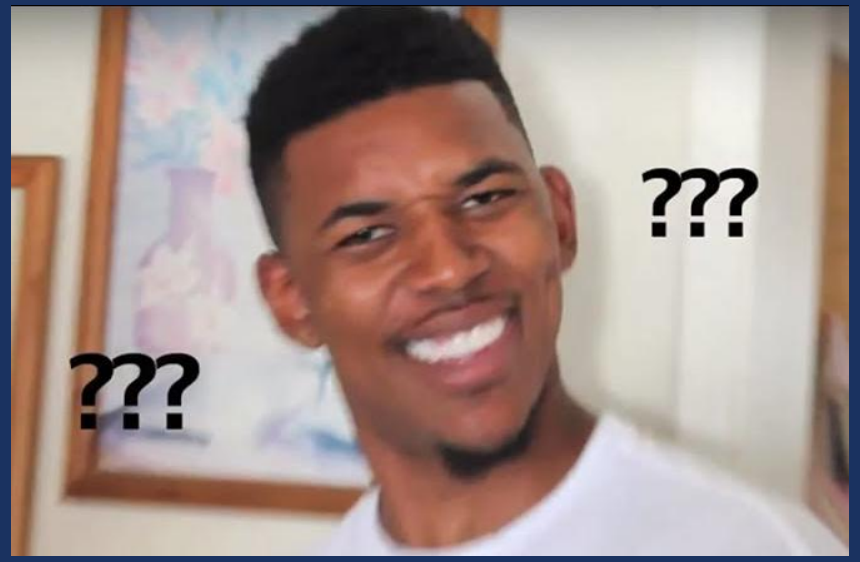
MALWARE REVERSE ENGINEERING

WANNACRY

WHAT IS IT?




95′
79′
POOL CONCEPT ONLY
COVERED PATIO
OUTDOOR LIVING
13' x 18'
MSTR SUITE
15' x 16'
12' CLG
1 CAR GARAGE
12' x 24'
GAME
15' x 16'
11' CLG
BRKFST
11' x 14'
11' CLG
BDRM 3
11' x 13'
11' CLG
WIC
B2
B3
FAMILY
17' x 19'
12' CLG
MSTR BATH
BDRM 2
11' x 11'
11' CLG
WIC
REF
ICE
DW
TO
15' x 16'
OV
WD
WIC
WARDROBE
UTIL.
BDRM 4
11' x 12'
11' CLG
B4
MEDIA
13' x 14'
11' CLG
PORCH
COVERED PATIO
2 CAR GARAGE
24' x 24'

BUT WHY?

- Understanding the adversary
- Spotting indicators of compromise (IOCs)
- Responding to an incident
- Understanding intangible warfare

MALWARE ANALYSIS

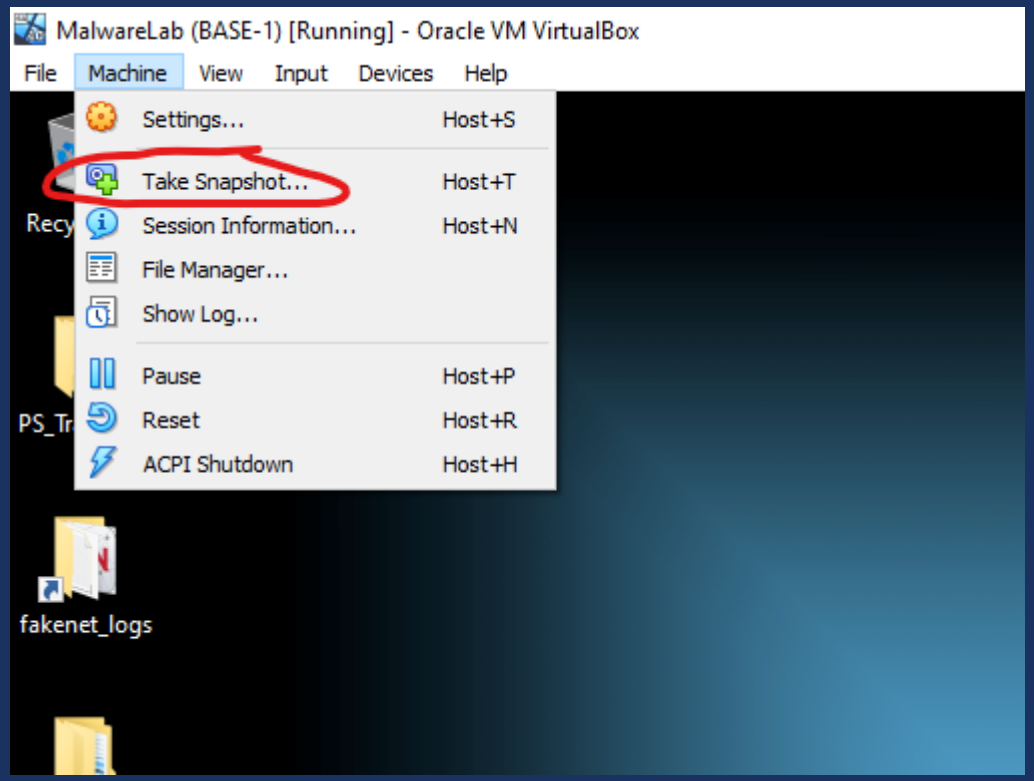
- **Basic Static Analysis** - Limited tools and looking at the sample when it is not running.

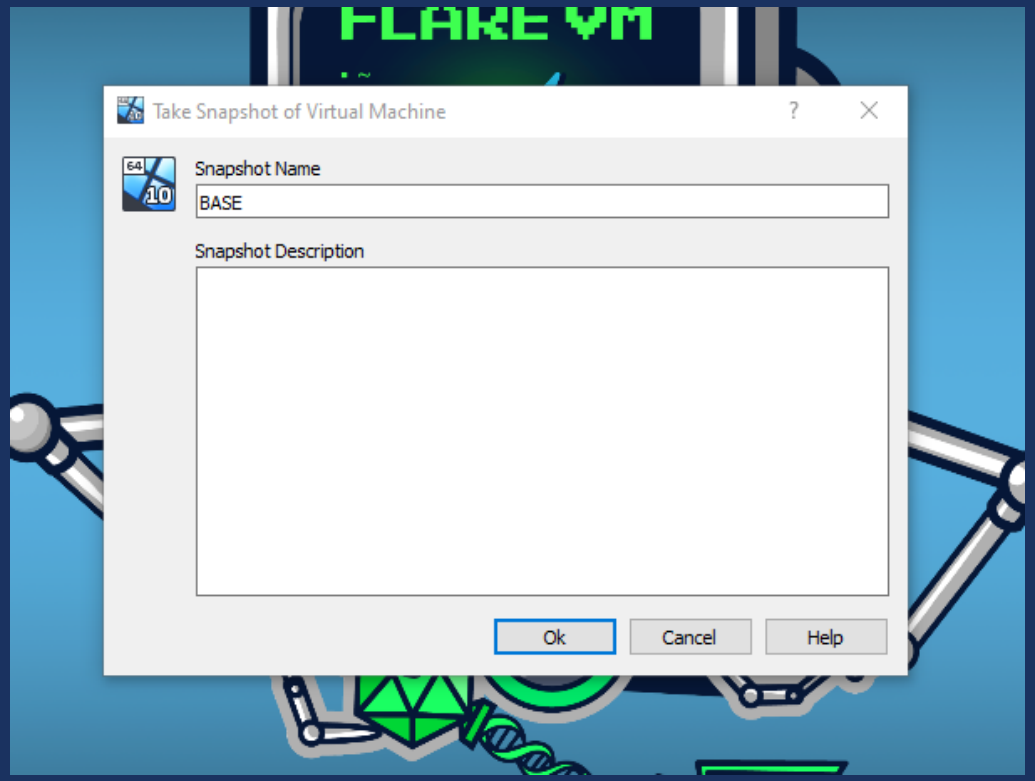
- **Basic Dynamic Analysis** - Executing the sample and collect basic information.

WHAT DO I NEED?

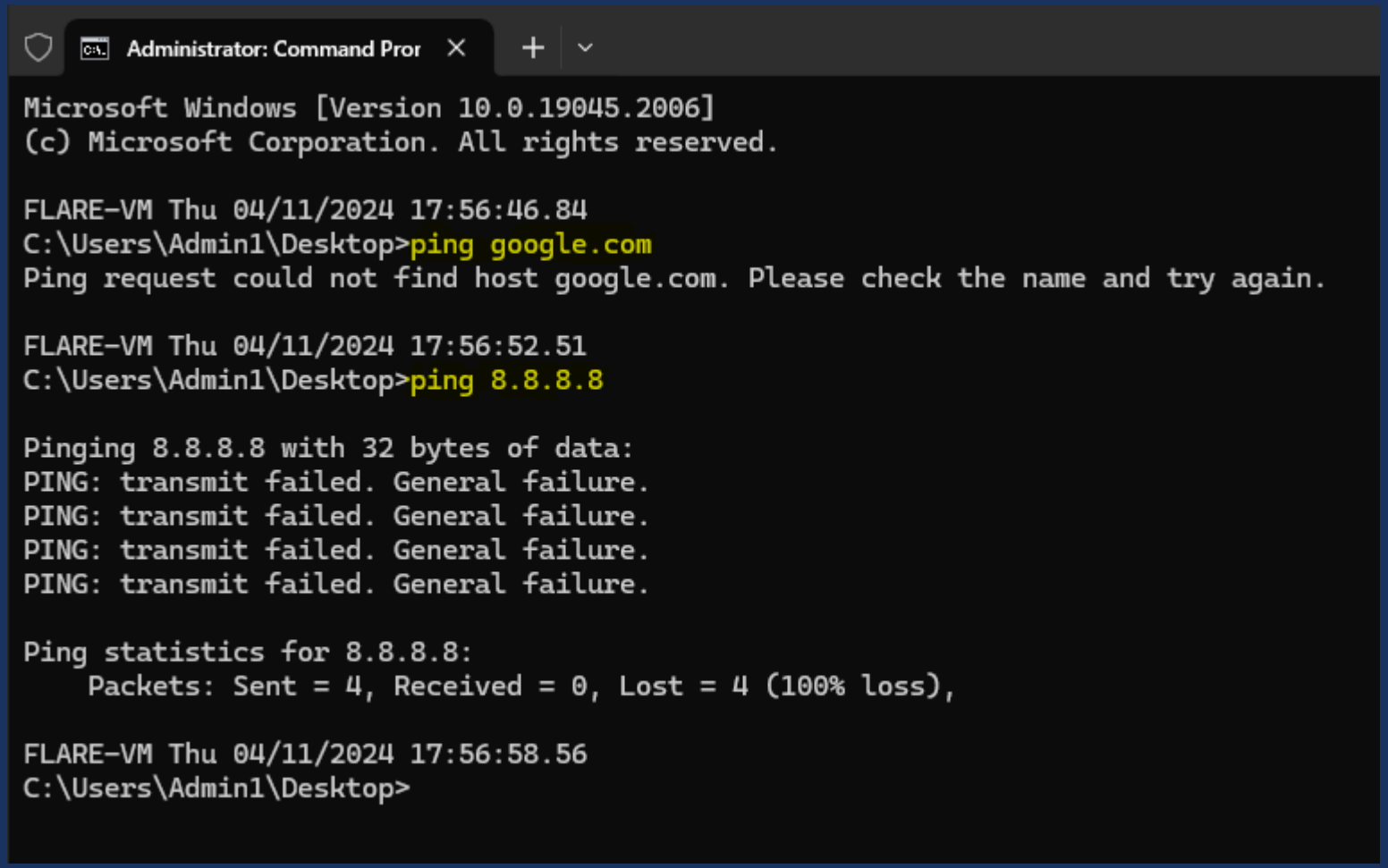
- FlareVM – Specialized Windows Reverse Engineering VM
- REMnux - Specialized Linux Reverse Engineering VM
- MITRE ATT&CK – A framework to show how cyber attacks happen
- Windows API – The different functions that make Windows Work

MALWARE SAFETY





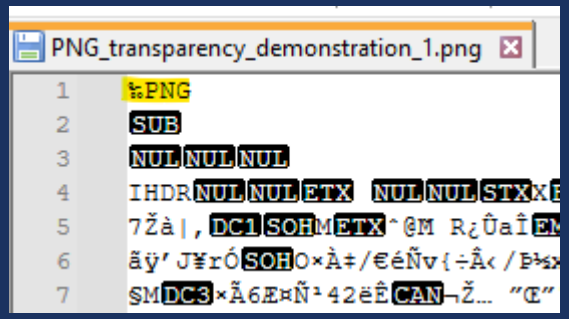
MALWARE SAFETY

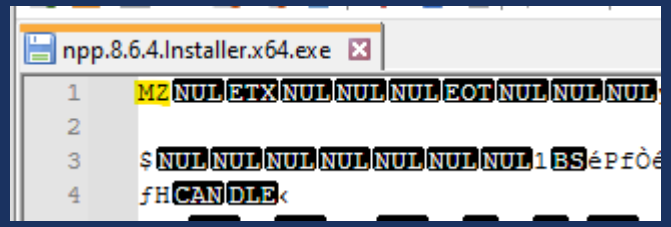


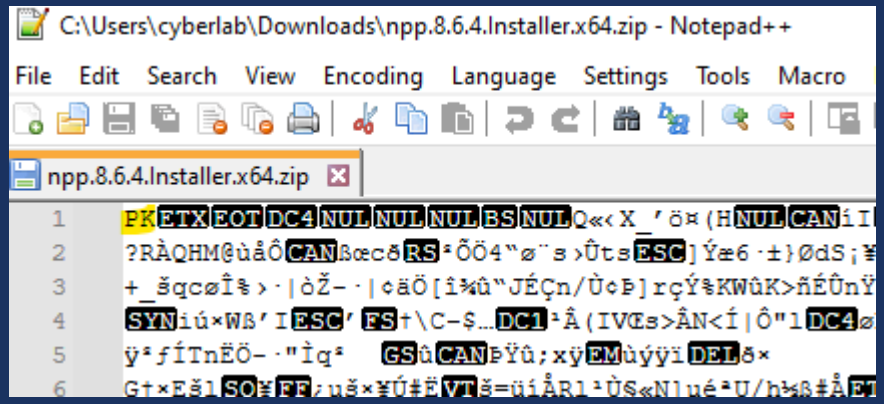

TIME TO START!


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
4/15/2024 12:33:43
Time Left
02:23:54:37
Your files will be lost on
4/19/2024 12:33:43
Time Left
06:23:54:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment
Decrypt

FILE HEADERS







FLOSS

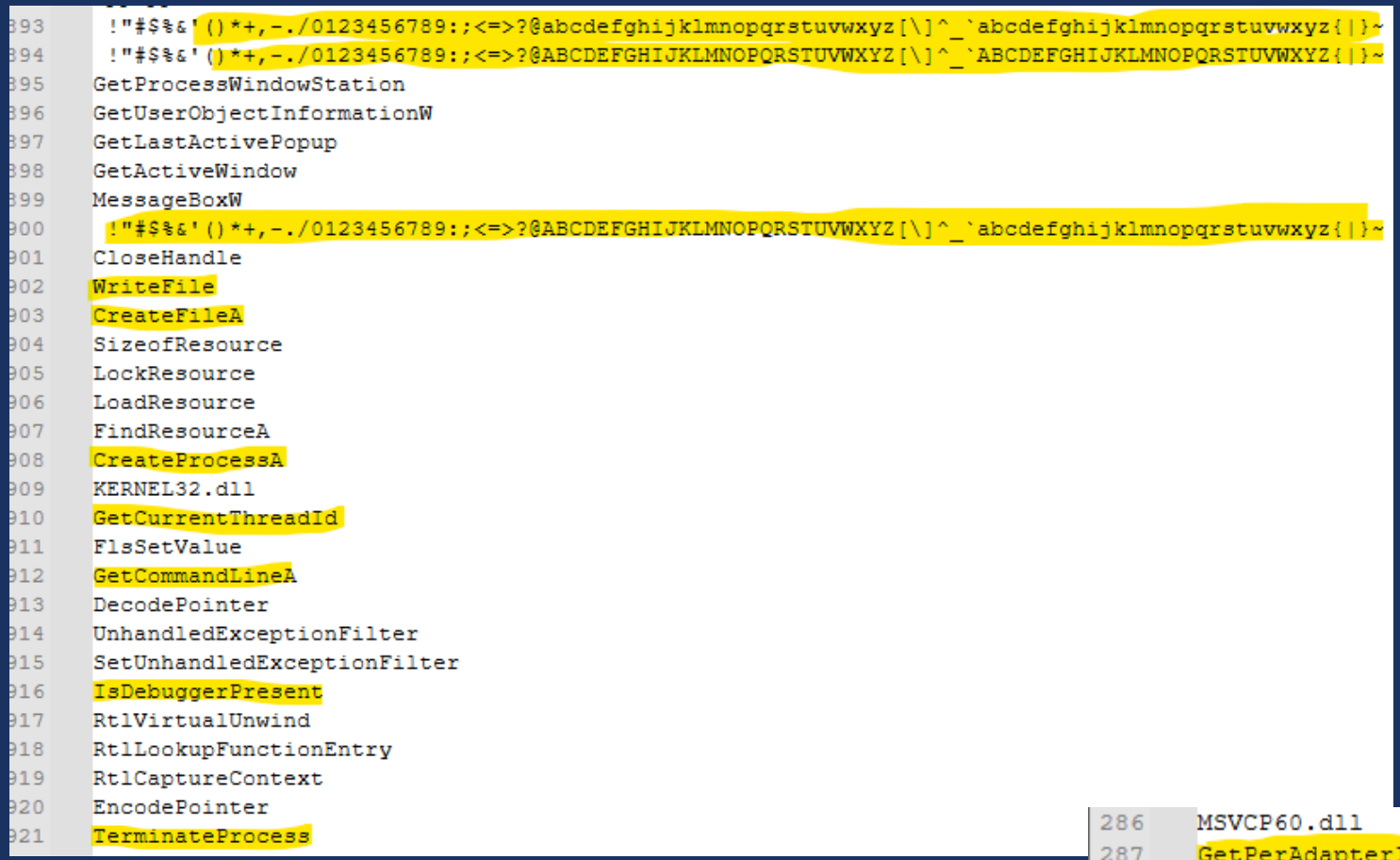
```
24
25  !This program cannot be run in DOS mode.
26  t4;1u#SV
27  GetTickCount
28  QueryPerformanceCounter
29  QueryPerformanceFrequency
```

```
164 Wednesday
165  !"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
166  !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~
167 GetProcessWindowStation
168 GetUserObjectInformationW
169 GetLastActivePopup
170 GetActiveWindow
171 MessageBoxW
172  !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
173 CloseHandle
```

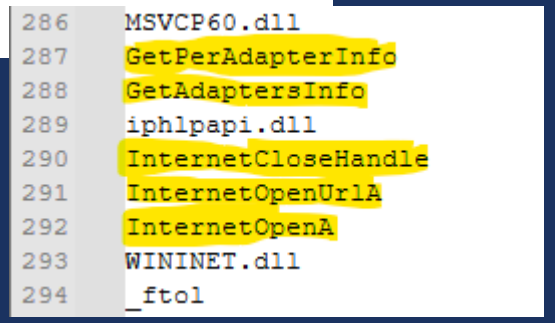
FLOSS

```
398    WriteFile
399    CreateFileA
400    CreateProcessA
401    http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
402    !This program cannot be run in DOS mode.
403    =j&&LZ66lA??~
404    f""D~**T
```

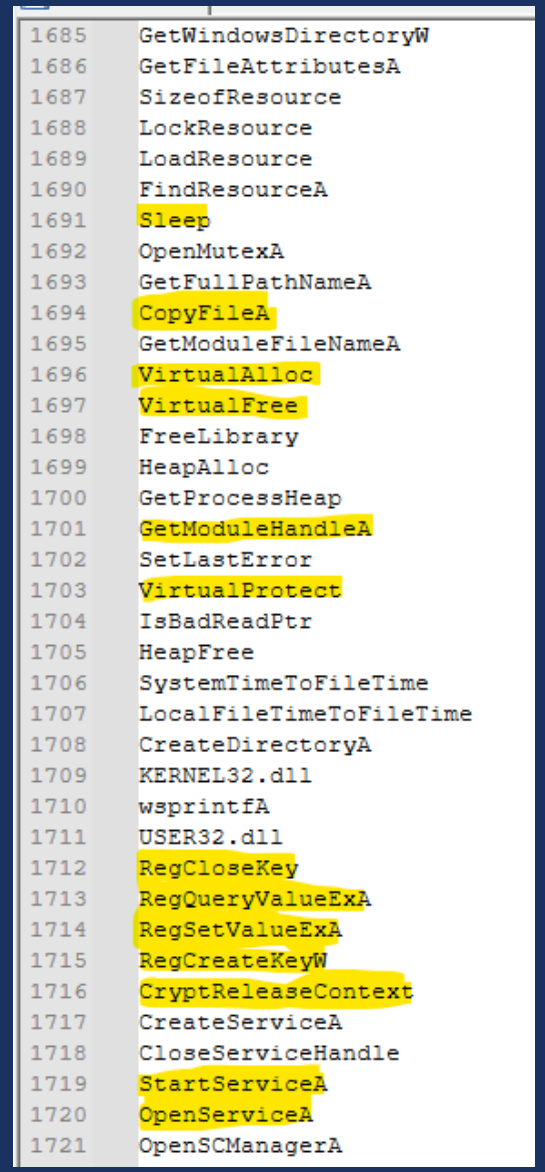
```
550    icacls . /grant Everyone:F /T /C /Q
551    attrib +h .
552    WNcry@2ol7
553    GetNativeSystemInfo
554    .?AVexception@@
555    incompatible version
```



```
 !"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~
GetProcessWindowStation
GetUserObjectInformationW
GetLastActivePopup
GetActiveWindow
MessageBoxW
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
CloseHandle
WriteFile
CreateFileA
SizeofResource
LockResource
LoadResource
FindResourceA
CreateProcessA
KERNEL32.dll
GetCurrentThreadId
FlsSetValue
GetCommandLineA
DecodePointer
UnhandledExceptionFilter
SetUnhandledExceptionFilter
IsDebuggerPresent
RtlVirtualUnwind
RtlLookupFunctionEntry
RtlCaptureContext
EncodePointer
TerminateProcess
```



```
MSVCP60.dll
GetPerAdapterInfo
GetAdaptersInfo
iphlpapi.dll
InternetCloseHandle
InternetOpenUrlA
InternetOpenA
WININET.dll
_ftol
```



```
GetWindowsDirectoryW
GetFileAttributesA
SizeofResource
LockResource
LoadResource
FindResourceA
Sleep
OpenMutexA
GetFullPathNameA
CopyFileA
GetModuleFileNameA
VirtualAlloc
VirtualFree
FreeLibrary
HeapAlloc
GetProcessHeap
GetModuleHandleA
SetLastError
VirtualProtect
IsBadReadPtr
HeapFree
SystemTimeToFileTime
LocalFileTimeToFileTime
CreateDirectoryA
KERNEL32.dll
wsprintfA
USER32.dll
RegCloseKey
RegQueryValueExA
RegSetValueExA
RegCreateKeyW
CryptReleaseContext
CreateServiceA
CloseServiceHandle
StartServiceA
OpenServiceA
OpenSCManagerA
```

USING AI FOR MALWARE

ChatGPT

Understanding the role of the Windows API functions listed in the FLOSS output can give deeper insight into the malware's behavior and its interaction with the Windows operating system. Here's an explanation of some of the key API functions and their relevance to the malware:

File and Directory Management

- `CreateFileA`, `ReadFile`, `WriteFile`: These are fundamental for interacting with files. `CreateFileA` opens or creates a file, `ReadFile` reads data from an open file, and `WriteFile` writes data to an open file. Malware uses these to read from or write to files, potentially for data theft or to manipulate files (e.g., encryption by ransomware).
- `DeleteFileW`, `MoveFileExW`: These functions delete and move files, respectively, which can be used by malware to remove traces or rearrange files to confuse users or thwart analysis.
- `CreateDirectoryA`, `CreateDirectoryW`: Used to create a new directory, which can be part of setting up a location to store malicious files or logs.

Process and Thread Management

- `CreateProcessA`: Launches a new process, which could be used to start another instance of the malware or another malicious process.
- `TerminateProcess`: Ends a process, potentially used to stop security software or other programs that could interfere with the malware's operations.
- `WaitForSingleObject`: Waits for a resource to become available. In malware, this could be used to synchronize events like waiting for a data decryption key.

PESTUDIO

indicator (33)	detail	level
file > embedded	signature: executable, location: .data, offset: 0x0000B020, size: 159744 (b...	1
file > embedded	signature: executable, location: .data, offset: 0x0000F080, size: 5297524 (...	1
file > embedded	signature: executable, location: .rsrc, offset: 0x000320A4, size: 3514368 (...	1
file > extension > count	159	1
libraries > flag	Windows Socket Library	1
libraries > flag	IP Helper API	1
libraries > flag	Internet Extensions for Win32 Library	1
imports > flag	28	1
string > size > suspicious	2039 bytes	2
string > size > suspicious	1403 bytes	2
string > size > suspicious	2693 bytes	2
string > size > suspicious	3926 bytes	2
string > size > suspicious	1554 bytes	2
string > size > suspicious	1430 bytes	2
string > size > suspicious	2988 bytes	2
resource > size	R.1831, 3514368 bytes	2
resources > file-ratio	94.41%	2
file > checksum	0x00000000	2
groups > API	synchronization | execution | file | resource | dynamic-library | memory |...	2
string > URL	http://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	2
label > mutex	Global\MsWinZonesCacheCounterMutex	2

PESTUDIO

library (7)	duplicate (0)	flag (3)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (91)	group	description
WS2_32.dll	-	x	0x0000A3C4	0x0000A144	implicit	13	network	Windows Socket Library
iphlpapi.dll	-	x	0x0000A3FC	0x0000A17C	implicit	2	network	IP Helper API
WININET.dll	-	x	0x0000A3B4	0x0000A134	implicit	3	network	Internet Extensions for Win32 Library
KERNEL32.dll	-	-	0x0000A2B0	0x0000A030	implicit	32	-	Windows NT BASE API Client
ADVAPI32.dll	-	-	0x0000A280	0x0000A000	implicit	11	-	Advanced Windows 32 Base API
MSVCP60.dll	-	-	0x0000A334	0x0000A0B4	implicit	2	-	Windows C Runtime Library
MSVCRT.dll	-	-	0x0000A340	0x0000A0C0	implicit	28	-	Microsoft C Runtime Library

PESTUDIO

imports (91)	flag (28)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (10)	technique (8)	type (6)	ordinal (1)	library (13)
StartServiceCtrlDispatcherA	x	0x0000A6F6	0x0000A6F6	586 (0x024A)	services	-	implicit	-	ADVAPI32.dll
ChangeServiceConfig2A	x	0x0000A6C0	0x0000A6C0	52 (0x0034)	services	T1569 | System Services	implicit	-	ADVAPI32.dll
CreateServiceA	x	0x0000A688	0x0000A688	100 (0x0064)	services	T1543 | Create or Modify System Proc...	implicit	-	ADVAPI32.dll
QueryPerformanceFrequency	x	0x0000A43A	0x0000A43A	676 (0x02A4)	reconnaissance	-	implicit	-	KERNEL32.dll
3 (closesocket)	x	0x80000003	0x80000003	0 (0x0000)	network	-	implicit	x	WS2_32.dll
16 (recv)	x	0x80000010	0x80000010	0 (0x0000)	network	-	implicit	x	WS2_32.dll
19 (send)	x	0x80000013	0x80000013	0 (0x0000)	network	-	implicit	x	WS2_32.dll
8 (htonl)	x	0x80000008	0x80000008	0 (0x0000)	network	-	implicit	x	WS2_32.dll
14 (ntohl)	x	0x8000000E	0x8000000E	0 (0x0000)	network	-	implicit	x	WS2_32.dll
115 (WSAStartup)	x	0x80000073	0x80000073	0 (0x0000)	network	-	implicit	x	WS2_32.dll
12 (inet_ntoa)	x	0x8000000C	0x8000000C	0 (0x0000)	network	-	implicit	x	WS2_32.dll
10 (ioctlsocket)	x	0x8000000A	0x8000000A	0 (0x0000)	network	-	implicit	x	WS2_32.dll
18 (select)	x	0x80000012	0x80000012	0 (0x0000)	network	-	implicit	x	WS2_32.dll
9 (htons)	x	0x80000009	0x80000009	0 (0x0000)	network	-	implicit	x	WS2_32.dll
23 (socket)	x	0x80000017	0x80000017	0 (0x0000)	network	-	implicit	x	WS2_32.dll
4 (connect)	x	0x80000004	0x80000004	0 (0x0000)	network	-	implicit	x	WS2_32.dll
11 (inet_addr)	x	0x8000000B	0x8000000B	0 (0x0000)	network	-	implicit	x	WS2_32.dll
GetAdaptersInfo	x	0x0000A792	0x0000A792	28 (0x001C)	network	-	implicit	-	iphlpapi.dll
InternetOpenA	x	0x0000A7DC	0x0000A7DC	146 (0x0092)	network	-	implicit	-	WININET.dll
InternetOpenUrlA	x	0x0000A7C8	0x0000A7C8	147 (0x0093)	network	-	implicit	-	WININET.dll
InternetCloseHandle	x	0x0000A7B2	0x0000A7B2	105 (0x0069)	network	-	implicit	-	WININET.dll
MoveFileExA	x	0x0000A576	0x0000A576	623 (0x026F)	file	T1105 | Remote File Copy	implicit	-	KERNEL32.dll
GetCurrentThreadId	x	0x0000A524	0x0000A524	326 (0x0146)	execution	T1057 | Process Discovery	implicit	-	KERNEL32.dll
GetCurrentThread	x	0x0000A53A	0x0000A53A	325 (0x0145)	execution	-	implicit	-	KERNEL32.dll
CryptGenRandom	x	0x0000A650	0x0000A650	150 (0x0096)	cryptography	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll
CryptAcquireContextA	x	0x0000A638	0x0000A638	133 (0x0085)	cryptography	T1027 | Obfuscated Files or Information	implicit	-	ADVAPI32.dll
rand	x	0x0000A824	0x0000A824	678 (0x02A6)	cryptography	T1027 | Obfuscated Files or Information	implicit	-	MSVCRT.dll
srand	x	0x0000A852	0x0000A852	692 (0x02B4)	cryptography	T1027 | Obfuscated Files or Information	implicit	-	MSVCRT.dll

PESTUDIO

encoding (2)	size (bytes)	location	flag (58)	label (541)	group (16)	technique (14)	value
ascii	13	section:.rdata	x	import	services	T1543 | Create or Modify System Proc...	CreateService
ascii	20	section:.rdata	x	import	services	T1569 | System Services	ChangeServiceConfig2
ascii	26	section:.rdata	x	import	services	-	StartServiceCtrlDispatcher
ascii	13	section:.rsrc	x	import	services	T1543 | Create or Modify System Proc...	CreateService
ascii	13	section:.rsrc	x	-	registry	T1112 | Modify Registry	RegSetValueEx
ascii	12	section:.rsrc	x	-	registry	T1112 | Modify Registry	RegCreateKey
ascii	25	section:.rdata	x	import	reconnaissance	-	QueryPerformanceFrequency
ascii	19	section:.data	x	-	reconnaissance	T1057 | Process Discovery	GetCurrentProcessId
ascii	19	section:.rsrc	x	-	reconnaissance	-	GetNativeSystemInfo
ascii	15	section:.rdata	x	import	network	-	GetAdaptersInfo
ascii	19	section:.rdata	x	import	network	-	InternetCloseHandle
ascii	15	section:.rdata	x	import	network	-	InternetOpenUrl
ascii	12	section:.rdata	x	import	network	-	InternetOpen
ascii	12	section:.rsrc	x	-	memory	T1055 | Process Injection	VirtualAlloc
ascii	14	section:.rsrc	x	-	memory	T1055 | Process Injection	VirtualProtect
ascii	10	section:.rdata	x	import	file	T1105 | Remote File Copy	MoveFileEx
ascii	10	section:.rsrc	x	import	file	T1105 | Remote File Copy	MoveFileEx
ascii	9	section:.data	x	-	file	-	WriteFile
ascii	9	section:.data	x	-	file	-	WriteFile
ascii	9	section:.data	x	-	file	-	WriteFile
ascii	9	section:.rsrc	x	-	file	-	WriteFile
ascii	17	section:.rsrc	x	-	file	-	SetFileAttributes
ascii	10	section:.rsrc	x	-	file	T1485 | Data Destruction	DeleteFile
ascii	8	section:.rsrc	x	-	file	T1105 | Remote File Copy	MoveFile
ascii	9	section:.rsrc	x	-	file	-	WriteFile
ascii	18	section:.rdata	x	import	execution	T1057 | Process Discovery	GetCurrentThreadId
ascii	16	section:.rdata	x	import	execution	-	GetCurrentThread
ascii	18	section:.data	x	import	execution	T1057 | Process Discovery	GetCurrentThreadId
ascii	13	section:.data	x	-	execution	T1106 | Execution through API	CreateProcess
ascii	13	section:.data	x	-	execution	T1106 | Execution through API	CreateProcess
ascii	22	section:.data	x	-	execution	-	RtlLookupFunctionEntry
ascii	16	section:.data	x	-	execution	-	TerminateProcess
ascii	17	section:.data	x	-	execution	T1057 | Process Discovery	GetCurrentProcess
ascii	21	section:.data	x	-	execution	-	GetEnvironmentStrings
ascii	13	section:.data	x	-	execution	T1106 | Execution through API	CreateProcess
ascii	18	section:.rsrc	x	-	execution	-	GetExitCodeProcess
ascii	16	section:.rsrc	x	-	execution	-	TerminateProcess
ascii	13	section:.rsrc	x	-	execution	T1106 | Execution through API	CreateProcess
ascii	23	section:.data	x	-	desktop	-	GetProcessWindowStation
ascii	24	section:.data	x	-	desktop	-	GetUserObjectInformation
ascii	19	section:.rdata	x	import	crypto | obfuscation	T1027 | Obfuscated Files or Information	CryptAcquireContext
ascii	14	section:.rdata	x	import	crypto | obfuscation	T1027 | Obfuscated Files or Information	CryptGenRandom
ascii	19	section:.rsrc	x	import	crypto | obfuscation	T1027 | Obfuscated Files or Information	CryptAcquireContext

CAPA

md5	db349b97c37d22f5ea1d1841e3c89eb4
sha1	e889544aff85ffaf8b0d0da705105dee7c97fe26
sha256	24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c
analysis	static
os	windows
format	pe
arch	i386
path	C:/Users/Admin1/Desktop/Ransomware.wannacry.exe.malz

ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	Obfuscated Files or Information::Indicator Removal from Tools T1027.005
DISCOVERY	File and Directory Discovery T1083 System Information Discovery T1082 System Network Configuration Discovery T1016
EXECUTION	Shared Modules T1129 System Services::Service Execution T1569.002
PERSISTENCE	Create or Modify System Process::Windows Service T1543.003

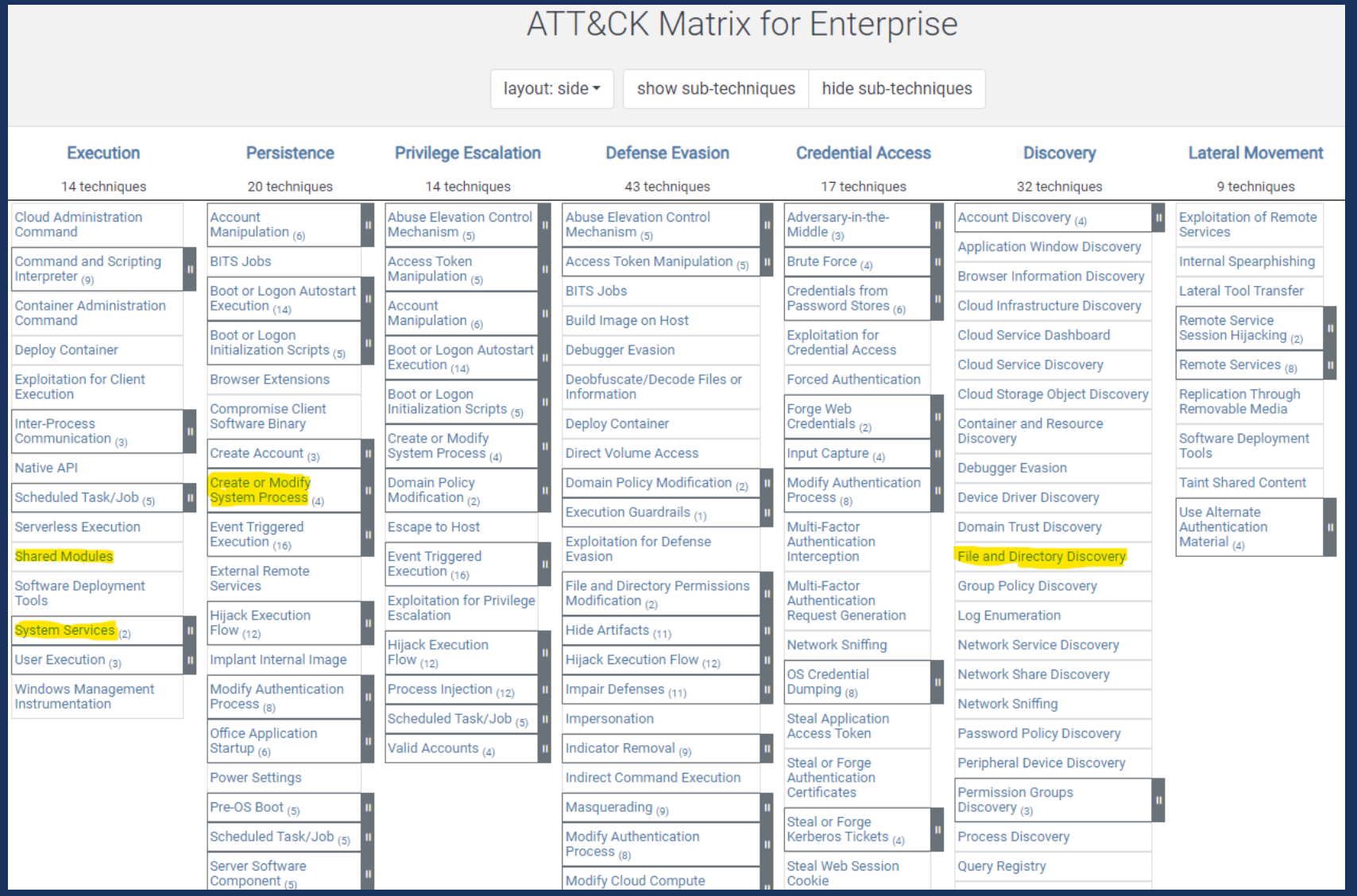
CAPA

MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Conditional Execution::Runs as Service [B0025.007] Debugger Detection::Timing/Delay Check QueryPerformanceCounter [B0001.033]
ANTI-STATIC ANALYSIS	Executable Code Obfuscation::Argument Obfuscation [B0032.020] Executable Code Obfuscation::Stack Strings [B0032.017]
COMMAND AND CONTROL	C2 Communication::Receive Data [B0030.002] C2 Communication::Send Data [B0030.001]
COMMUNICATION	HTTP Communication::Create Request [C0002.012] HTTP Communication::Open URL [C0002.004] Socket Communication::Connect Socket [C0001.004] Socket Communication::Create TCP Socket [C0001.011] Socket Communication::Create UDP Socket [C0001.010] Socket Communication::Get Socket Status [C0001.012] Socket Communication::Initialize Winsock Library [C0001.009] Socket Communication::Receive Data [C0001.006] Socket Communication::Send Data [C0001.007] Socket Communication::Set Socket Config [C0001.001] Socket Communication::TCP Client [C0001.008]
CRYPTOGRAPHY	Generate Pseudo-random Sequence::Use API [C0021.003]
DATA	Compression Library [C0060]
DISCOVERY	Code Discovery::Inspect Section Memory Permissions [B0046.002] File and Directory Discovery [E1083]
EXECUTION	Install Additional Program [B0023]
FILE SYSTEM	Move File [C0063] Read File [C0051]
PROCESS	Create Thread [C0038] Terminate Process [C0018] Terminate Thread [C0039]

CAPA

Capability	Namespace
check for time delay via QueryPerformanceCounter	anti-analysis/anti-debugging/debugger-detection
contain obfuscated stackstrings	anti-analysis/obfuscation/string/stackstring
receive data (5 matches)	communication
send data (5 matches)	communication
connect to URL	communication/http/client
get socket status	communication/socket
initialize Winsock library	communication/socket
set socket configuration	communication/socket
create UDP socket (4 matches)	communication/socket/udp/send
act as TCP client	communication/tcp/client
generate random numbers via WinAPI	data-manipulation/prng
extract resource via kernel32 functions	executable/resource
contain an embedded PE file	executable/subfile/pe
get file size	host-interaction/file-system/meta
move file	host-interaction/file-system/move
read file on Windows	host-interaction/file-system/read
get number of processors	host-interaction/hardware/cpu
terminate process	host-interaction/process/terminate
run as service	host-interaction/service
create service	host-interaction/service/create
modify service	host-interaction/service/modify
start service	host-interaction/service/start
create thread (4 matches)	host-interaction/thread/create
terminate thread	host-interaction/thread/terminate
link function at runtime on Windows	linking/runtime-linking
linked against ZLIB	linking/static/zlib
inspect section memory permissions	load-code/pe
persist via Windows service	persistence/service

MITRE ATT&CK


ATT&CK Matrix for Enterprise
layout: side
show sub-techniques
hide sub-techniques
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter (9)
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication (3)
Native API
Scheduled Task/Job (5)
Serverless Execution
Shared Modules
Software Deployment Tools
System Services (2)
User Execution (3)
Windows Management Instrumentation
Persistence
20 techniques
Account Manipulation (6)
BITS Jobs
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Browser Extensions
Compromise Client Software Binary
Create Account (3)
Create or Modify System Process (4)
Event Triggered Execution (16)
External Remote Services
Hijack Execution Flow (12)
Implant Internal Image
Modify Authentication Process (8)
Office Application Startup (6)
Power Settings
Pre-OS Boot (5)
Scheduled Task/Job (5)
Server Software Component (5)
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism (5)
Access Token Manipulation (5)
Account Manipulation (6)
Boot or Logon Autostart Execution (14)
Boot or Logon Initialization Scripts (5)
Create or Modify System Process (4)
Domain Policy Modification (2)
Escape to Host
Event Triggered Execution (16)
Exploitation for Privilege Escalation
Hijack Execution Flow (12)
Process Injection (12)
Scheduled Task/Job (5)
Valid Accounts (4)
Defense Evasion
43 techniques
Abuse Elevation Control Mechanism (5)
Access Token Manipulation (5)
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification (2)
Execution Guardrails (1)
Exploitation for Defense Evasion
File and Directory Permissions Modification (2)
Hide Artifacts (11)
Hijack Execution Flow (12)
Impair Defenses (11)
Impersonation
Indicator Removal (9)
Indirect Command Execution
Masquerading (9)
Modify Authentication Process (8)
Modify Cloud Compute
Credential Access
17 techniques
Adversary-in-the-Middle (3)
Brute Force (4)
Credentials from Password Stores (6)
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials (2)
Input Capture (4)
Modify Authentication Process (8)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (8)
Steal Application Access Token
Steal or Forge Authentication Certificates
Steal or Forge Kerberos Tickets (4)
Steal Web Session Cookie
Discovery
32 techniques
Account Discovery (4)
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Log Enumeration
Network Service Discovery
Network Share Discovery
Network Sniffing
Password Policy Discovery
Peripheral Device Discovery
Permission Groups Discovery (3)
Process Discovery
Query Registry
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking (2)
Remote Services (8)
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (4)

PROCMON

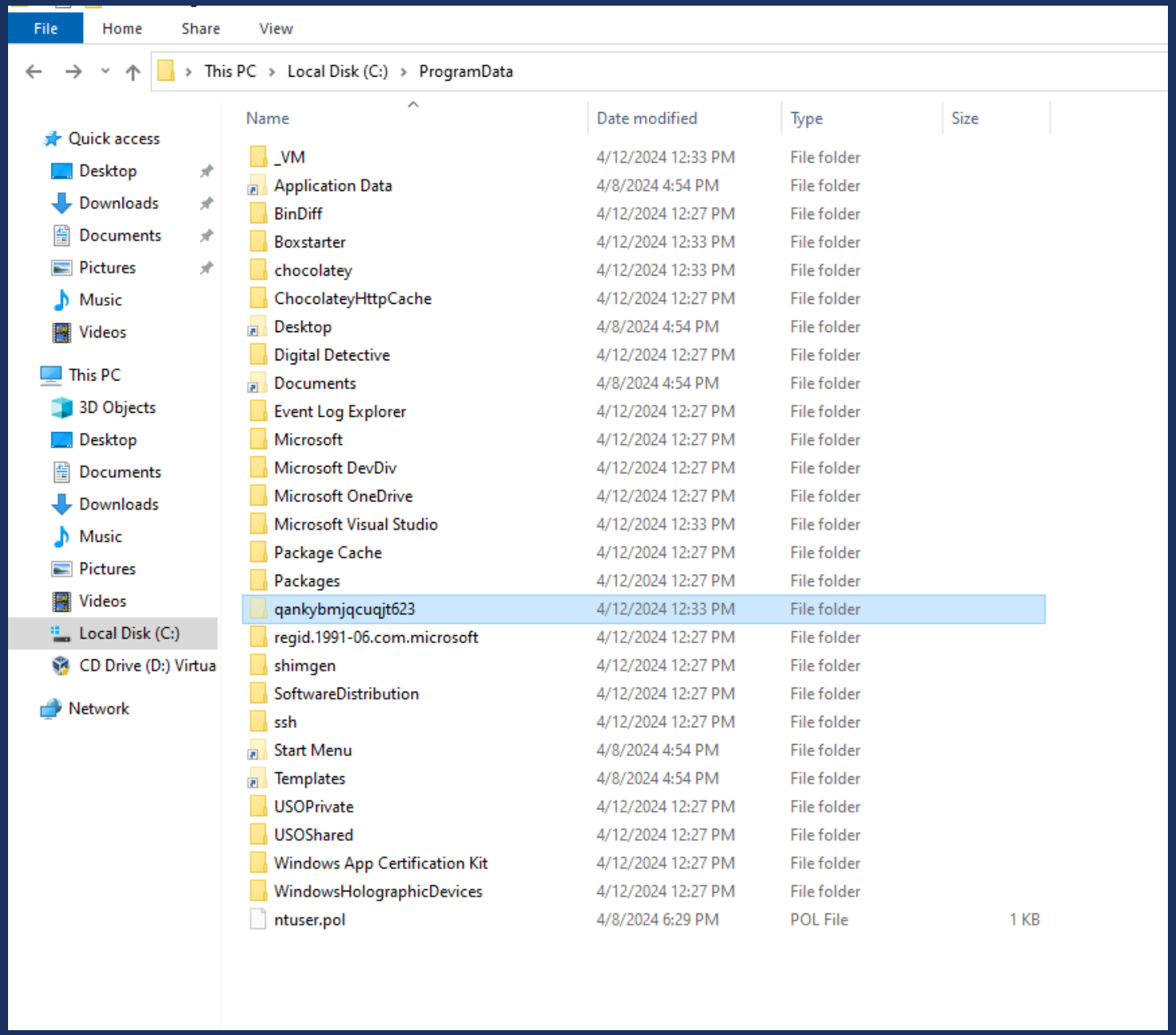
9:08:02.6215303 AM	Ransomware.w...	5096	QuerySecurityFile	C:\Windows\SysWOW64\OnDemandConnRouteHelper.dll	BUFFER OVERFL...	Information: Owner
9:08:02.6215452 AM	Ransomware.w...	5096	QuerySecurityFile	C:\Windows\SysWOW64\OnDemandConnRouteHelper.dll	SUCCESS	Information: Owner
9:08:02.6215546 AM	Ransomware.w...	5096	CloseFile	C:\Windows\SysWOW64\OnDemandConnRouteHelper.dll	SUCCESS	
9:08:02.6216951 AM	Ransomware.w...	5096	ReadFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Offset: 3,163,136, ...
9:08:02.6223223 AM	Ransomware.w...	5096	CreateFile	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Desired Access: R...
9:08:02.6223542 AM	Ransomware.w...	5096	QueryBasicInfor...	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	CreationTime: 9/7/...
9:08:02.6223635 AM	Ransomware.w...	5096	CloseFile	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	
9:08:02.6224428 AM	Ransomware.w...	5096	CreateFile	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Desired Access: R...
9:08:02.6224690 AM	Ransomware.w...	5096	CreateFileMapp...	C:\Windows\SysWOW64\winhttp.dll	FILE LOCKED WI...	SyncType: SyncTy...
9:08:02.6227559 AM	Ransomware.w...	5096	CreateFileMapp...	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	SyncType: SyncTy...
9:08:02.6229944 AM	Ransomware.w...	5096	CloseFile	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	
9:08:02.6230926 AM	Ransomware.w...	5096	CreateFile	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Desired Access: R...
9:08:02.6231196 AM	Ransomware.w...	5096	QuerySecurityFile	C:\Windows\SysWOW64\winhttp.dll	BUFFER OVERFL...	Information: Owner
9:08:02.6231290 AM	Ransomware.w...	5096	QuerySecurityFile	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	Information: Owner
9:08:02.6231374 AM	Ransomware.w...	5096	CloseFile	C:\Windows\SysWOW64\winhttp.dll	SUCCESS	
9:08:02.6236293 AM	Ransomware.w...	5096	ReadFile	C:\Windows\SysWOW64\wininet.dll	SUCCESS	Offset: 2,688,000, ...

PROCMON

9:08:44.8760867 AM	Ransomware.w...	5096	QueryBasicInfor...	C:\Windows\tasksche.exe	SUCCESS	CreationTime: 4/12...
9:08:44.8869216 AM	Ransomware.w...	5096	CreateFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	Desired Access: G...
9:08:44.8869568 AM	Ransomware.w...	5096	QueryStandardI...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,0...
9:08:44.8869661 AM	Ransomware.w...	5096	QueryStandardI...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,0...
9:08:44.8869771 AM	Ransomware.w...	5096	CreateFileMapp...	C:\Windows\apppatch\sysmain.sdb	FILE LOCKED WI...	SyncType: SyncTy...
9:08:44.8869868 AM	Ransomware.w...	5096	QueryStandardI...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	AllocationSize: 4,0...
9:08:44.8870024 AM	Ransomware.w...	5096	CreateFileMapp...	C:\Windows\apppatch\sysmain.sdb	SUCCESS	SyncType: SyncTy...
9:08:44.8870520 AM	Ransomware.w...	5096	CloseFile	C:\Windows\apppatch\sysmain.sdb	SUCCESS	
9:08:44.8871184 AM	Ransomware.w...	5096	CloseFile	C:\Windows\tasksche.exe	SUCCESS	
9:08:44.8872306 AM	Ransomware.w...	5096	ReadFile	C:\Windows\SysWOW64\urlmon.dll	SUCCESS	Offset: 562,176, Le...
9:08:44.8900908 AM	Ransomware.w...	2948	CreateFile	C:\Windows\SysWOW64\dhcpcsvc6.dll	SUCCESS	Desired Access: R...
9:08:44.8901094 AM	Ransomware.w...	2948	QueryBasicInfor...	C:\Windows\SysWOW64\dhcpcsvc6.dll	SUCCESS	CreationTime: 9/7/...
9:08:44.8901179 AM	Ransomware.w...	2948	CloseFile	C:\Windows\SysWOW64\dhcpcsvc6.dll	SUCCESS	
9:08:44.8902333 AM	Ransomware.w...	2948	CreateFile	C:\Windows\SysWOW64\dhcpcsvc6.dll	SUCCESS	Desired Access: R...
9:08:44.8902607 AM	Ransomware.w...	2948	CreateFileMapp...	C:\Windows\SysWOW64\dhcpcsvc6.dll	FILE LOCKED WI...	SyncType: SyncTy...
9:08:44.8902806 AM	Ransomware.w...	2948	CreateFileMapp...	C:\Windows\SysWOW64\dhcpcsvc6.dll	SUCCESS	SyncType: SyncTy...
9:08:44.8903997 AM	Ransomware.w...	2948	CloseFile	C:\Windows\SysWOW64\dhcpcsvc6.dll	SUCCESS	
9:08:44.9372877 AM	Ransomware.w...	5096	ReadFile	C:\Windows\SysWOW64\msvcp60.dll	SUCCESS	Offset: 128,000, Le...
9:08:44.9452573 AM	Ransomware.w...	5096	CloseFile	C:\Windows	SUCCESS	
9:08:44.9453300 AM	Ransomware.w...	5096	CloseFile	C:\Users\Admin1\Desktop	SUCCESS	
9:08:44.9610076 AM	Ransomware.w...	5096	CloseFile	C:\Windows\System32\en-US\mswsock.dll.mui	SUCCESS	

PROCMON

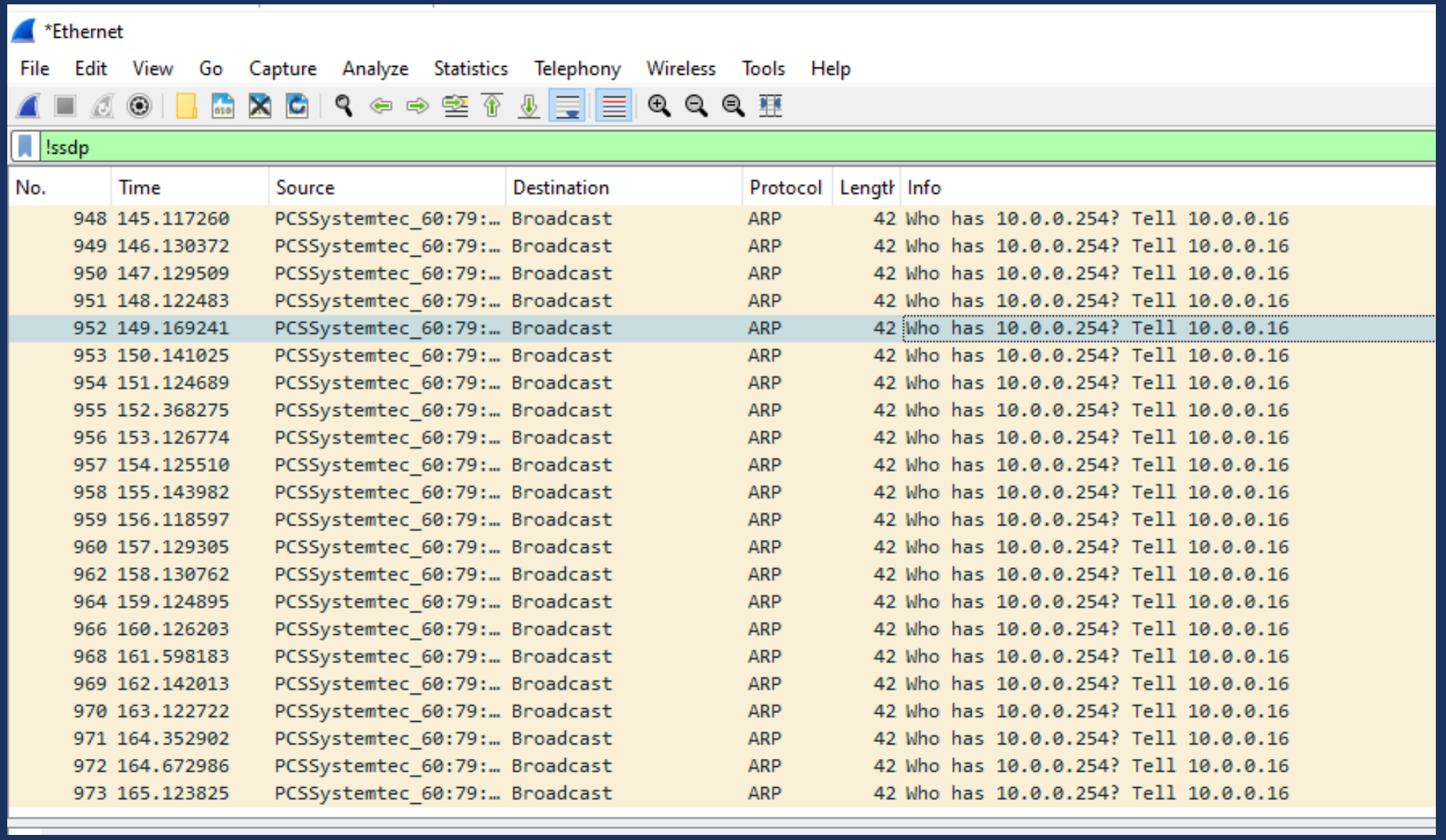
12:25:40.6322732 PM	tasksche.exe	3472	CreateFile	C:\ProgramData	SUCCESS	Desired Access: E...
12:25:40.6322935 PM	tasksche.exe	3472	CloseFile	C:\Users\Admin1\Desktop	SUCCESS	
12:25:40.6324150 PM	tasksche.exe	3472	CreateFile	C:\ProgramData\qankybmjqcuqjt623	SUCCESS	Desired Access: R...
12:25:40.6324519 PM	tasksche.exe	3472	ReadFile	C:\$Secure:$SDH:$INDEX_ALLOCATION	SUCCESS	Offset: 32,768, Len...
12:25:40.6329788 PM	tasksche.exe	3472	CloseFile	C:\ProgramData\qankybmjqcuqjt623	SUCCESS	
12:25:40.6338176 PM	tasksche.exe	3472	CreateFile	C:\ProgramData\qankybmjqcuqjt623	SUCCESS	Desired Access: E...
12:25:40.6338575 PM	tasksche.exe	3472	CloseFile	C:\ProgramData	SUCCESS	
12:25:40.6340223 PM	tasksche.exe	3472	CreateFile	C:\ProgramData\qankybmjqcuqjt623\qankybmjqcuqjt623	NAME NOT FOUND	Desired Access: R...
12:25:40.6341096 PM	tasksche.exe	3472	CreateFile	C:\ProgramData\qankybmjqcuqjt623\qankybmjqcuqjt623	NAME NOT FOUND	Desired Access: W...


File
Home
Share
View
This PC
Local Disk (C:)
ProgramData
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
CD Drive (D:) Virtua
Network
Name
Date modified
Type
Size
_VM 4/12/2024 12:33 PM File folder
Application Data 4/8/2024 4:54 PM File folder
BinDiff 4/12/2024 12:27 PM File folder
Boxstarter 4/12/2024 12:33 PM File folder
chocolatey 4/12/2024 12:33 PM File folder
ChocolateyHttpCache 4/12/2024 12:27 PM File folder
Desktop 4/8/2024 4:54 PM File folder
Digital Detective 4/12/2024 12:27 PM File folder
Documents 4/8/2024 4:54 PM File folder
Event Log Explorer 4/12/2024 12:27 PM File folder
Microsoft 4/12/2024 12:27 PM File folder
Microsoft DevDiv 4/12/2024 12:27 PM File folder
Microsoft OneDrive 4/12/2024 12:27 PM File folder
Microsoft Visual Studio 4/12/2024 12:33 PM File folder
Package Cache 4/12/2024 12:27 PM File folder
Packages 4/12/2024 12:27 PM File folder
qankybmjqcuqjt623 4/12/2024 12:33 PM File folder
regid.1991-06.com.microsoft 4/12/2024 12:27 PM File folder
shimgen 4/12/2024 12:27 PM File folder
SoftwareDistribution 4/12/2024 12:27 PM File folder
ssh 4/12/2024 12:27 PM File folder
Start Menu 4/8/2024 4:54 PM File folder
Templates 4/8/2024 4:54 PM File folder
USOPrivate 4/12/2024 12:27 PM File folder
USOShared 4/12/2024 12:27 PM File folder
Windows App Certification Kit 4/12/2024 12:27 PM File folder
WindowsHolographicDevices 4/12/2024 12:27 PM File folder
ntuser.pol 4/8/2024 6:29 PM POL File 1 KB

TCPVIEW

spoolsv.exe	2368	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	4/12/2024 11:21:07 AM	Spooler
services.exe	600	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	4/12/2024 11:21:08 AM	services.exe
svchost.exe	2648	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	4/12/2024 11:21:09 AM	PolicyAgent
Ransomware.wannacr...	1444	TCP	Syn Sent	10.0.0.16	49773	10.0.0.74	445	4/12/2024 11:29:41 AM	mssecsvc2.0
Ransomware.wannacr...	1444	TCP	Syn Sent	10.0.0.16	49775	10.0.0.75	445	4/12/2024 11:29:41 AM	mssecsvc2.0
Ransomware.wannacr...	1444	TCP	Syn Sent	10.0.0.16	49776	10.0.0.76	445	4/12/2024 11:29:41 AM	mssecsvc2.0
Ransomware.wannacr...	1444	TCP	Syn Sent	10.0.0.16	49778	10.0.0.77	445	4/12/2024 11:29:41 AM	mssecsvc2.0
Ransomware.wannacr...	1444	TCP	Syn Sent	10.0.0.16	49779	10.0.0.78	445	4/12/2024 11:29:41 AM	mssecsvc2.0
Ransomware.wannacr...	1444	TCP	Syn Sent	10.0.0.16	49781	10.0.0.79	445	4/12/2024 11:29:41 AM	mssecsvc2.0
Ransomware.wannacr...	1444	TCP	Syn Sent	10.0.0.16	49783	10.0.0.80	445	4/12/2024 11:29:42 AM	mssecsvc2.0
Ransomware.wannacr...	1444	TCP	Syn Sent	10.0.0.16	49785	10.0.0.81	445	4/12/2024 11:29:42 AM	mssecsvc2.0
Ransomware.wannacr...	1444	TCP	Syn Sent	10.0.0.16	49786	10.0.0.82	445	4/12/2024 11:29:42 AM	mssecsvc2.0
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	4/12/2024 11:21:08 AM	System
svchost.exe	2080	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	4/12/2024 11:21:07 AM	DoSvc

WIRESHARK


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
!ssdp
No. Time Source Destination Protocol Length Info
948 145.117260 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
949 146.130372 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
950 147.129509 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
951 148.122483 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
952 149.169241 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
953 150.141025 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
954 151.124689 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
955 152.368275 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
956 153.126774 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
957 154.125510 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
958 155.143982 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
959 156.118597 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
960 157.129305 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
962 158.130762 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
964 159.124895 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
966 160.126203 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
968 161.598183 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
969 162.142013 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
970 163.122722 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
971 164.352902 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
972 164.672986 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16
973 165.123825 PCSSystemtec_60:79:… Broadcast ARP 42 Who has 10.0.0.254? Tell 10.0.0.16


THANK YOU!
kellanj103@proton.me