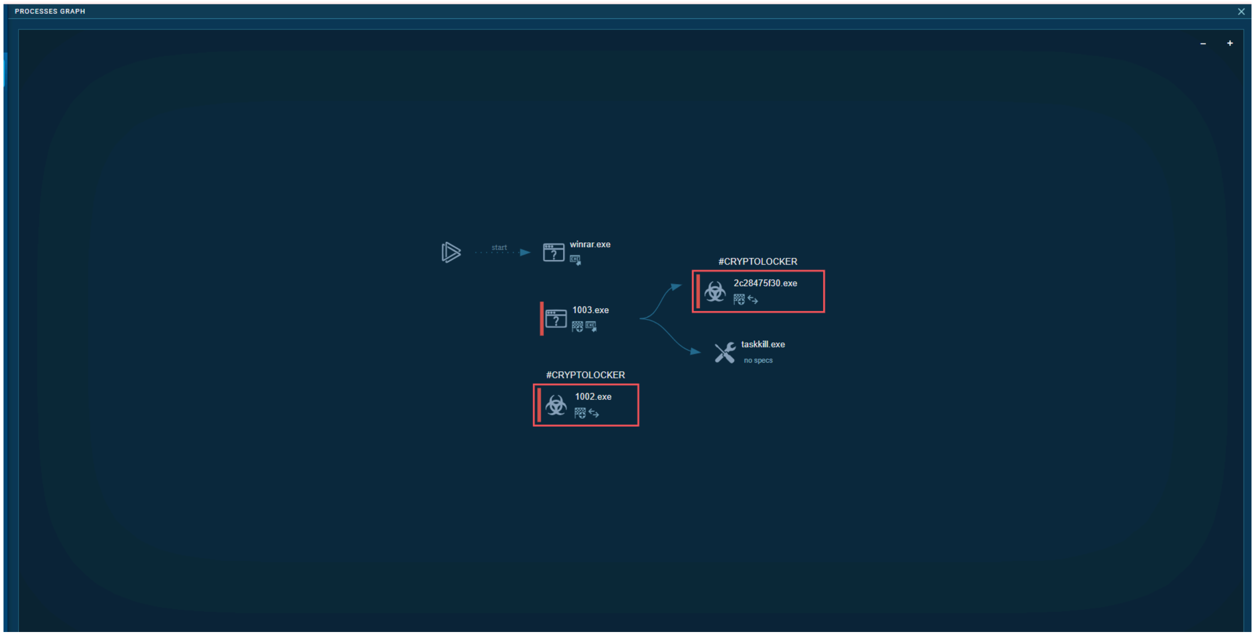
Task 2

For this task, we use a Malware sample from the Malware Zoo.

The sample I decided to use was the Crypto.Locker malware from January 22 2014.

Now with that out of the way, we can go with the analysis

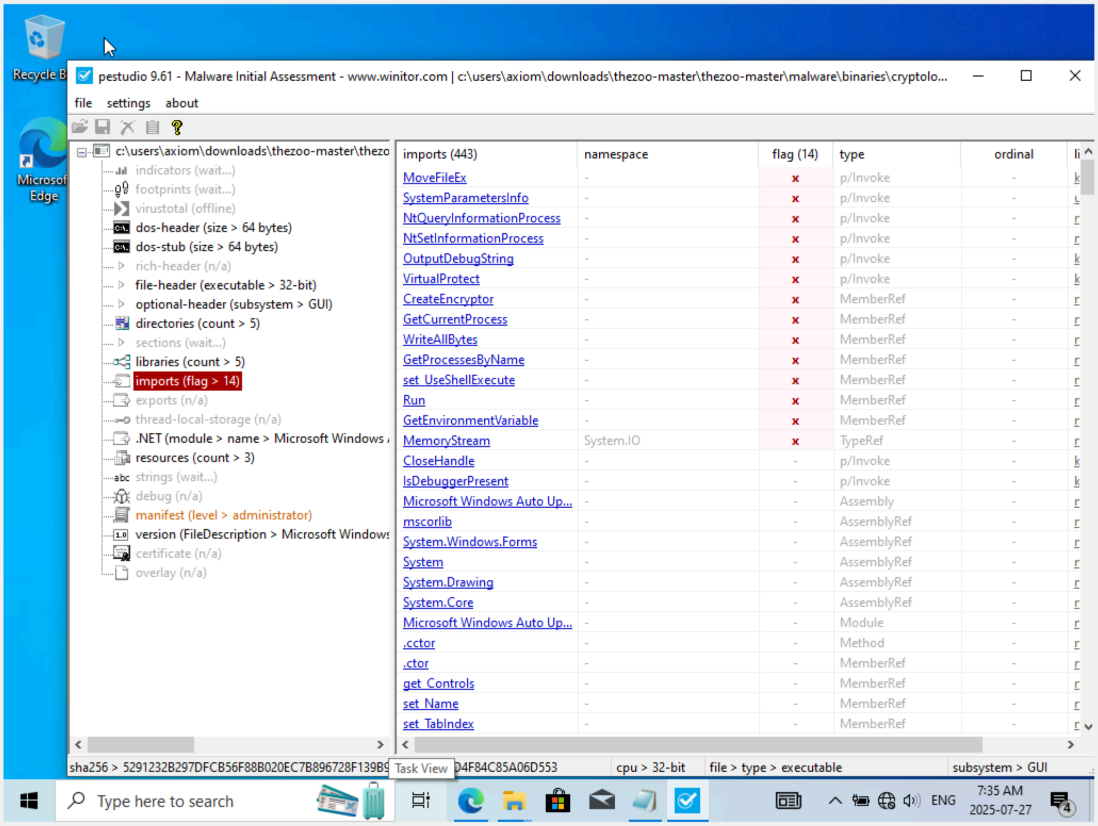
According to our Any.run report, our process graph looks like this:



As we can see there is one exe file that drops our ransomware onto the victim system. While the actual exe is wrapped into the dropper exe. The Dropper exe file is 1003.exe while the actual ransomware is in 1002.exe, but the report assigns it a filename of 2c8475f30.exe. Which for our purposes, is the same executable.

Static Analysis

Screenshots from PEStudio:



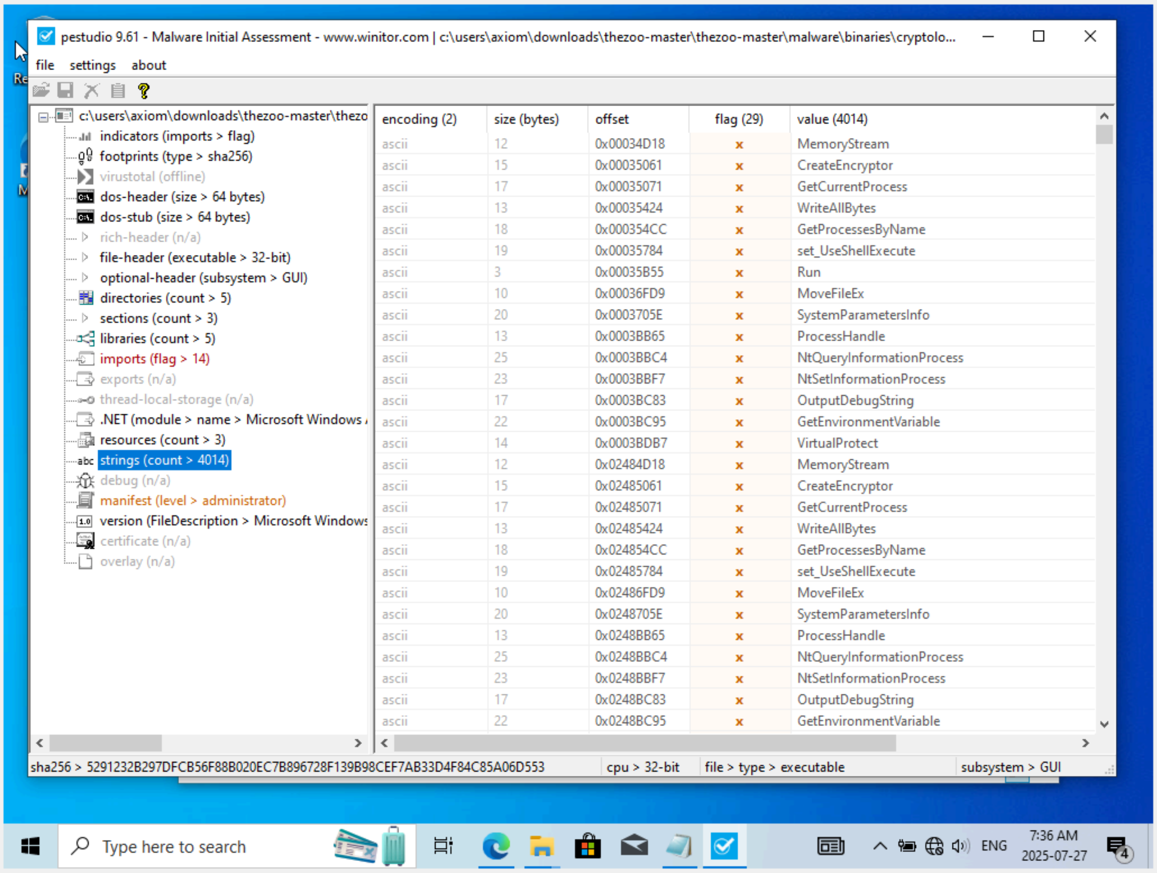
pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\axiom\downloads\thezoo-master\thezoo-master\malware\binaries\cryptolo...

c:\users\axiom\downloads\thezoo-master\thezo
- indicators (wait...)
- footprints (wait...)
- virustotal (offline)
- dos-header (size > 64 bytes)
- dos-stub (size > 64 bytes)
- rich-header (n/a)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 5)
- sections (wait...)
- libraries (count > 5)
- imports (flag > 14)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (module > name > Microsoft Windows
- resources (count > 3)
- strings (wait...)
- debug (n/a)
- manifest (level > administrator)
- version (FileDescription > Microsoft Windows
- certificate (n/a)
- overlay (n/a)

imports (443)	namespace	flag (14)	type	ordinal	li
MoveFileEx	-	x	p/Invoke	-	k
SystemParametersInfo	-	x	p/Invoke	-	u
NtQueryInformationProcess	-	x	p/Invoke	-	r
NtSetInformationProcess	-	x	p/Invoke	-	r
OutputDebugString	-	x	p/Invoke	-	k
VirtualProtect	-	x	p/Invoke	-	k
CreateEncryptor	-	x	MemberRef	-	r
GetCurrentProcess	-	x	MemberRef	-	r
WriteAllBytes	-	x	MemberRef	-	r
GetProcessesByName	-	x	MemberRef	-	r
set_UseShellExecute	-	x	MemberRef	-	r
Run	-	x	MemberRef	-	r
GetEnvironmentVariable	-	x	MemberRef	-	r
MemoryStream	System.IO	x	TypeRef	-	r
CloseHandle	-	-	p/Invoke	-	k
IsDebuggerPresent	-	-	p/Invoke	-	k
Microsoft Windows Auto Up...	-	-	Assembly	-	r
mscorlib	-	-	AssemblyRef	-	r
System.Windows.Forms	-	-	AssemblyRef	-	r
System	-	-	AssemblyRef	-	r
System.Drawing	-	-	AssemblyRef	-	r
System.Core	-	-	AssemblyRef	-	r
Microsoft Windows Auto Up...	-	-	Module	-	r
.cctor	-	-	Method	-	r
.ctor	-	-	MemberRef	-	r
get_Controls	-	-	MemberRef	-	r
set_Name	-	-	MemberRef	-	r
set_TabIndex	-	-	MemberRef	-	r

sha256 > 5291232B297DFCB56F88B020EC7B896728F139B9 Task View D4F84C85A06D553 | cpu > 32-bit | file > type > executable | subsystem > GUI

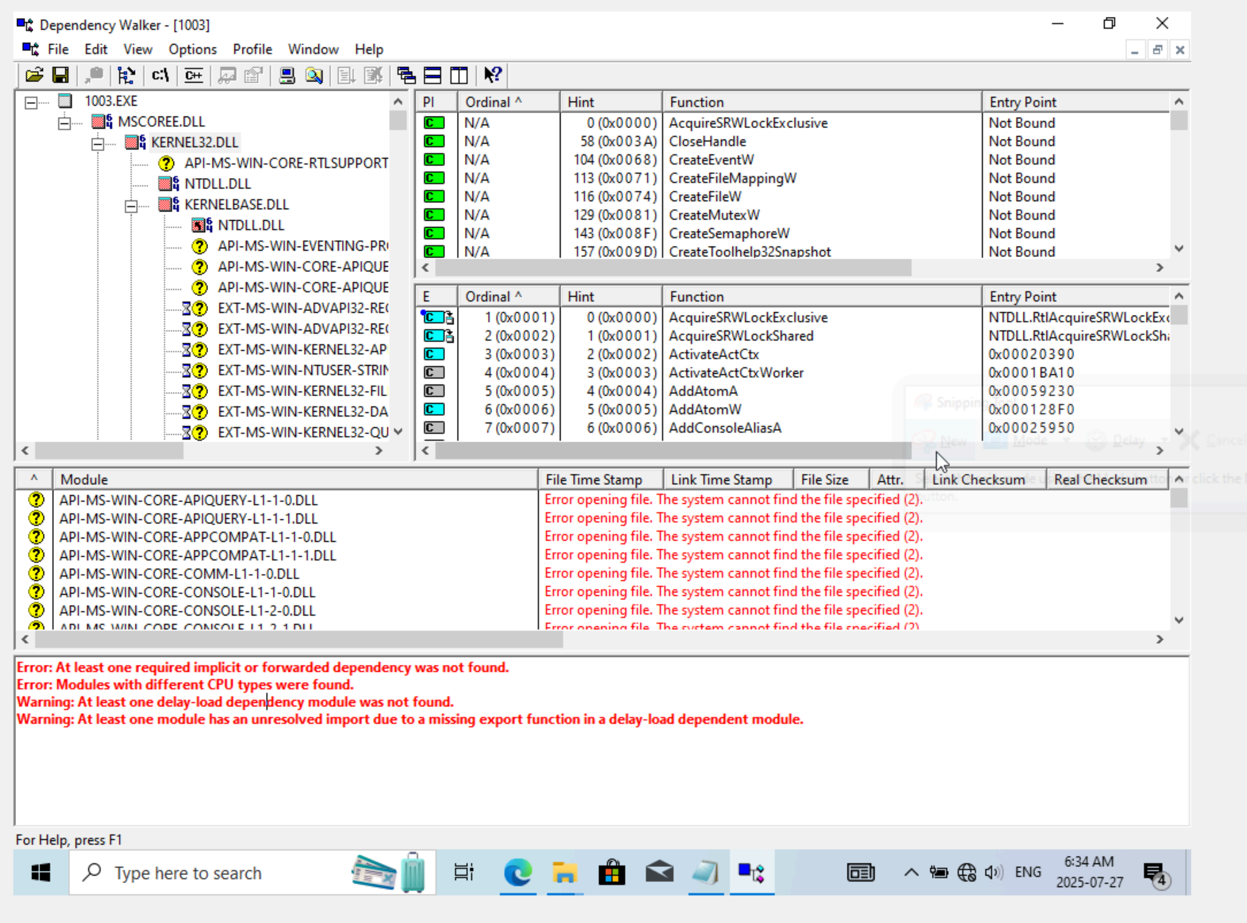
As we can see from the “Imports Tab” , PEstudio has flagged more than several library calls from our sample. The most interesting ones are “MoveFileEx”, “SystemParametersInfo” and “CreateEncryptor”. These three function calls all suggest that not only the victim’s user profile might be modified in some fashion. But also MoveFileEx and CreateEncryptor suggest that not only the the ransomware copies itself onto the user’s disk but also perhaps encrypts itself to avoid detection by AV and EDR systems.


pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\axiom\downloads\thezoo-master\thezoo-master\malware\binaries\cryptolo...
file
settings
about
c:\users\axiom\downloads\thezoo-master\thezo
indicators (imports > flag)
footprints (type > sha256)
virustotal (offline)
dos-header (size > 64 bytes)
dos-stub (size > 64 bytes)
rich-header (n/a)
file-header (executable > 32-bit)
optional-header (subsystem > GUI)
directories (count > 5)
sections (count > 3)
libraries (count > 5)
imports (flag > 14)
exports (n/a)
thread-local-storage (n/a)
.NET (module > name > Microsoft Windows /
resources (count > 3)
strings (count > 4014)
debug (n/a)
manifest (level > administrator)
version (FileDescription > Microsoft Windows
certificate (n/a)
overlay (n/a)
Type here to search
ENG
7:36 AM
2025-07-27

encoding (2)	size (bytes)	offset	flag (29)	value (4014)
ascii	12	0x00034D18	x	MemoryStream
ascii	15	0x00035061	x	CreateEncryptor
ascii	17	0x00035071	x	GetCurrentProcess
ascii	13	0x00035424	x	WriteAllBytes
ascii	18	0x000354CC	x	GetProcessesByName
ascii	19	0x00035784	x	set_UseShellExecute
ascii	3	0x00035B55	x	Run
ascii	10	0x00036FD9	x	MoveFileEx
ascii	20	0x0003705E	x	SystemParametersInfo
ascii	13	0x0003BB65	x	ProcessHandle
ascii	25	0x0003BBC4	x	NtQueryInformationProcess
ascii	23	0x0003BBF7	x	NtSetInformationProcess
ascii	17	0x0003BC83	x	OutputDebugString
ascii	22	0x0003BC95	x	GetEnvironmentVariable
ascii	14	0x0003BDB7	x	VirtualProtect
ascii	12	0x02484D18	x	MemoryStream
ascii	15	0x02485061	x	CreateEncryptor
ascii	17	0x02485071	x	GetCurrentProcess
ascii	13	0x02485424	x	WriteAllBytes
ascii	18	0x024854CC	x	GetProcessesByName
ascii	19	0x02485784	x	set_UseShellExecute
ascii	10	0x02486FD9	x	MoveFileEx
ascii	20	0x0248705E	x	SystemParametersInfo
ascii	13	0x0248BB65	x	ProcessHandle
ascii	25	0x0248BBC4	x	NtQueryInformationProcess
ascii	23	0x0248BBF7	x	NtSetInformationProcess
ascii	17	0x0248BC83	x	OutputDebugString
ascii	22	0x0248BC95	x	GetEnvironmentVariable

sha256 > 5291232B297DFCB56F88B020EC7B896728F139B98CEF7AB33D4F84C85A06D553 | cpu > 32-bit | file > type > executable | subsystem > GUI

From looking at the strings section, The PEStudio program has flagged at least 100 strings that it deems suspicious in the malware sample. As one can see from the screenshot we can see the MoveFileInfo, SystemParametersEx, and CreateEncryptor calls from before. Along with we can see that set_UseShellExecute is invocated to perhaps execute 1002.exe after decryption.


Dependency Walker - [1003]
File Edit View Options Profile Window Help
For Help, press F1
Type here to search
ENG
6:34 AM
2025-07-27

```
1003.EXE
  MSCOREE.DLL
    KERNEL32.DLL
      API-MS-WIN-CORE-RTLSUPPORT
      NTDLL.DLL
      KERNELBASE.DLL
        NTDLL.DLL
        API-MS-WIN-EVENTING-PR
        API-MS-WIN-CORE-APIQUE
        API-MS-WIN-CORE-APIQUE
        EXT-MS-WIN-ADVAPI32-RE
        EXT-MS-WIN-ADVAPI32-RE
        EXT-MS-WIN-KERNEL32-AP
        EXT-MS-WIN-NTUSER-STRIN
        EXT-MS-WIN-KERNEL32-FIL
        EXT-MS-WIN-KERNEL32-DA
        EXT-MS-WIN-KERNEL32-QU
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	AcquireSRWLockExclusive	Not Bound
C	N/A	58 (0x003A)	CloseHandle	Not Bound
C	N/A	104 (0x0068)	CreateEventW	Not Bound
C	N/A	113 (0x0071)	CreateFileMappingW	Not Bound
C	N/A	116 (0x0074)	CreateFileW	Not Bound
C	N/A	129 (0x0081)	CreateMutexW	Not Bound
C	N/A	143 (0x008F)	CreateSemaphoreW	Not Bound
C	N/A	157 (0x009D)	CreateToolhelp32Snapshot	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockEx
C	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockSh
C	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x00020390
C	4 (0x0004)	3 (0x0003)	ActivateActCtxWorker	0x0001BA10
C	5 (0x0005)	4 (0x0004)	AddAtomA	0x00059230
C	6 (0x0006)	5 (0x0005)	AddAtomW	0x000128F0
C	7 (0x0007)	6 (0x0006)	AddConsoleAliasA	0x00025950

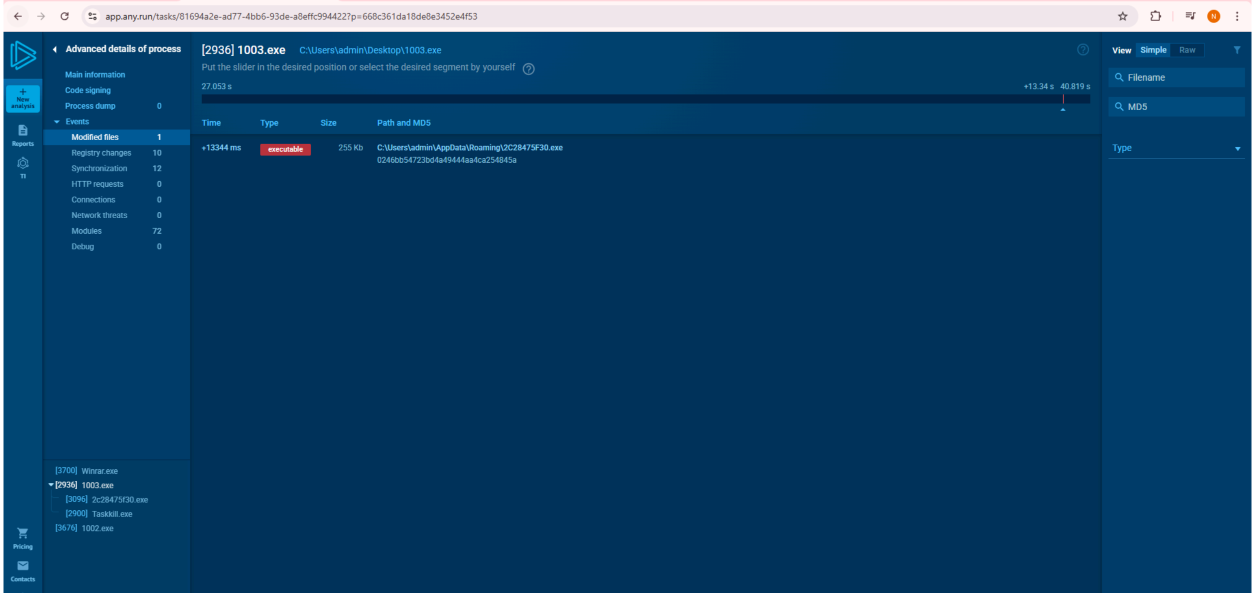
^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum
?	API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. The system cannot find the file specified (2).					

```
Error: At least one required implicit or forwarded dependency was not found.
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

If that is still not convincing enough, we also run our 1003.exe into Dependency Walker:

As we can see, the most important DLLs for analysis here are MSCOREE, NTDLL, and KERNALBASE. MSCOREE the DLL associated with the .NET Core framework and is associated with the runtime engine for .NET applications. Meaning, the application itself is written in .NET. NTDLL, contains libraries and data that are used by other programs and is a crucial operating system file. And KERNALBASE is invocated when there are kernel level changes made to the operating system itself. So combining all of these three finds together, we know that the Cryptolocker is an executable meant to make changes to the operating system and trying to bypass the memory protections offered by the operating system itself by executing itself in kernel mode.

Dynamic Analysis:



[2936] 1003.exe C:\Users\admin\Desktop\1003.exe

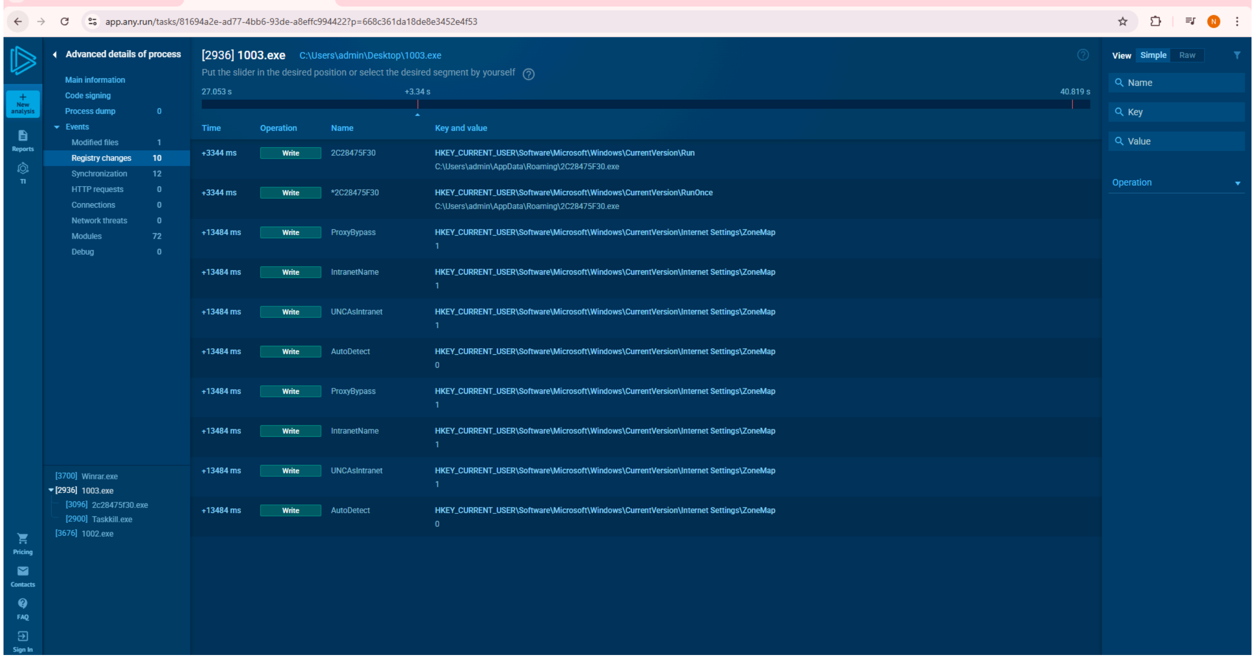
Put the slider in the desired position or select the desired segment by yourself

27.053 s +13.34 s 40.819 s

Time	Type	Size	Path and MD5
+13344 ms	executable	255 Kb	C:\Users\admin\AppData\Roaming\2C28475F30.exe 0246bb54723bd4a49444aa4ca254845a

Obtaining the the Any.run report for the Cryptolocker malware, we can see that the malware makes some changes to the C:\users\admin\Appdata\Roaming\ directory. Appdata contains application specific data and data placed in the Roaming folder are synced onto other devices that are logged in from the same domain. So in other words, logging into a different computer on the same domain would cause the ransomware to spread.

Also 1003.exe makes a lot of Registry Changes listed below:



[2936] 1003.exe C:\Users\admin\Desktop\1003.exe

Put the slider in the desired position or select the desired segment by yourself

27.053 s +3.34 s 40.819 s

Time	Operation	Name	Key and value
+3344 ms	Write	2C28475F30	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run C:\Users\admin\AppData\Roaming\2C28475F30.exe
+3344 ms	Write	*2C28475F30	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce C:\Users\admin\AppData\Roaming\2C28475F30.exe
+13484 ms	Write	ProxyBypass	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+13484 ms	Write	IntranetName	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+13484 ms	Write	UNCAsIntranet	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+13484 ms	Write	AutoDetect	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 0
+13484 ms	Write	ProxyBypass	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+13484 ms	Write	IntranetName	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+13484 ms	Write	UNCAsIntranet	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 1
+13484 ms	Write	AutoDetect	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap 0

So in other words our IOCs then go as follows:

Modifications are made to
C:\users\admin\Appdata\Roaming\

Modifications are made to:
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

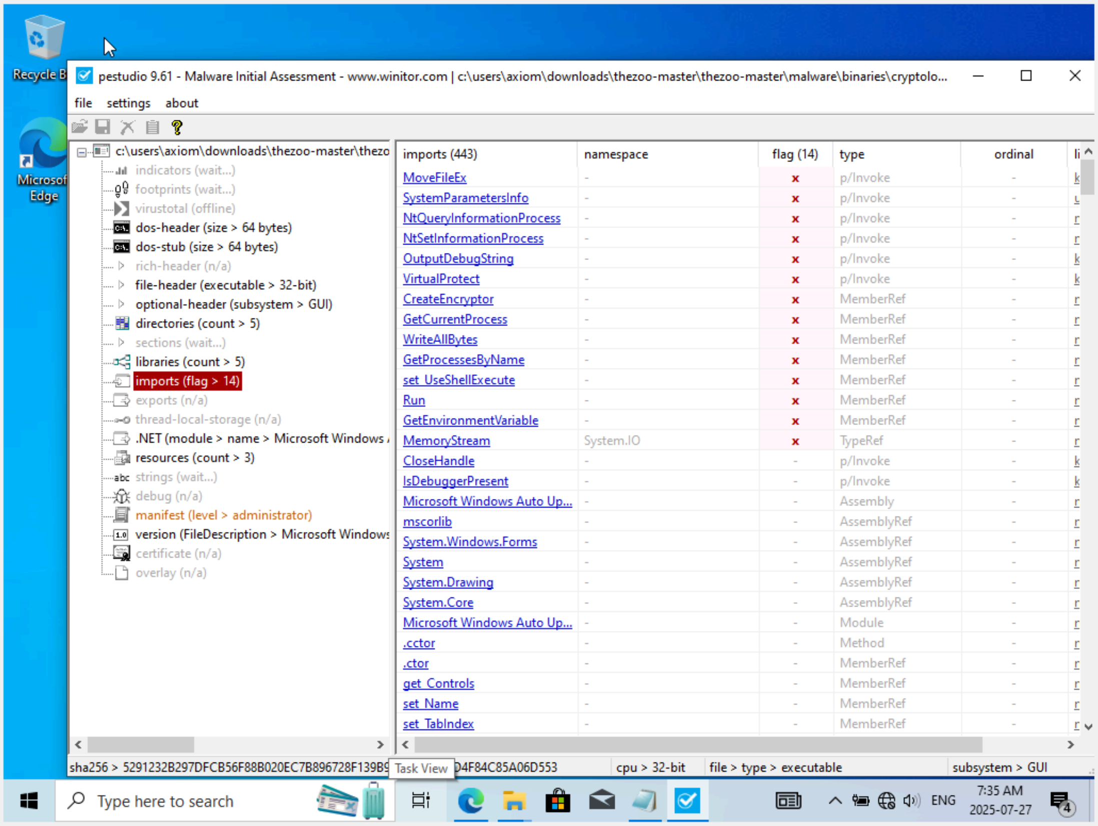
Modifications are made to:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zonemap

Moving on, we then go on with our analysis of 1002.exe the actual exe file the name of our Cryptolocker.

Static Analysis

As we can see, our Cryptolocker uses roughly the same libraries as 1003.exe.



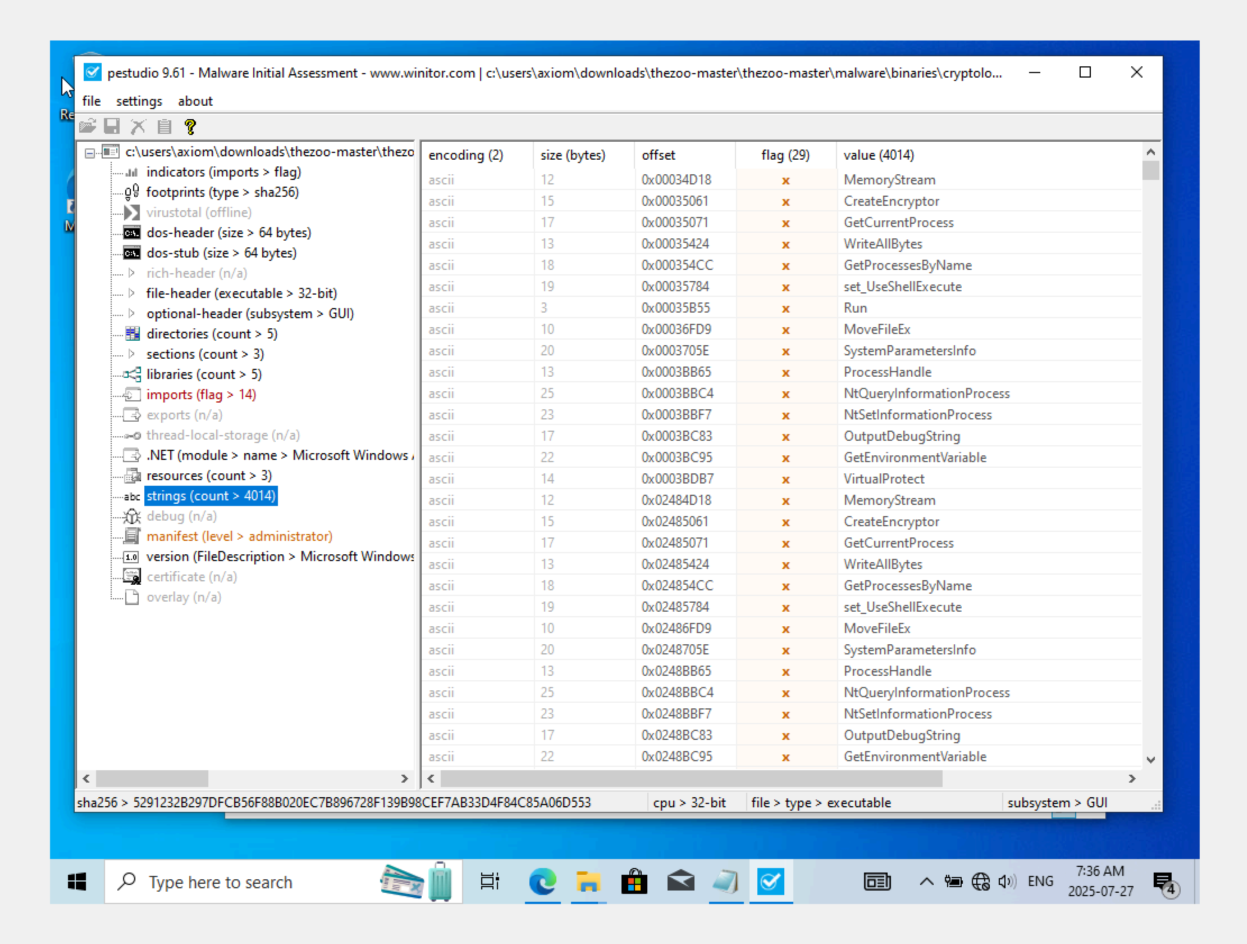
Recycle B
Microsof
Edge
pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\axiom\downloads\thezoo-master\thezoo-master\malware\binaries\cryptolo...
file
settings
about
Type here to search
Task View
ENG
7:35 AM
2025-07-27

```
c:\users\axiom\downloads\thezoo-master\thezo
    indicators (wait...)
    footprints (wait...)
    virustotal (offline)
    dos-header (size > 64 bytes)
    dos-stub (size > 64 bytes)
    rich-header (n/a)
    file-header (executable > 32-bit)
    optional-header (subsystem > GUI)
    directories (count > 5)
    sections (wait...)
    libraries (count > 5)
    imports (flag > 14)
    exports (n/a)
    thread-local-storage (n/a)
    .NET (module > name > Microsoft Windows /
    resources (count > 3)
    strings (wait...)
    debug (n/a)
    manifest (level > administrator)
    version (FileDescription > Microsoft Windows
    certificate (n/a)
    overlay (n/a)
```

imports (443)	namespace	flag (14)	type	ordinal	li
MoveFileEx	-	x	p/Invoke	-	k
SystemParametersInfo	-	x	p/Invoke	-	u
NtQueryInformationProcess	-	x	p/Invoke	-	r
NtSetInformationProcess	-	x	p/Invoke	-	r
OutputDebugString	-	x	p/Invoke	-	k
VirtualProtect	-	x	p/Invoke	-	k
CreateEncryptor	-	x	MemberRef	-	r
GetCurrentProcess	-	x	MemberRef	-	r
WriteAllBytes	-	x	MemberRef	-	r
GetProcessesByName	-	x	MemberRef	-	r
set_UseShellExecute	-	x	MemberRef	-	r
Run	-	x	MemberRef	-	r
GetEnvironmentVariable	-	x	MemberRef	-	r
MemoryStream	System.IO	x	TypeRef	-	r
CloseHandle	-	-	p/Invoke	-	k
IsDebuggerPresent	-	-	p/Invoke	-	k
Microsoft Windows Auto Up...	-	-	Assembly	-	r
mscorlib	-	-	AssemblyRef	-	r
System.Windows.Forms	-	-	AssemblyRef	-	r
System	-	-	AssemblyRef	-	r
System.Drawing	-	-	AssemblyRef	-	r
System.Core	-	-	AssemblyRef	-	r
Microsoft Windows Auto Up...	-	-	Module	-	r
.cctor	-	-	Method	-	r
.ctor	-	-	MemberRef	-	r
get_Controls	-	-	MemberRef	-	r
set_Name	-	-	MemberRef	-	r
set_TabIndex	-	-	MemberRef	-	r

```
sha256 > 5291232B297DFCB56F88B020EC7B896728F139B9    D4F84C85A06D553    cpu > 32-bit    file > type > executable    subsystem > GUI
```

However it seems like the purpose of using the functions are different. Rather instead of encrypting itself to drop on the victim system, it seeks to move the files on the victim's system and encrypt all of the files on the victim's system. I believe some combination of MoveFileInfo, SystemParametersEx, and CreateEncryptor calls are used to achieve this.



pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\axiom\downloads\thezoo-master\thezoo-master\malware\binaries\cryptolo...

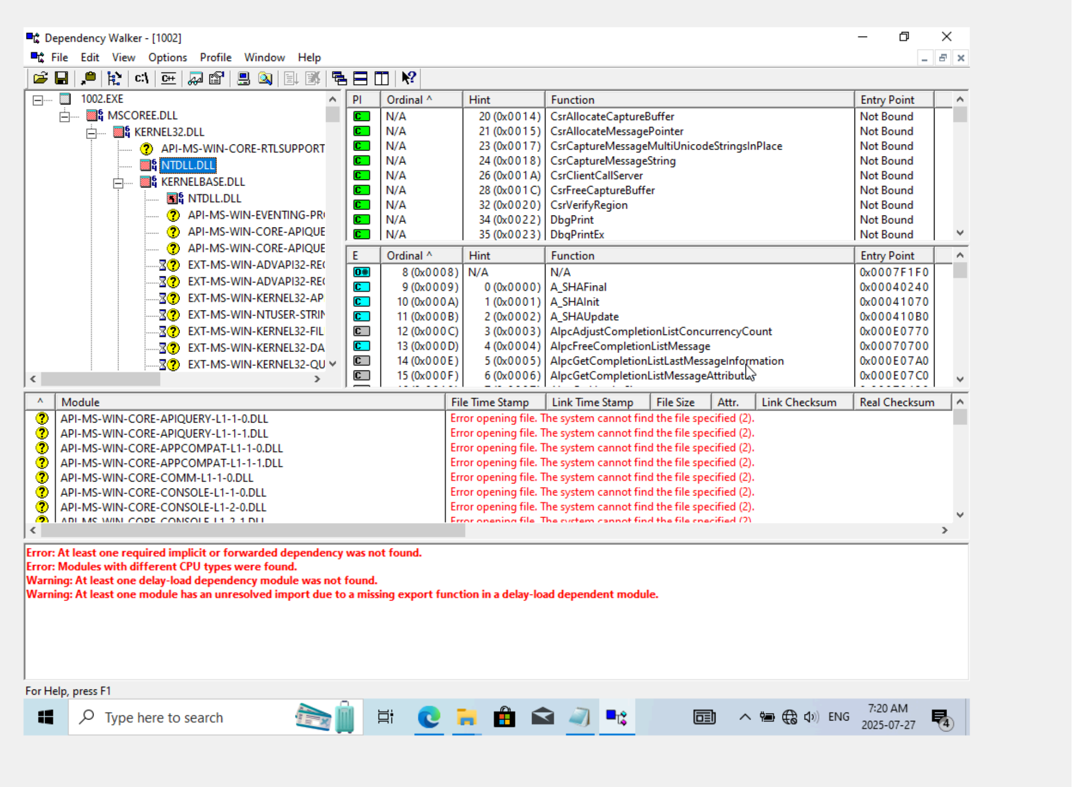
- c:\users\axiom\downloads\thezoo-master\thezo
  - indicators (imports > flag)
  - footprints (type > sha256)
  - virustotal (offline)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 64 bytes)
  - rich-header (n/a)
  - file-header (executable > 32-bit)
  - optional-header (subsystem > GUI)
  - directories (count > 5)
  - sections (count > 3)
  - libraries (count > 5)
  - imports (flag > 14)
  - exports (n/a)
  - thread-local-storage (n/a)
  - .NET (module > name > Microsoft Windows
  - resources (count > 3)
  - strings (count > 4014)
  - debug (n/a)
  - manifest (level > administrator)
  - version (FileDescription > Microsoft Windows
  - certificate (n/a)
  - overlay (n/a)

encoding (2)	size (bytes)	offset	flag (29)	value (4014)
ascii	12	0x00034D18	x	MemoryStream
ascii	15	0x00035061	x	CreateEncryptor
ascii	17	0x00035071	x	GetCurrentProcess
ascii	13	0x00035424	x	WriteAllBytes
ascii	18	0x000354CC	x	GetProcessesByName
ascii	19	0x00035784	x	set_UseShellExecute
ascii	3	0x00035B55	x	Run
ascii	10	0x00036FD9	x	MoveFileEx
ascii	20	0x0003705E	x	SystemParametersInfo
ascii	13	0x0003BB65	x	ProcessHandle
ascii	25	0x0003BBC4	x	NtQueryInformationProcess
ascii	23	0x0003BBF7	x	NtSetInformationProcess
ascii	17	0x0003BC83	x	OutputDebugString
ascii	22	0x0003BC95	x	GetEnvironmentVariable
ascii	14	0x0003BDB7	x	VirtualProtect
ascii	12	0x02484D18	x	MemoryStream
ascii	15	0x02485061	x	CreateEncryptor
ascii	17	0x02485071	x	GetCurrentProcess
ascii	13	0x02485424	x	WriteAllBytes
ascii	18	0x024854CC	x	GetProcessesByName
ascii	19	0x02485784	x	set_UseShellExecute
ascii	10	0x02486FD9	x	MoveFileEx
ascii	20	0x0248705E	x	SystemParametersInfo
ascii	13	0x0248BB65	x	ProcessHandle
ascii	25	0x0248BBC4	x	NtQueryInformationProcess
ascii	23	0x0248BBF7	x	NtSetInformationProcess
ascii	17	0x0248BC83	x	OutputDebugString
ascii	22	0x0248BC95	x	GetEnvironmentVariable

sha256 > 5291232B297DFCB56F88B020EC7B896728F139B98CEF7AB33D4F84C85A06D553 | cpu > 32-bit | file > type > executable | subsystem > GUI

Going further into our strings tab in PEstudio, we can see that PEstudio has flagged the WriteAllBytes call, suggesting to use that the malware might encrypt the user's files.

Also running our sample through PEStudio, we obtain the following DLL tree that looks like this.



```
1002.EXE
    MSCOREE.DLL
        KERNEL32.DLL
            API-MS-WIN-CORE-RTLSUPPORT
            NTDLL.DLL
            KERNELBASE.DLL
                NTDLL.DLL
                API-MS-WIN-EVENTING-PR
                API-MS-WIN-CORE-APIQUE
                API-MS-WIN-CORE-APIQUE
                EXT-MS-WIN-ADVAPI32-RE
                EXT-MS-WIN-ADVAPI32-RE
                EXT-MS-WIN-KERNEL32-AP
                EXT-MS-WIN-NTUSER-STRIN
                EXT-MS-WIN-KERNEL32-FIL
                EXT-MS-WIN-KERNEL32-DA
                EXT-MS-WIN-KERNEL32-QU
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	20 (0x0014)	CsrAllocateCaptureBuffer	Not Bound
C	N/A	21 (0x0015)	CsrAllocateMessagePointer	Not Bound
C	N/A	23 (0x0017)	CsrCaptureMessageMultiUnicodeStringsInPlace	Not Bound
C	N/A	24 (0x0018)	CsrCaptureMessageString	Not Bound
C	N/A	26 (0x001A)	CsrClientCallServer	Not Bound
C	N/A	28 (0x001C)	CsrFreeCaptureBuffer	Not Bound
C	N/A	32 (0x0020)	CsrVerifyRegion	Not Bound
C	N/A	34 (0x0022)	DbgPrint	Not Bound
C	N/A	35 (0x0023)	DbgPrintEx	Not Bound

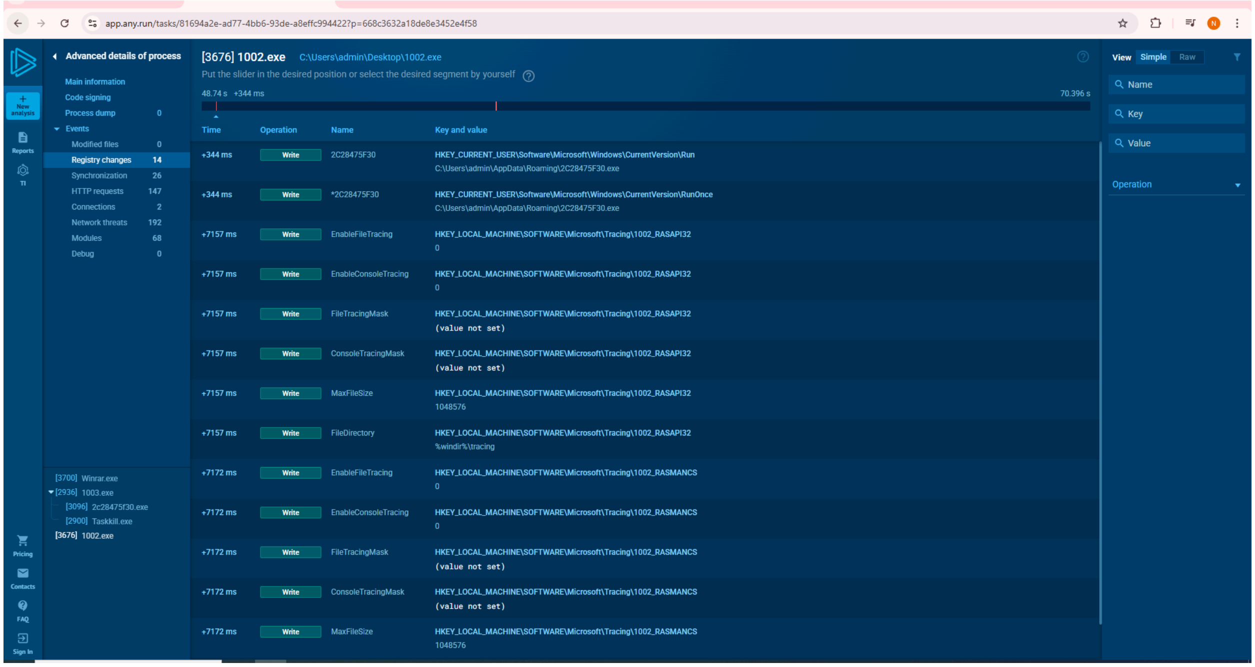
E	Ordinal ^	Hint	Function	Entry Point
O#	8 (0x0008)	N/A	N/A	0x0007F1F0
C	9 (0x0009)	0 (0x0000)	A_SHAFinal	0x00040240
C	10 (0x000A)	1 (0x0001)	A_SHAInit	0x00041070
C	11 (0x000B)	2 (0x0002)	A_SHAUpdate	0x000410B0
C	12 (0x000C)	3 (0x0003)	AlpcAdjustCompletionListConcurrencyCount	0x000E0770
C	13 (0x000D)	4 (0x0004)	AlpcFreeCompletionListMessage	0x00070700
C	14 (0x000E)	5 (0x0005)	AlpcGetCompletionListLastMessageInformation	0x000E07A0
C	15 (0x000F)	6 (0x0006)	AlpcGetCompletionListMessageAttribut	0x000E07C0

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum
?	API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-APIQUERY-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-APPCOMPAT-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-COMM-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).					
?	API-MS-WIN-CORE-CONSOLE-L1-2-0.DLL	Error opening file. The system cannot find the file specified (2).					

```
Error: At least one required implicit or forwarded dependency was not found.
Error: Modules with different CPU types were found.
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.
```

Somewhat similar to our DLL analysis that we did for 1003.exe; MSCOREE is the DLL associated with the .NET Core framework and is associated with the runtime engine for .NET applications. Meaning, the application itself is written in .NET. NTDLL, contains libraries and data that are used by other programs and is a crucial operating system file. And KERNALBASE is invocated when there are kernel level changes made to the operating system itself. So combining all of these three finds together, we know that the Cryptolocker is an executable meant to make changes to the operating system and trying to bypass the memory protections offered by the operating system itself by executing itself in kernel mode.

Dynamic Analysis:



[3676] 1002.exe C:\Users\admin\Desktop\1002.exe

Put the slider in the desired position or select the desired segment by yourself

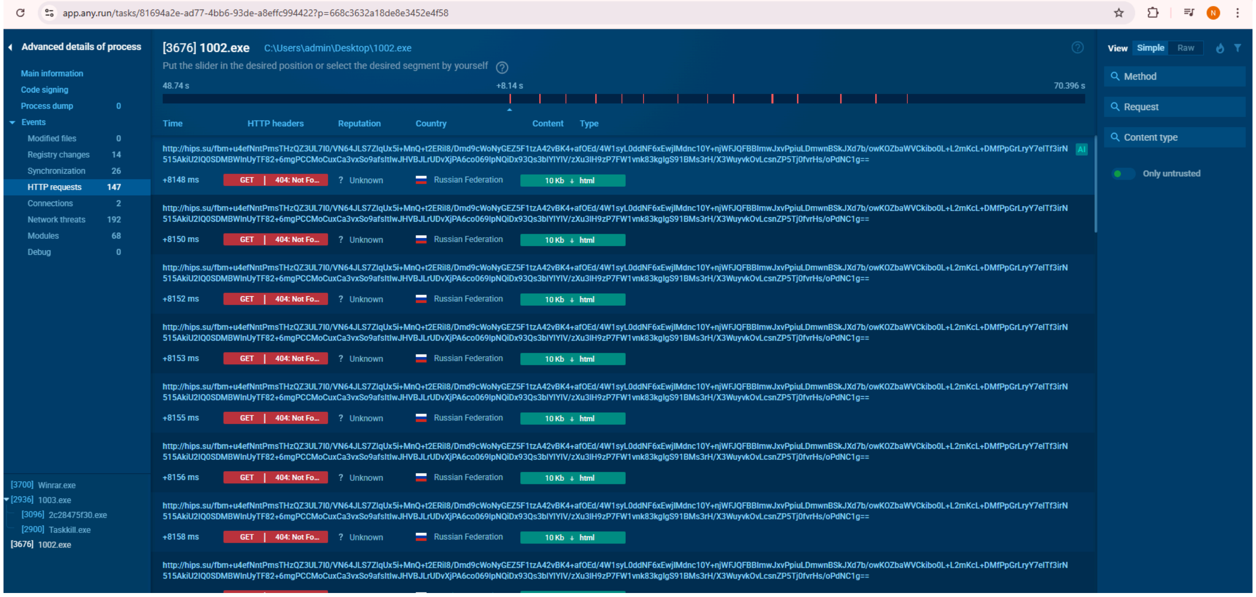
48.74 s +344 ms 70.396 s

Time	Operation	Name	Key and value
+344 ms	Write	2C28475F30	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run C:\Users\admin\AppData\Roaming\2C28475F30.exe
+344 ms	Write	*2C28475F30	HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce C:\Users\admin\AppData\Roaming\2C28475F30.exe
+7157 ms	Write	EnableFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASAPI32 0
+7157 ms	Write	EnableConsoleTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASAPI32 0
+7157 ms	Write	FileTracingMask	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASAPI32 (value not set)
+7157 ms	Write	ConsoleTracingMask	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASAPI32 (value not set)
+7157 ms	Write	MaxFileSize	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASAPI32 1048576
+7157 ms	Write	FileDirectory	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASAPI32 %windir%\tracing
+7172 ms	Write	EnableFileTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASMANCS 0
+7172 ms	Write	EnableConsoleTracing	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASMANCS 0
+7172 ms	Write	FileTracingMask	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASMANCS (value not set)
+7172 ms	Write	ConsoleTracingMask	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASMANCS (value not set)
+7172 ms	Write	MaxFileSize	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\1002_RASMANCS 1048576

As one can see here, multiple Registry keys are being modified. But we can group them together as follows:

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\

Also 1002.exe seems to attempt to make connection request to a .su domain. SU I believe denotes Soviet Union, so we can deduce that the domain is of Russian origin



[3676] 1002.exe C:\Users\admin\Desktop\1002.exe

Put the slider in the desired position or select the desired segment by yourself

48.74 s +8.14 s 70.396 s

Time	HTTP headers	Reputation	Country	Content Type
http://hips.su/fbm+u4efNntPmsTHzQZ3UL7I0/VN64JLS7ZIqUx5i+MnQ+t2ERil8/Dmd9cWoNyGEZ5F1tzA42vBK4+afOEd/4W1syL0ddNF6xEwjIMdnc10Y+njWFJQFBBImwJxvPpiuLDmwnBSkJXd7b/owKOZbaWVCkibo0L+L2mKcL+DMfPpGrLryY7eITf3irN515AkiU2IQ0SDMBWInUyTF82+6mgPCCMoCuxCa3vxSo9afsItlwJHVBJLrUDvXjPA6co069IpNQiDx93Qs3bIYIYIV/zXu3IH9zP7FW1vnk83kgIgS91BMs3rH/X3WuyvkOvLcsnZP5Tj0fvrHs/oPdNC1g==				
+8148 ms	GET | 404: Not Fo...	? Unknown	Russian Federation	10 Kb ↓ html
http://hips.su/fbm+u4efNntPmsTHzQZ3UL7I0/VN64JLS7ZIqUx5i+MnQ+t2ERil8/Dmd9cWoNyGEZ5F1tzA42vBK4+afOEd/4W1syL0ddNF6xEwjIMdnc10Y+njWFJQFBBImwJxvPpiuLDmwnBSkJXd7b/owKOZbaWVCkibo0L+L2mKcL+DMfPpGrLryY7eITf3irN515AkiU2IQ0SDMBWInUyTF82+6mgPCCMoCuxCa3vxSo9afsItlwJHVBJLrUDvXjPA6co069IpNQiDx93Qs3bIYIYIV/zXu3IH9zP7FW1vnk83kgIgS91BMs3rH/X3WuyvkOvLcsnZP5Tj0fvrHs/oPdNC1g==				
+8150 ms	GET | 404: Not Fo...	? Unknown	Russian Federation	10 Kb ↓ html
http://hips.su/fbm+u4efNntPmsTHzQZ3UL7I0/VN64JLS7ZIqUx5i+MnQ+t2ERil8/Dmd9cWoNyGEZ5F1tzA42vBK4+afOEd/4W1syL0ddNF6xEwjIMdnc10Y+njWFJQFBBImwJxvPpiuLDmwnBSkJXd7b/owKOZbaWVCkibo0L+L2mKcL+DMfPpGrLryY7eITf3irN515AkiU2IQ0SDMBWInUyTF82+6mgPCCMoCuxCa3vxSo9afsItlwJHVBJLrUDvXjPA6co069IpNQiDx93Qs3bIYIYIV/zXu3IH9zP7FW1vnk83kgIgS91BMs3rH/X3WuyvkOvLcsnZP5Tj0fvrHs/oPdNC1g==				
+8152 ms	GET | 404: Not Fo...	? Unknown	Russian Federation	10 Kb ↓ html
http://hips.su/fbm+u4efNntPmsTHzQZ3UL7I0/VN64JLS7ZIqUx5i+MnQ+t2ERil8/Dmd9cWoNyGEZ5F1tzA42vBK4+afOEd/4W1syL0ddNF6xEwjIMdnc10Y+njWFJQFBBImwJxvPpiuLDmwnBSkJXd7b/owKOZbaWVCkibo0L+L2mKcL+DMfPpGrLryY7eITf3irN515AkiU2IQ0SDMBWInUyTF82+6mgPCCMoCuxCa3vxSo9afsItlwJHVBJLrUDvXjPA6co069IpNQiDx93Qs3bIYIYIV/zXu3IH9zP7FW1vnk83kgIgS91BMs3rH/X3WuyvkOvLcsnZP5Tj0fvrHs/oPdNC1g==				
+8153 ms	GET | 404: Not Fo...	? Unknown	Russian Federation	10 Kb ↓ html
http://hips.su/fbm+u4efNntPmsTHzQZ3UL7I0/VN64JLS7ZIqUx5i+MnQ+t2ERil8/Dmd9cWoNyGEZ5F1tzA42vBK4+afOEd/4W1syL0ddNF6xEwjIMdnc10Y+njWFJQFBBImwJxvPpiuLDmwnBSkJXd7b/owKOZbaWVCkibo0L+L2mKcL+DMfPpGrLryY7eITf3irN515AkiU2IQ0SDMBWInUyTF82+6mgPCCMoCuxCa3vxSo9afsItlwJHVBJLrUDvXjPA6co069IpNQiDx93Qs3bIYIYIV/zXu3IH9zP7FW1vnk83kgIgS91BMs3rH/X3WuyvkOvLcsnZP5Tj0fvrHs/oPdNC1g==				
+8155 ms	GET | 404: Not Fo...	? Unknown	Russian Federation	10 Kb ↓ html
http://hips.su/fbm+u4efNntPmsTHzQZ3UL7I0/VN64JLS7ZIqUx5i+MnQ+t2ERil8/Dmd9cWoNyGEZ5F1tzA42vBK4+afOEd/4W1syL0ddNF6xEwjIMdnc10Y+njWFJQFBBImwJxvPpiuLDmwnBSkJXd7b/owKOZbaWVCkibo0L+L2mKcL+DMfPpGrLryY7eITf3irN515AkiU2IQ0SDMBWInUyTF82+6mgPCCMoCuxCa3vxSo9afsItlwJHVBJLrUDvXjPA6co069IpNQiDx93Qs3bIYIYIV/zXu3IH9zP7FW1vnk83kgIgS91BMs3rH/X3WuyvkOvLcsnZP5Tj0fvrHs/oPdNC1g==				
+8156 ms	GET | 404: Not Fo...	? Unknown	Russian Federation	10 Kb ↓ html
http://hips.su/fbm+u4efNntPmsTHzQZ3UL7I0/VN64JLS7ZIqUx5i+MnQ+t2ERil8/Dmd9cWoNyGEZ5F1tzA42vBK4+afOEd/4W1syL0ddNF6xEwjIMdnc10Y+njWFJQFBBImwJxvPpiuLDmwnBSkJXd7b/owKOZbaWVCkibo0L+L2mKcL+DMfPpGrLryY7eITf3irN515AkiU2IQ0SDMBWInUyTF82+6mgPCCMoCuxCa3vxSo9afsItlwJHVBJLrUDvXjPA6co069IpNQiDx93Qs3bIYIYIV/zXu3IH9zP7FW1vnk83kgIgS91BMs3rH/X3WuyvkOvLcsnZP5Tj0fvrHs/oPdNC1g==				
+8158 ms	GET | 404: Not Fo...	? Unknown	Russian Federation	10 Kb ↓ html
http://hips.su/fbm+u4efNntPmsTHzQZ3UL7I0/VN64JLS7ZIqUx5i+MnQ+t2ERil8/Dmd9cWoNyGEZ5F1tzA42vBK4+afOEd/4W1syL0ddNF6xEwjIMdnc10Y+njWFJQFBBImwJxvPpiuLDmwnBSkJXd7b/owKOZbaWVCkibo0L+L2mKcL+DMfPpGrLryY7eITf3irN515AkiU2IQ0SDMBWInUyTF82+6mgPCCMoCuxCa3vxSo9afsItlwJHVBJLrUDvXjPA6co069IpNQiDx93Qs3bIYIYIV/zXu3IH9zP7FW1vnk83kgIgS91BMs3rH/X3WuyvkOvLcsnZP5Tj0fvrHs/oPdNC1g==				

In other words our IOCs for 1002.exe goes as follows:

- The following registry keys have been modified:
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
  - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\
- The malware attempts to make a connection request to a malicious .su domain