4 local_b;
  undefined4 local_7;
  undefined2 local_3;
  undefined local_1;

  strange_url = (undefined4 *)s_http://www.iuqerfsodp9ifjaposdfj_004313d0;
  strange_url_copy = strange_url_buffer;
  for (i = 0xe; i != 0; i = i + -1) {
    *strange_url_copy = *strange_url;
    strange_url = strange_url + 1;
    strange_url_copy = strange_url_copy + 1;
  }
  *(undefined *)strange_url_copy = *(undefined *)strange_url;
  local_17 = 0;
  local_13 = 0;
  local_f = 0;
  local_b = 0;
  local_7 = 0;
  local_3 = 0;
  local_1 = 0;
  InternetOpenA((LPCSTR)0x0,1,(LPCSTR)0x0,(LPCSTR)0x0,0);
  hInternet_return =
       InternetOpenUrlA(hInternet,(LPCSTR)strange_url_buffer,(LPCSTR)0x0,0,0x84000000,0);
                    /* If the url fails, run this. This url is the famous kill switch. */
  if (hInternet_return == (HINTERNET)0x0) {
    InternetCloseHandle(hInternet);
    InternetCloseHandle(0);
    wannacry_real_entry();
    return 0;
  }
  InternetCloseHandle(hInternet);
  InternetCloseHandle(hInternet_return);
  return 0;
}
```

The process terminates soon after with no sub processes.



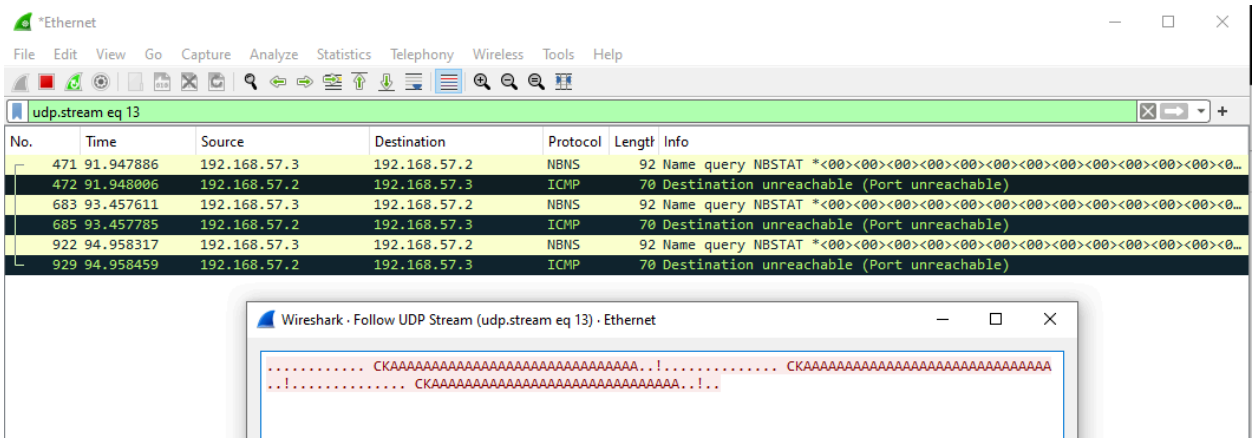
So in this case I could not observe the malicious effects of the malware.

Dynamic Analysis Round 2

Host OS: Linux Mint 21.2. VirtualBox used as the Hypervisor.
Victim Virtual Machine: Flare VM on Windows 10 Home 22H2.
Lab Network Topology: Fake-NG

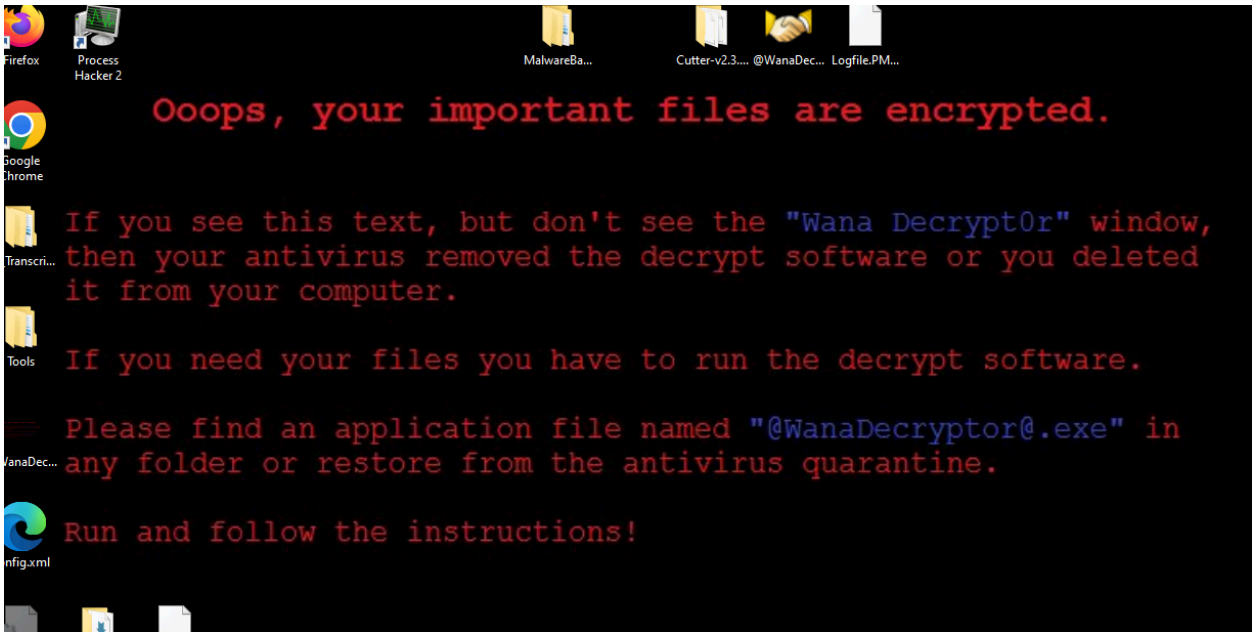
Dynamic Analysis Observations Second Attempt

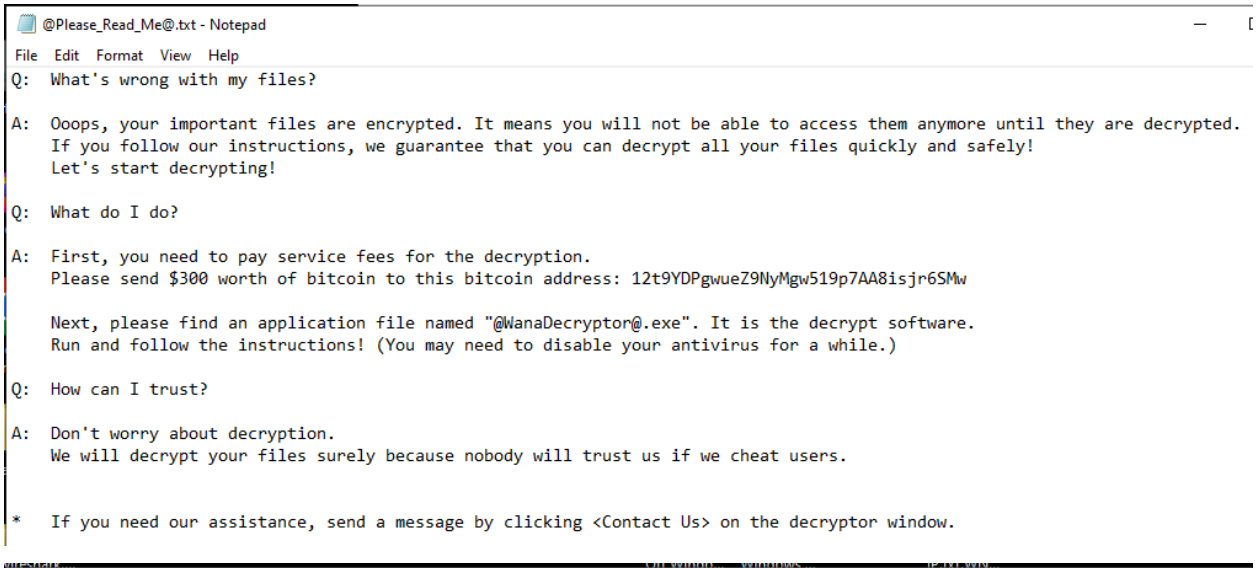
I

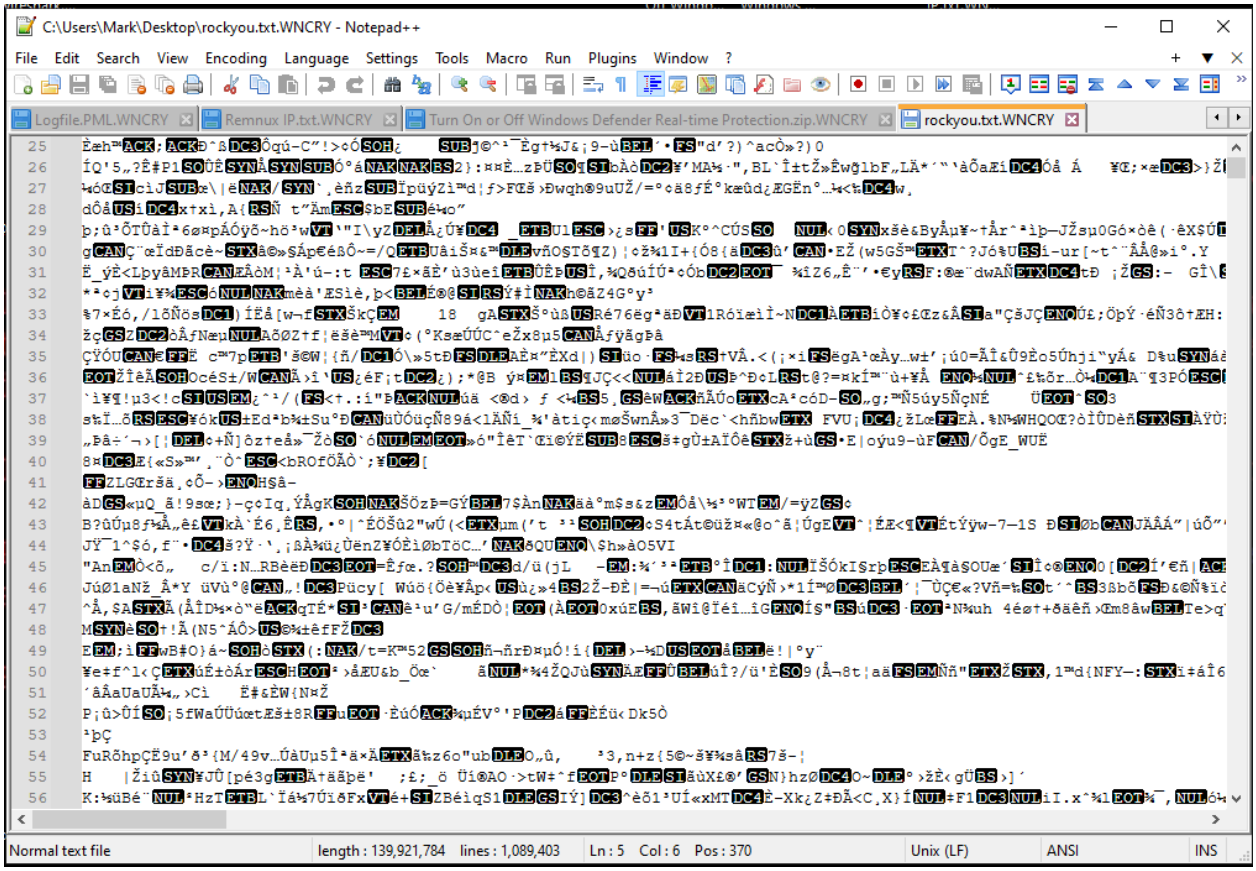


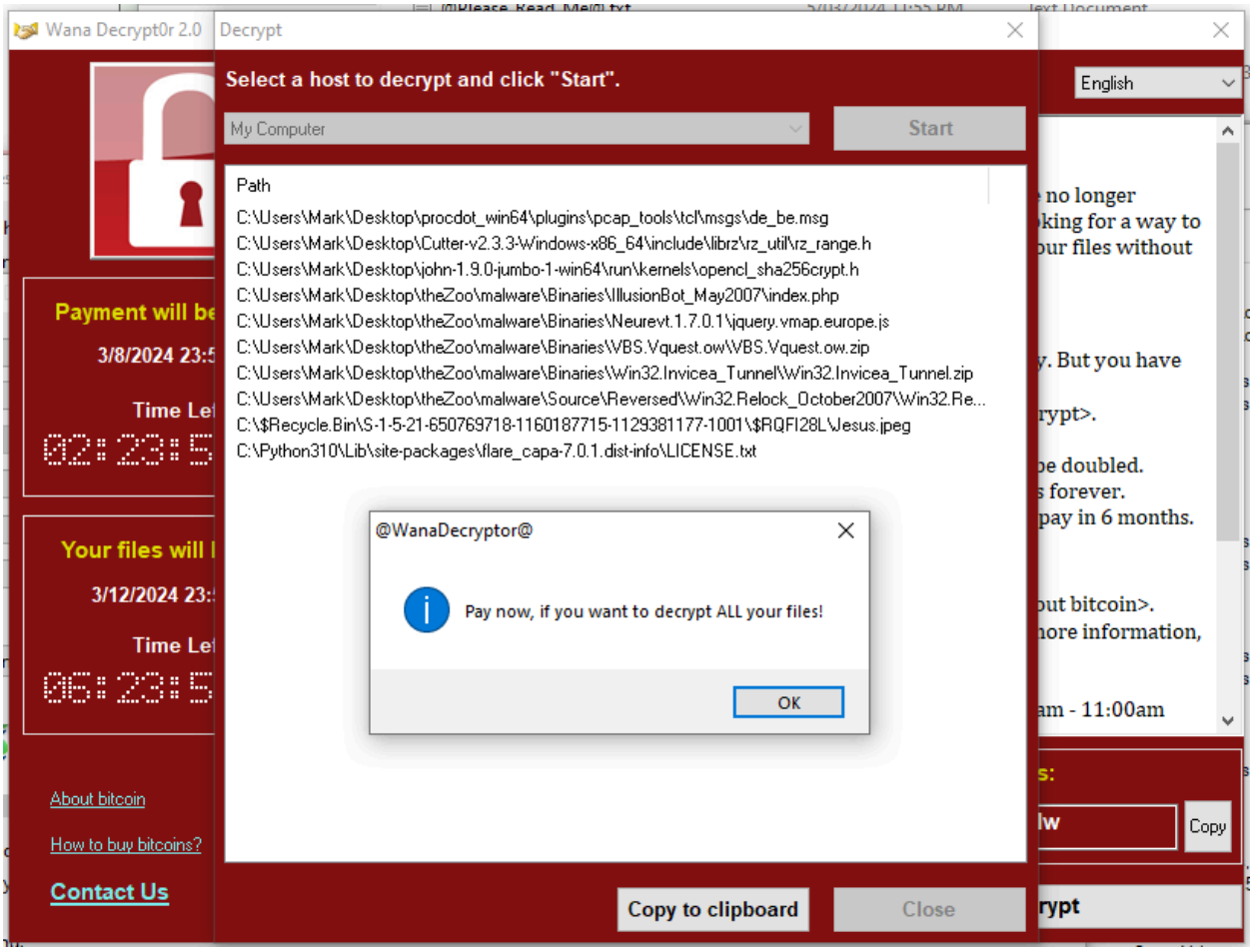
After 6 days the ransom goes up from $300 to $600


Wana Decrypt0r 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
Payment will be raised on
3/9/2024 00:03:08
Time Left
00:00:00:00
Your files will be lost on
3/13/2024 00:03:08
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


Firefox
Process Hacker 2
MalwareBa...
Cutter-v2.3....
@WanaDec...
Logfile.PM...
Google Chrome
Transcri...
Tools
WanaDec...
nfig.xml
Ooops, your important files are encrypted.
If you see this text, but don't see the "Wana Decrypt0r" 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!

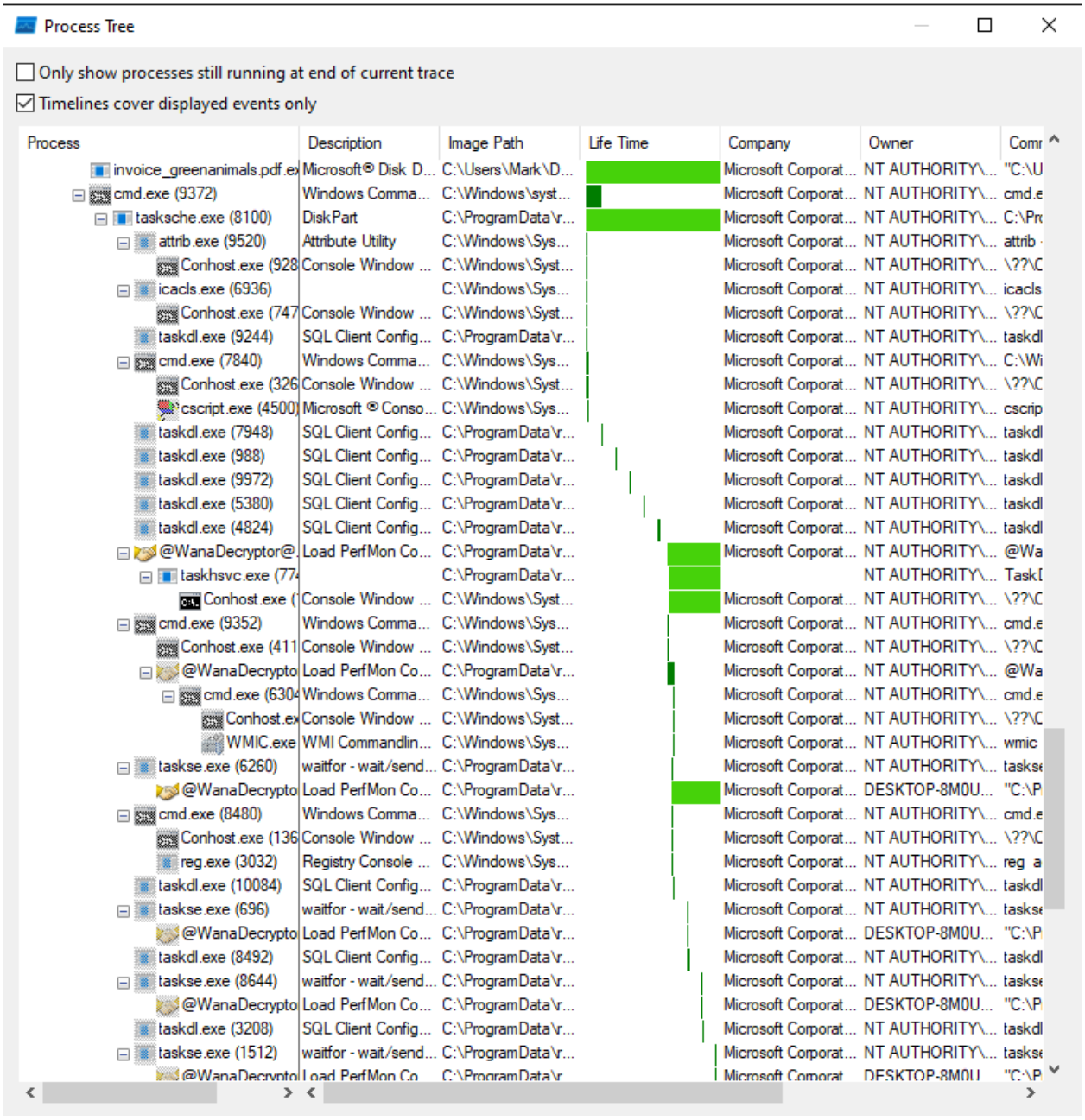

@Please_Read_Me@.txt - Notepad
File Edit Format View Help
Q: What's wrong with my files?
A: Ooops, your important files are encrypted. It means you will not be able to access them anymore until they are decrypted.
If you follow our instructions, we guarantee that you can decrypt all your files quickly and safely!
Let's start decrypting!
Q: What do I do?
A: First, you need to pay service fees for the decryption.
Please send $300 worth of bitcoin to this bitcoin address: 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Next, please find an application file named "@WanaDecryptor@.exe". It is the decrypt software.
Run and follow the instructions! (You may need to disable your antivirus for a while.)
Q: How can I trust?
A: Don't worry about decryption.
We will decrypt your files surely because nobody will trust us if we cheat users.
* If you need our assistance, send a message by clicking <Contact Us> on the decryptor window.


C:\Users\Mark\Desktop\rockyou.txt.WNCRY - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Logfile.PML.WNCRY
Remnux IP.txt.WNCRY
Turn On or Off Windows Defender Real-time Protection.zip.WNCRY
rockyou.txt.WNCRY
Normal text file
length : 139,921,784 lines : 1,089,403
Ln : 5 Col : 6 Pos : 370
Unix (LF)
ANSI
INS



Process Explorer

tasksche.exe	< 0.01	18,172 K	25,952 K	8100 DiskPart	Microsoft Corporation
@WanaDecryptor@.exe		1,704 K	9,672 K	7188 Load PerfMon Counters	Microsoft Corporation
taskhsvc.exe	< 0.01	7,160 K	15,768 K	7744	
conhost.exe		6,244 K	10,988 K	124 Console Window Host	Microsoft Corporation


Process Tree
Only show processes still running at end of current trace
Timelines cover displayed events only
Process
Description
Image Path
Life Time
Company
Owner
Comr
invoice_greenanimals.pdf.ex
Microsoft® Disk D...
C:\Users\Mark\D...
Microsoft Corporat...
NT AUTHORITY\...
"C:\U
cmd.exe (9372)
Windows Comma...
C:\Windows\syst...
Microsoft Corporat...
NT AUTHORITY\...
cmd.e
tasksche.exe (8100)
DiskPart
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
C:\Pr
attrib.exe (9520)
Attribute Utility
C:\Windows\Sys...
Microsoft Corporat...
NT AUTHORITY\...
attrib
Conhost.exe (928
Console Window ...
C:\Windows\Syst...
Microsoft Corporat...
NT AUTHORITY\...
\??\C
icacls.exe (6936)
C:\Windows\Sys...
Microsoft Corporat...
NT AUTHORITY\...
icacls
Conhost.exe (747
Console Window ...
C:\Windows\Syst...
Microsoft Corporat...
NT AUTHORITY\...
\??\C
taskdl.exe (9244)
SQL Client Config...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskdl
cmd.exe (7840)
Windows Comma...
C:\Windows\Sys...
Microsoft Corporat...
NT AUTHORITY\...
C:\Wi
Conhost.exe (326
Console Window ...
C:\Windows\Syst...
Microsoft Corporat...
NT AUTHORITY\...
\??\C
cscript.exe (4500)
Microsoft ® Conso...
C:\Windows\Sys...
Microsoft Corporat...
NT AUTHORITY\...
cscrip
taskdl.exe (7948)
SQL Client Config...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskdl
taskdl.exe (988)
SQL Client Config...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskdl
taskdl.exe (9972)
SQL Client Config...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskdl
taskdl.exe (5380)
SQL Client Config...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskdl
taskdl.exe (4824)
SQL Client Config...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskdl
@WanaDecryptor@.
Load PerfMon Co...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
@Wa
taskhsvc.exe (774
C:\ProgramData\r...
NT AUTHORITY\...
Task
Conhost.exe (
Console Window ...
C:\Windows\Syst...
Microsoft Corporat...
NT AUTHORITY\...
\??\C
cmd.exe (9352)
Windows Comma...
C:\Windows\Sys...
Microsoft Corporat...
NT AUTHORITY\...
cmd.e
Conhost.exe (411
Console Window ...
C:\Windows\Syst...
Microsoft Corporat...
NT AUTHORITY\...
\??\C
@WanaDecrypto
Load PerfMon Co...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
@Wa
cmd.exe (6304
Windows Comma...
C:\Windows\Sys...
Microsoft Corporat...
NT AUTHORITY\...
cmd.e
Conhost.ex
Console Window ...
C:\Windows\Syst...
Microsoft Corporat...
NT AUTHORITY\...
\??\C
WMIC.exe
WMI Commandlin...
C:\Windows\Sys...
Microsoft Corporat...
NT AUTHORITY\...
wmic
taskse.exe (6260)
waitfor - wait/send...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskse
@WanaDecrypto
Load PerfMon Co...
C:\ProgramData\r...
Microsoft Corporat...
DESKTOP-8M0U...
"C:\P
cmd.exe (8480)
Windows Comma...
C:\Windows\Sys...
Microsoft Corporat...
NT AUTHORITY\...
cmd.e
Conhost.exe (136
Console Window ...
C:\Windows\Syst...
Microsoft Corporat...
NT AUTHORITY\...
\??\C
reg.exe (3032)
Registry Console ...
C:\Windows\Sys...
Microsoft Corporat...
NT AUTHORITY\...
reg a
taskdl.exe (10084)
SQL Client Config...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskdl
taskse.exe (696)
waitfor - wait/send...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskse
@WanaDecrypto
Load PerfMon Co...
C:\ProgramData\r...
Microsoft Corporat...
DESKTOP-8M0U...
"C:\P
taskdl.exe (8492)
SQL Client Config...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskdl
taskse.exe (8644)
waitfor - wait/send...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskse
@WanaDecrypto
Load PerfMon Co...
C:\ProgramData\r...
Microsoft Corporat...
DESKTOP-8M0U...
"C:\P
taskdl.exe (3208)
SQL Client Config...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskdl
taskse.exe (1512)
waitfor - wait/send...
C:\ProgramData\r...
Microsoft Corporat...
NT AUTHORITY\...
taskse

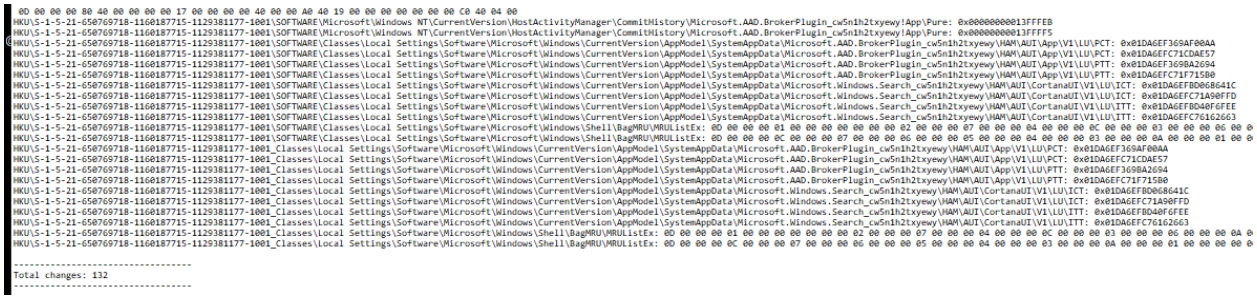
~res-x64.txt - Notepad

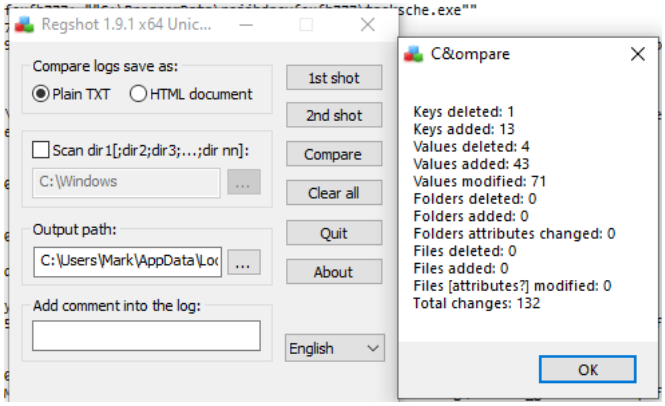
File Edit Format View Help

```
Regshot 1.9.1 x64 Unicode (beta r321)
Comments:
Datetime: 2024-03-05 12:52:39, 2024-03-05 12:56:33
Computer: DESKTOP-8M0UP0B, DESKTOP-8M0UP0B
Username: Mark, Mark

----------------------------------
Keys deleted: 1
----------------------------------
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData

----------------------------------
Keys added: 13
----------------------------------
HKLM\SOFTWARE\Microsoft\RADAR\HeapLeakDetection\DiagnosedApplications\Regshot-x64-Unicode.exe
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\9432
HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0
HKLM\SYSTEM\ControlSet001\Services\rojjbdpcyfeufb777
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0
HKLM\SYSTEM\CurrentControlSet\Services\rojjbdpcyfeufb777
HKU\.DEFAULT\Software\Microsoft\Windows Script Host
HKU\.DEFAULT\Software\Microsoft\Windows Script Host\Settings
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000002
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000002
HKU\S-1-5-18\Software\Microsoft\Windows Script Host
HKU\S-1-5-18\Software\Microsoft\Windows Script Host\Settings

----------------------------------
Values deleted: 4
----------------------------------
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\windows.immersivecontrolpanel_cw5n1h2txyewy!
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\Microsoft.Windows.ControlPanel: 0x01DA6EFB6F
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notep
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy!
```

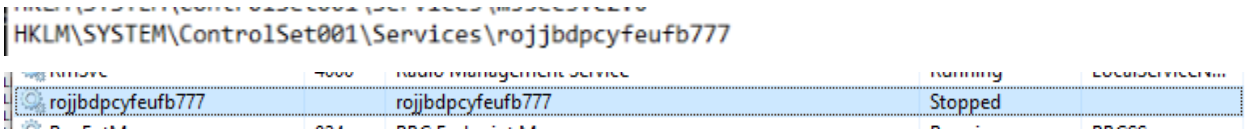
```
----------------------------------
Values added: 43
----------------------------------
HKLM\SOFTWARE\Microsoft\RADAR\HeapLeakDetection\DiagnosedApplications\Regshot-x64-Unicode.exe\LastDetectionTime: 0x01DA6EFC8A01DD73
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\9432\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\9432\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\9432\CreationTime: 0x01DA6EFC71F49DD0
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\rojjbdpcyfeufb777: ""C:\ProgramData\rojjbdpcyfeufb777\tasksche.exe""
HKLM\SOFTWARE\WOW6432Node\WanaCrypt0r\wd: "C:\ProgramData\rojjbdpcyfeufb777"
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-650769718-1160187715-1129381177-1001\\Device\HarddiskVolume2\ProgramData\rojjbdpcyfeufb777\@WanaDecryptor@.exe: BB E8 72 89 FC 6E DA 01 00
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\Type: 0x00000010
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\ImagePath: "C:\Users\Mark\Desktop\MalwareBazaar\WannaCry - Reverse Engineering\invoice_greenanimals.pdf.exe -m security"
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\DisplayName: "Microsoft Security Center (2.0) Service"
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\WOW64: 0x0000014C
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\mssecsvc2.0\FailureActions: 00 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 14 00 00 00 01 00 00 00 60 EA 00 00
HKLM\SYSTEM\ControlSet001\Services\rojjbdpcyfeufb777\Type: 0x00000010
HKLM\SYSTEM\ControlSet001\Services\rojjbdpcyfeufb777\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\rojjbdpcyfeufb777\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\rojjbdpcyfeufb777\ImagePath: "cmd.exe /c "C:\ProgramData\rojjbdpcyfeufb777\tasksche.exe""
HKLM\SYSTEM\ControlSet001\Services\rojjbdpcyfeufb777\DisplayName: "rojjbdpcyfeufb777"
HKLM\SYSTEM\ControlSet001\Services\rojjbdpcyfeufb777\WOW64: 0x0000014C
HKLM\SYSTEM\ControlSet001\Services\rojjbdpcyfeufb777\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-650769718-1160187715-1129381177-1001\\Device\HarddiskVolume2\ProgramData\rojjbdpcyfeufb777\@WanaDecryptor@.exe: 74 81 48 9B FC 6E DA 01
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\Type: 0x00000010
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\ImagePath: "C:\Users\Mark\Desktop\MalwareBazaar\WannaCry - Reverse Engineering\invoice_greenanimals.pdf.exe -m security"
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\DisplayName: "Microsoft Security Center (2.0) Service"
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\WOW64: 0x0000014C
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\ObjectName: "LocalSystem"
HKLM\SYSTEM\CurrentControlSet\Services\mssecsvc2.0\FailureActions: 00 00 00 00 01 00 00 00 01 00 00 00 01 00 00 00 14 00 00 00 01 00 00 00 60 EA 00 00
HKLM\SYSTEM\CurrentControlSet\Services\rojjbdpcyfeufb777\Type: 0x00000010
HKLM\SYSTEM\CurrentControlSet\Services\rojjbdpcyfeufb777\Start: 0x00000002
HKLM\SYSTEM\CurrentControlSet\Services\rojjbdpcyfeufb777\ErrorControl: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\rojjbdpcyfeufb777\ImagePath: "cmd.exe /c "C:\ProgramData\rojjbdpcyfeufb777\tasksche.exe""
HKLM\SYSTEM\CurrentControlSet\Services\rojjbdpcyfeufb777\DisplayName: "rojjbdpcyfeufb777"
HKLM\SYSTEM\CurrentControlSet\Services\rojjbdpcyfeufb777\WOW64: 0x0000014C
HKLM\SYSTEM\CurrentControlSet\Services\rojjbdpcyfeufb777\ObjectName: "LocalSystem"
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Znex\Qrfxgbc\ZnyjnerOmmne\JnaanPel - Er
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000002503SE\VirtualDesktop: 10 00 00 00 30 30 44 56 85 E
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000002B02B2\VirtualDesktop: 10 00 00 00 30 30 44 56 85 E
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\Flighting\CachedFeatureString: ""
HKU\S-1-5-21-650769718-1160187715-1129381177-1001\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store\C:\Users\Mark\Desktop\MalwareBazaar\WannaCry - Reverse Engineering

----------------------------------
```

```
CE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Znex\Qrfxgbc\ZnyjnerOmmne\JnaanPel - Erirefr Ratvarrevat\vaibvpr_terranavznyf.cqs.rkr: 00
ionViewManagement\W32:00000000002503SE\VirtualDesktop: 10 00 00 00 30 30 44 56 85 E8 04 A2 D4 2F 21 46 9D 44 A0 BC 7B 57 7D E8
ionViewManagement\W32:00000000002B02B2\VirtualDesktop: 10 00 00 00 30 30 44 56 85 E8 04 A2 D4 2F 21 46 9D 44 A0 BC 7B 57 7D E8
tring: ""
Assistant\Store\C:\Users\Mark\Desktop\MalwareBazaar\WannaCry - Reverse Engineering\invoice_greenanimals.pdf.exe: 53 41 43 50 01 00 00
```

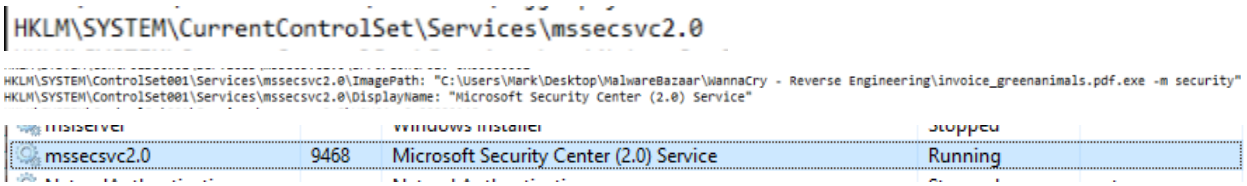




In task manager I wanted to look up the services that I saw registries were being created for.



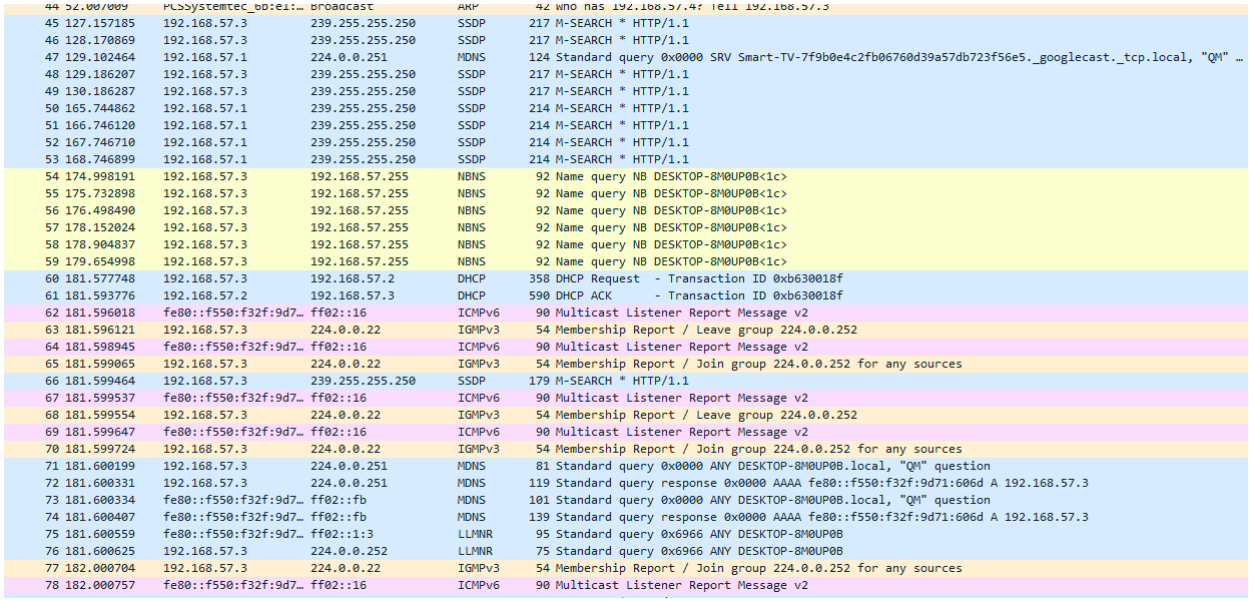
I found a fake microsoft security center service.



Disk part runs on startup.

Name	Publisher	Status	Startup impact
DiskPart	Microsoft Corporation	Enabled	Not measured
Microsoft Edge	Microsoft Corporation	Enabled	Not measured
Sysinternals Screen Magnifier	Sysinternals - www.sysin...	Enabled	Not measured
Windows Security notification icon	Microsoft Corporation	Enabled	Low

I discovered when I stopped mssecsvc2.0 and disabled diskpart



44 52.007009	PCSystemtec_bb:e1:…	Broadcast	ARP	42	Who has 192.168.57.4? Tell 192.168.57.3
45 127.157185	192.168.57.3	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
46 128.170869	192.168.57.3	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
47 129.102464	192.168.57.1	224.0.0.251	MDNS	124	Standard query 0x0000 SRV Smart-TV-7f9b0e4c2fb06760d39a57db723f56e5._googlecast._tcp.local, "QM" …
48 129.186207	192.168.57.3	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
49 130.186287	192.168.57.3	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
50 165.744862	192.168.57.1	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
51 166.746120	192.168.57.1	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
52 167.746710	192.168.57.1	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
53 168.746899	192.168.57.1	239.255.255.250	SSDP	214	M-SEARCH * HTTP/1.1
54 174.998191	192.168.57.3	192.168.57.255	NBNS	92	Name query NB DESKTOP-8M0UP0B<1c>
55 175.732898	192.168.57.3	192.168.57.255	NBNS	92	Name query NB DESKTOP-8M0UP0B<1c>
56 176.498490	192.168.57.3	192.168.57.255	NBNS	92	Name query NB DESKTOP-8M0UP0B<1c>
57 178.152024	192.168.57.3	192.168.57.255	NBNS	92	Name query NB DESKTOP-8M0UP0B<1c>
58 178.904837	192.168.57.3	192.168.57.255	NBNS	92	Name query NB DESKTOP-8M0UP0B<1c>
59 179.654998	192.168.57.3	192.168.57.255	NBNS	92	Name query NB DESKTOP-8M0UP0B<1c>
60 181.577748	192.168.57.3	192.168.57.2	DHCP	358	DHCP Request - Transaction ID 0xb630018f
61 181.593776	192.168.57.2	192.168.57.3	DHCP	590	DHCP ACK - Transaction ID 0xb630018f
62 181.596018	fe80::f550:f32f:9d7…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
63 181.596121	192.168.57.3	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
64 181.598945	fe80::f550:f32f:9d7…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
65 181.599065	192.168.57.3	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
66 181.599464	192.168.57.3	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
67 181.599537	fe80::f550:f32f:9d7…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
68 181.599554	192.168.57.3	224.0.0.22	IGMPv3	54	Membership Report / Leave group 224.0.0.252
69 181.599647	fe80::f550:f32f:9d7…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
70 181.599724	192.168.57.3	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
71 181.600199	192.168.57.3	224.0.0.251	MDNS	81	Standard query 0x0000 ANY DESKTOP-8M0UP0B.local, "QM" question
72 181.600331	192.168.57.3	224.0.0.251	MDNS	119	Standard query response 0x0000 AAAA fe80::f550:f32f:9d71:606d A 192.168.57.3
73 181.600334	fe80::f550:f32f:9d7…	ff02::fb	MDNS	101	Standard query 0x0000 ANY DESKTOP-8M0UP0B.local, "QM" question
74 181.600407	fe80::f550:f32f:9d7…	ff02::fb	MDNS	139	Standard query response 0x0000 AAAA fe80::f550:f32f:9d71:606d A 192.168.57.3
75 181.600559	fe80::f550:f32f:9d7…	ff02::1:3	LLMNR	95	Standard query 0x6966 ANY DESKTOP-8M0UP0B
76 181.600625	192.168.57.3	224.0.0.252	LLMNR	75	Standard query 0x6966 ANY DESKTOP-8M0UP0B
77 182.000704	192.168.57.3	224.0.0.22	IGMPv3	54	Membership Report / Join group 224.0.0.252 for any sources
78 182.000757	fe80::f550:f32f:9d7…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2

MITRE ATT&CK Mapping

Detected with CAPA

Tactic	ID	Technique	Procedure
Execution	T1129	Shared Modules	
	T1569.002	System Services::Service Execution	WannaCry may abuse the Windows service control manager to execute malicious commands or payloads with **ChangeServiceConfig2A**, **CloseServiceHandle**, **OpenSCManagerA**, and **StartServiceA**.
Persistence	T1543	Create or Modify System Process::Windows Service	WannaCry may create or modify Windows services to repeatedly execute malicious payloads as part of persistence with **CreateServiceA**, **OpenServiceA**, and **SetServiceStatus**.
Defence Evasion	T1027	Obfuscated Files or Information	WannaCry may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit with **CryptAcquireContextA**, **CryptGenRandom**, **rand**, and **srand**.
	T1497	Virtualization/Sandbox Evasion	WannaCry may employ various means to detect and avoid virtualization and analysis environments with **Sleep**.

Discovery	T1083	File and Directory Discovery	
	T1082	System Information Discovery	
	T1016	System Network Configuration Discovery	WannaCry may look for details about the network configuration and settings, such as IP and/or MAC addresses, of systems they access or through information discovery of remote systems with **RegisterServiceCtrlHandlerA**.
	T1057	Process Discovery	WannaCry may attempt to get information about running processes on a system with **GetCurrentThreadId**.
	T1124	System Time Discovery	WannaCry may gather the system time and/or time zone from a local or remote system with **GetTickCount**.
Command and Control	T1105	Ingress Tool Transfer	WannaCry may transfer tools or other files from an external system into a compromised environment with **MoveFileExA**.

Annexures

YARA Rules

```
rule DETECTED_WannaCry_File
{
   meta:
      description = "DETECTED WannaCry File"
      author = "MB"
      date = "2024-02-27"
      /* Detects the mz file header, pk file file header and the libraries flagged by pestudio*/

   strings:
      $mz = {4D 5A}
      $q = "CreateServiceA"
      $w = "RegCreateKeyW"
      $e = "RegSetValueExA"
      $r = "VirtualAlloc"
      $t = "VirtualProtect"
      $y = "WriteFile"
      $u = "SetFileAttributesW"
```

```
        $i = "CreateProcessA"
        $o = "TerminateProcess"
        $p = "GetExitCodeProcess"
        $a = "CryptReleaseContext"
        $s = "rand"
        $d = "srand"
        $f = "SetCurrentDirectoryW"
        $g = "SetCurrentDirectoryA"
        $PK_hex = {50 4B 03 04 14 00 01 00 08 00 AA A1 AB 4A FE 21 6D 67 54 37}

    condition:
        $mz at 0
        and all of them
}
```

```
C:\Users\Mark\Desktop\theZoo\malware\Binaries\Ransomware.WannaCry>yara -r C:\Users\Mark\Desktop\theZoo\malware\Binaries\
Ransomware.WannaCry\yara_rule.yara C:\Users\Mark\Desktop\
DETECTED_WannaCry_Ransomware_File C:\Users\Mark\Desktop\\MalwareBazaar\WannaCry - Reverse Engineering\invoice_greenanima
ls.pdf.exe
DETECTED_WannaCry_Ransomware_File C:\Users\Mark\Desktop\\MalwareBazaar\WannaCry - Reverse Engineering\R.dump
DETECTED_WannaCry_Ransomware_File C:\Users\Mark\Desktop\\theZoo\malware\Binaries\Ransomware.WannaCry\ed01ebfbc9eb5bbea54
5af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe
DETECTED_WannaCry_Ransomware_File C:\Users\Mark\Desktop\\theZoo\malware\Binaries\Ransomware.WannaCry_Plus\Win32.Wannacry
.exe
```

IOCs

URL	http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
Mutex	Global\MsWinZonesCacheCounterMutex
Bitcoin Wallet Addresses	115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw 13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94