CSCE-652 Software Reverse Engineering
Spring 2024 Final Project
Ayushri Jain [redacted]
Cerber ransomware
Source: https://github.com/ytisf/theZoo/tree/master/malware/Binaries/Ransomware.Cerber

Analysis Summary

Cerber is a ransomware. Upon execution, it reads information regarding network, cryptography, system, etc. for identifying the environment. It then sends encrypted data to multiple IP addresses on port 6893 via UDP. During runtime, it decrypts its malicious payload. It searches for files and directories recursively and starts the encryption process. First, it modifies the attributes of the target file and then reads the file at multiple offsets. It encrypts the data in memory and overwrites the original file with encrypted data using multiple write operations at multiple offsets. It then renames the original file with a gibberish name and extension (4th part of Machine GUID found in registry key HKLM\SOFTWARE\MICROSOFT\Cryptography\MachineGuid). After encrypting the files, it queries four domains - api.blockcypher.com, btc.blockr.io, bitaps.com and chain.so – and tries to get these two resources:

1. /v1/btc/main/addrs/17gd1mspFnMcEMF1MitTNSsYs7w7AQyct?_=1714156121538 from the server, api.blockcypher.com
2. /api/v1/address/txs/17gd1mspFnMcEMF1MitTNSsYs7w7AQyct?_=1714156121538 from the server btc.blockr.io

The string, 17gd1mspFnMcEMF1MitTNSsYs7w7AQyct looks like a pay to public key hash BTC wallet address and 1714156121538 is the UNIX timestamp of the infected machine. The desktop wallpaper is changed. It also creates ransom notes in each directory that it attacks and opens the ransom note. Finally, it launches a command prompt to kill itself.

Basic Static Analysis

Strings


```
C:\Users\Sysuser>C:\Users\Sysuser\Desktop\Strings\strings.exe C:\Users\Sysuser\D
ownloads\theZoo-master\theZoo-master\malware\Binaries\Ransomware.Cerber\Ransomwa
re.Cerber\cerber.exe > cerber_strings.txt

Strings v2.54 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2021 Mark Russinovich
Sysinternals - www.sysinternals.com
```

Figure 1

AddAtomW	GetTempPathW	lstrcmpiW	RegEnumKeyW
CloseHandle	GetThreadLocale	lstrcpyW	RegOpenKeyExW
CompareFileTime	GetTickCount	lstrlenW	RegOpenKeyW
ConvertDefaultLocale	GetTimeFormatW	KERNEL32.dll	RegQueryValueExW
CopyFileA	GetUserDefaultLCID	CloseWindowStation	RegQueryValueW
CopyFileW	GetVersion	CreateMenu	RegSetValueExW
CreateDirectoryW	GetVersionExA	CreateWindowStationA	RegSetValueW
CreateFileA	GetVolumeInformationW	DefMDIChildProcW	RevertToSelf
CreateFileW	GetWindowsDirectoryW	DefWindowProcW	SaferCloseLevel
CreateProcessW	Heap32ListFirst	DrawFocusRect	SaferComputeTokenFromLevel
CreateThread	HeapAlloc	FillRect	SaferIdentifyLevel
DeleteFileA	HeapFree	FindWindowW	SaferRecordEventLogEntry
DeleteFileW	HeapReAlloc	GetMenuCheckMarkDimensions	ADVAPI32.dll
DuplicateHandle	HeapSize	GetProcessWindowStation	WOWShellExecute
EnterCriticalSection	InitializeCriticalSection	GetSysColorBrush	ShellExecuteExW
EraseTape	InterlockedDecrement	GetThreadDesktop	ShellExecuteA
ExpandEnvironmentStringsW	InterlockedIncrement	GetUpdateRgn	ShellAboutA
FileTimeToLocalFileTime	IsSystemResumeAutomatic	GetUserObjectInformationW	SHIsFileAvailableOffline
FileTimeToSystemTime	LeaveCriticalSection	InflateRect	SHGetSettings
FillConsoleOutputAttribute	**LoadLibraryA**	InsertMenuItemW	SHGetMalloc
FillConsoleOutputCharacterW	**LoadLibraryW**	IsIconic	SHGetDiskFreeSpaceA
FindClose	LocalFree	LockWindowUpdate	SHGetDataFromIDListA
FindFirstFileA	MoveFileExA	MessageBeep	SHFileOperationA
FindFirstFileW	MoveFileExW	MessageBoxW	SHEmptyRecycleBinA
FindNextFileA	MoveFileW	MonitorFromWindow	SHCreateProcessAsUserW
FindNextFileW	MultiByteToWideChar	OffsetRect	SHChangeNotify
FlushConsoleInputBuffer	OpenProcess	PostMessageW	SHBrowseForFolderA
FlushFileBuffers	QueryPerformanceCounter	RealGetWindowClass	SHAppBarMessage
FormatMessageW	QueueUserAPC	SendMessageW	ExtractIconExW
FreeLibrary	RaiseException	SetUserObjectInformationW	DragQueryFileAorW
GetBinaryType	ReadConsoleW	ShowWindow	DragQueryFile
GetBinaryTypeW	ReadFile	ToUnicode	CheckEscapesW
GetCPInfo	ReadProcessMemory	WinHelpA	SHELL32.dll
GetCommandLineW	RemoveDirectoryW	LoadCursorW	StrChrIA
GetCompressedFileSizeW	ScrollConsoleScreenBufferW	GetKBCodePage	StrCmpNA
GetConsoleMode	SearchPathW	USER32.dll	StrCmpNW
GetConsoleOutputCP	SetConsoleCtrlHandler	AddFontMemResourceEx	StrStrIA
GetConsoleScreenBufferInfo	SetConsoleCursorPosition	AnimatePalette	StrStrIW
GetConsoleTitleW	SetConsoleMode	Arc	SHLWAPI.dll
GetCurrentDirectoryW	SetConsoleTextAttribute	BRUSHOBJ_pvAllocRbrush	ImageList_Create
GetCurrentProcess	SetConsoleTitleW	ColorMatchToTarget	COMCTL32.dll
GetCurrentProcessId	SetCurrentDirectoryW	CopyEnhMetaFileA	_XcptFilter
GetCurrentThread	SetEnvironmentVariableW	CreatePatternBrush	__getmainargs
GetCurrentThreadId	SetErrorMode	DescribePixelFormat	__initenv
GetDateFormatW	SetFileAttributesW	EngFreeModule	__p__commode
GetDiskFreeSpaceExW	SetFilePointer	EngTextOut	__p__fmode
GetDriveTypeW	SetFileTime	EnumFontsW	__set_app_type
GetEnvironmentStringsW	SetLastError	FillRgn	__setusermatherr
GetEnvironmentVariableW	SetLocalTime	GdiGetPageCount	_adjust_fdiv
GetExitCodeProcess	SetSystemTime	GetGlyphOutlineW	_c_exit
GetFileAttributesExW	SetThreadLocale	GetMiterLimit	_cexit
GetFileAttributesW	SetUnhandledExceptionFilter	GetOutlineTextMetricsA	_close
GetFileSize	SetVolumeLabelA	GetTextFaceW	_controlfp
GetFileType	SleepEx	GetViewportOrgEx	_dup
GetFullPathNameW	SwitchToThread	OffsetClipRgn	_dup2
GetLastError	SystemTimeToFileTime	PtVisible	_errno
GetLocalTime	TerminateProcess	SetBitmapBits	_except_handler3
GetLocaleInfoW	TransmitCommChar	SetMapperFlags	_exit
GetModuleFileNameA	UnhandledExceptionFilter	SetMiterLimit	_get_osfhandle
GetModuleFileNameW	VirtualAlloc	StartPage	_getch
GetModuleHandleA	VirtualFree	GDI32.dll	_initterm
GetModuleHandleW	VirtualFreeEx	CreateProcessAsUserW	_iob
GetPrivateProfileStringW	VirtualQuery	FreeSid	_open_osfhandle
GetProcAddress	WaitForSingleObject	GetFileSecurityW	_pclose
GetProcessHeap	WideCharToMultiByte	GetSecurityDescriptorOwner	_pipe
GetStartupInfoA	WriteConsoleW	ImpersonateLoggedOnUser	_seh_longjmp_unwind
GetStdHandle	WriteFile	LookupAccountSidW	_setjmp3
GetSystemTime	WritePrivateProfileSectionA	RegCloseKey	_setmode
GetSystemTimeAsFileTime	_hwrite	RegCreateKeyExW	_snwprintf
GetTempFileNameW	lstrcmpW	RegDeleteKeyW	_tell

_ultoa	fprintf	realloc	wcslen
_vsnwprintf	free	setlocale	wcsncmp
_wcsicmp	iswalpha	srand	wcsncpy
_wcslwr	iswdigit	swprintf	wcsrchr
_wcsnicmp	iswspace	swscanf	wcsspn
_wcsupr	iswxdigit	time	wcsstr
_wpopen	longjmp	towlower	wcstol
_wtol	malloc	towupper	wcstoul
calloc	memmove	wcscat	msvcrt.dll
exit	printf	wcschr	
fflush	qsort	wcscmp	
fgets	rand	wcscpy	

11111kicu4p3050f55f298b5211cf2bb82200aa00bdce0bf
VS_VERSION_INFO
StringFileInfo
000004B0
CompanyName
Elaborate   Bytes AG
VarFileInfo
Translation
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
version="5.0.0.0"
processorArchitecture="X86"
name="Siber.Systems.roboform"
type="win32"
<description>Form Filler And Password Mananger.</description>
<dependency>
<dependentAssembly>
<assemblyIdentity
type="win32"
name="Microsoft.Windows.Common-Controls"
version="6.0.0.0"
processorArchitecture="X86"
publicKeyToken="6595b64144ccf1df"
language="*"
/>
</dependentAssembly>
</dependency>
<!-- Identify the application security requirements. -->
<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
<security>
<requestedPrivileges>
<requestedExecutionLevel
level="asInvoker"/>
</requestedPrivileges>
</security>
</trustInfo>
<!-- Setup program compatibility. Inform the system the application supports Windows 7. -->
<compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
<application>
<!--The ID below indicates application support for Windows 7 -->
<supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"/>
<!-- The ID below indicates application support for Windows 8 -->
<supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}"/>
<!-- The ID below indicates application support for Windows 8.1 -->
<supportedOS Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}"/>
</application>
</compatibility>
<asmv3:application xmlns:asmv3="urn:schemas-microsoft-com:asm.v3">
<asmv3:windowsSettings
xmlns="http://schemas.microsoft.com/SMI/2005/WindowsSettings">
<dpiAware>true</dpiAware>
</asmv3:windowsSettings>
</asmv3:application>
</assembly>

There are so many strings present in the exe file that it seems it is unpacked. But the presence of functions LoadLibrary and GetProcAddress makes things suspicious as they are used to load and gain access to additional functions, indicating that these strings might be added as dead code to confuse us. Let's assume for now that the file is packed with a custom packer.

- **Function Calls**: Strings such as **CreateProcessW**, **CreateThread**, **OpenProcess**, **WriteFile**, **ReadFile**, **VirtualAlloc**, **VirtualFree**, **TerminateProcess**, etc., indicate various Windows API functions. It seems that this program will perform actions related to process manipulation, file operations, memory allocation, and termination.
- **System Information**: Strings like **GetSystemTime**, **GetVersionExA**, **GetWindowsDirectoryW, GetVolumeInformationW**, etc., indicate that this program will gather system-specific information. It might use this information to adapt its behavior based on the target environment.

- **File Operations**: Strings including **CopyFileA**, **MoveFileExA**, **DeleteFileA, CreateFileA** indicate that this program will manipulate files. **FindFirstFileA** and **FindNextFileA** might be used to recursively work on directories.
- **Registry Manipulation**: Strings such as **RegCloseKey**, **RegCreateKeyExW**, **RegDeleteKeyW**, **RegQueryValueExW**, **RegSetValueExW**, etc., suggest that this program interacts with the Windows registry for persistence or configuration purposes.
- **Resource Information**: The XML manifest within the executable suggests it is a Windows application named "Siber.Systems.roboform," likely a form filler and password manager. It contains version details, company information, compatibility settings, and required dependencies, aiding in identifying its origin and target environment. The manifest ensures proper management by the operating system but could also be a scheme to evade antivirus detection by including seemingly benign code.
- **Code Injection**: Functions like **ReadProcessMemory**, **QueueUserAPC**, etc., are commonly associated with code injection techniques. In QueueUserAPC process injection, shellcode is not injected into the existing process's memory. Instead, a new process is created in a suspended state and injects our shell into the suspended state. After that, the process is made to wait in a queue before being executed.
- **Dynamic Link Libraries (DLLs)**: There are multiple system DLL strings like **KERNEL32.dll**, **USER32.dll**, **GDI32.dll**, **ADVAPI32.dll**, **SHELL32.dll**, etc.
- **Encrypted Strings**: The string **11111kicu4p3050f55f298b5211cf2bb82200aa00bdce0bf** appears to be a randomly generated or encrypted string.

<u>Exploring Dynamically Linked Functions with Dependency Walker</u>

The application imports the following DLLs:

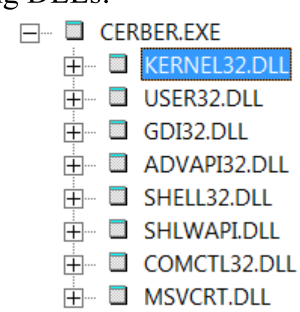


Figure 2

From KERNEL32.DLL, it imports many functions. CreateProcessW and CreateThreadW indicate that it will probably create another process.

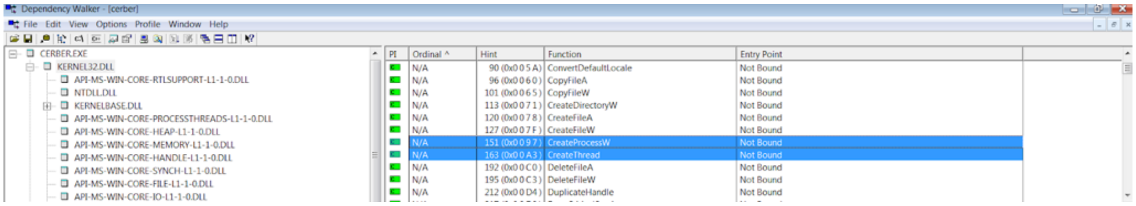
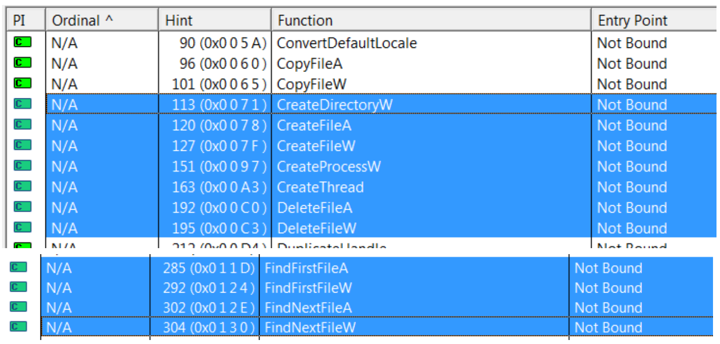


Figure 3

CreateDirectory, CreateFile, DeleteFile hint that it will probably manipulate files and directories. FindFirstFile, FindNextFile further indicate that this application will search through directories.

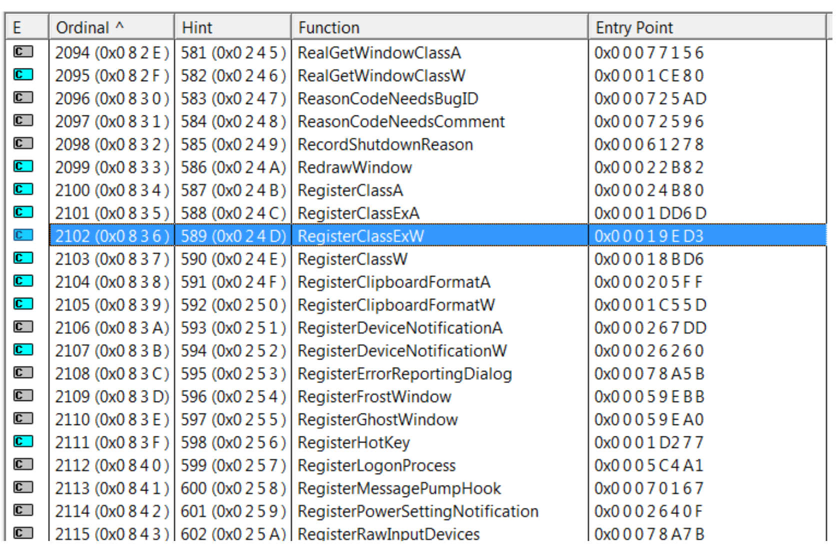


PI	Ordinal ^	Hint	Function	Entry Point
	N/A	90 (0x005A)	ConvertDefaultLocale	Not Bound
	N/A	96 (0x0060)	CopyFileA	Not Bound
	N/A	101 (0x0065)	CopyFileW	Not Bound
	N/A	113 (0x0071)	CreateDirectoryW	Not Bound
	N/A	120 (0x0078)	CreateFileA	Not Bound
	N/A	127 (0x007F)	CreateFileW	Not Bound
	N/A	151 (0x0097)	CreateProcessW	Not Bound
	N/A	163 (0x00A3)	CreateThread	Not Bound
	N/A	192 (0x00C0)	DeleteFileA	Not Bound
	N/A	195 (0x00C3)	DeleteFileW	Not Bound
	N/A	212 (0x00D4)	DuplicateHandle	Not Bound
	N/A	285 (0x011D)	FindFirstFileA	Not Bound
	N/A	292 (0x0124)	FindFirstFileW	Not Bound
	N/A	302 (0x012E)	FindNextFileA	Not Bound
	N/A	304 (0x0130)	FindNextFileW	Not Bound

Figure 4

There are other file functions like CopyFile, ReadFile, WriteFile, SetFileTime, etc. This indicates that the program is going to manipulate the file system.

The imports from User32.dll include large number of GUI manipulation functions (such as RegisterClassEx, SetWindowText, and ShowWindow) indicating a high likelihood that this program has a GUI.



E	Ordinal ^	Hint	Function	Entry Point
	2094 (0x082E)	581 (0x0245)	RealGetWindowClassA	0x00077156
	2095 (0x082F)	582 (0x0246)	RealGetWindowClassW	0x0001CE80
	2096 (0x0830)	583 (0x0247)	ReasonCodeNeedsBugID	0x000725AD
	2097 (0x0831)	584 (0x0248)	ReasonCodeNeedsComment	0x00072596
	2098 (0x0832)	585 (0x0249)	RecordShutdownReason	0x00061278
	2099 (0x0833)	586 (0x024A)	RedrawWindow	0x00022B82
	2100 (0x0834)	587 (0x024B)	RegisterClassA	0x00024B80
	2101 (0x0835)	588 (0x024C)	RegisterClassExA	0x0001DD6D
	2102 (0x0836)	589 (0x024D)	RegisterClassExW	0x00019ED3
	2103 (0x0837)	590 (0x024E)	RegisterClassW	0x00018BD6
	2104 (0x0838)	591 (0x024F)	RegisterClipboardFormatA	0x000205FF
	2105 (0x0839)	592 (0x0250)	RegisterClipboardFormatW	0x0001C55D
	2106 (0x083A)	593 (0x0251)	RegisterDeviceNotificationA	0x000267DD
	2107 (0x083B)	594 (0x0252)	RegisterDeviceNotificationW	0x00026260
	2108 (0x083C)	595 (0x0253)	RegisterErrorReportingDialog	0x00078A5B
	2109 (0x083D)	596 (0x0254)	RegisterFrostWindow	0x00059EBB
	2110 (0x083E)	597 (0x0255)	RegisterGhostWindow	0x00059EA0
	2111 (0x083F)	598 (0x0256)	RegisterHotKey	0x0001D277
	2112 (0x0840)	599 (0x0257)	RegisterLogonProcess	0x0005C4A1
	2113 (0x0841)	600 (0x0258)	RegisterMessagePumpHook	0x00070167
	2114 (0x0842)	601 (0x0259)	RegisterPowerSettingNotification	0x0002640F
	2115 (0x0843)	602 (0x025A)	RegisterRawInputDevices	0x00078A7B

Figure 5

The function RegisterHotKey is also interesting.

2111 (0x0 8 3 F)	598 (0x0 2 5 6)	RegisterHotKey	0x0 0 0 1 D2 7 7
2112 (0x0 8 4 0)	599 (0x0 2 5 7)	RegisterLogonProcess	0x0 0 0 5 C4 A1

Figure 6

The function SetWindowsHookEx is commonly used in keyloggers.

2230 (0x0 8 B6)	717 (0x0 2 C D)	SetWindowsHookA	0x0 0 0 5 8 C1 7
2231 (0x0 8 B7)	718 (0x0 2 C E)	SetWindowsHookExA	0x0 0 0 2 8 3 6 4
2232 (0x0 8 B8)	719 (0x0 2 C F)	SetWindowsHookExW	0x0 0 0 3 0 6 B3
2233 (0x0 8 B9)	720 (0x0 2 D0)	SetWindowsHookW	0x0 0 0 5 8 C3 2
2234 (0x0 8 B A)	721 (0x0 2 D1)	SfmDxBindSwapChain	0x0 0 0 2 5 DD6

Figure 7

The imports from GDI32.dll are graphics-related and simply mean that the program probably has a GUI.

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	2 (0x0 0 0 2)	AddFontMemResourceEx	Not Bound
	N/A	9 (0x0 0 0 9)	AnimatePalette	Not Bound
	N/A	11 (0x0 0 0 B)	Arc	Not Bound
	N/A	14 (0x0 0 0 E)	BRUSHOBJ_pvAllocRbrush	Not Bound
	N/A	32 (0x0 0 2 0)	ColorMatchToTarget	Not Bound
	N/A	36 (0x0 0 2 4)	CopyEnhMetaFileA	Not Bound
	N/A	72 (0x0 0 4 8)	CreatePatternBrush	Not Bound
	N/A	209 (0x0 0 D1)	DescribePixelFormat	Not Bound
	N/A	244 (0x0 0 F 4)	EngFreeModule	Not Bound
	N/A	264 (0x0 1 0 8)	EngTextOut	Not Bound
	N/A	275 (0x0 1 1 3)	EnumFontsW	Not Bound
	N/A	301 (0x0 1 2 D)	FillRgn	Not Bound
	N/A	363 (0x0 1 6 B)	GdiGetPageCount	Not Bound
	N/A	459 (0x0 1 C B)	GetGlyphOutlineW	Not Bound
	N/A	476 (0x0 1 DC)	GetMiterLimit	Not Bound
	N/A	485 (0x0 1 E 5)	GetOutlineTextMetricsA	Not Bound
	N/A	523 (0x0 2 0 B)	GetTextFaceW	Not Bound
	N/A	528 (0x0 2 1 0)	GetViewportOrgEx	Not Bound
	N/A	547 (0x0 2 2 3)	OffsetClipRgn	Not Bound
	N/A	577 (0x0 2 4 1)	PtVisible	Not Bound
	N/A	611 (0x0 2 6 3)	SetBitmapBits	Not Bound
	N/A	636 (0x0 2 7 C)	SetMapperFlags	Not Bound

Figure 8

The imports from Shell32.dll tell us that this program can launch other programs.

N/A	6 (0x0 0 0 6)	CheckEscapesW	Not Bound
N/A	29 (0x0 0 1 D)	DragQueryFile	Not Bound
N/A	31 (0x0 0 1 F)	DragQueryFileAorW	Not Bound
N/A	43 (0x0 0 2 B)	ExtractIconExW	Not Bound
N/A	112 (0x0 0 7 0)	SHAppBarMessage	Not Bound
N/A	119 (0x0 0 7 7)	SHBrowseForFolderA	Not Bound
N/A	124 (0x0 0 7 C)	SHChangeNotify	Not Bound
N/A	146 (0x0 0 9 2)	SHCreateProcessAsUserW	Not Bound
N/A	161 (0x0 0 A1)	SHEmptyRecycleBinA	Not Bound
N/A	168 (0x0 0 A8)	SHFileOperationA	Not Bound
N/A	177 (0x0 0 B1)	SHGetDataFromIDListA	Not Bound
N/A	180 (0x0 0 B4)	SHGetDiskFreeSpaceA	Not Bound
N/A	201 (0x0 0 C9)	SHGetMalloc	Not Bound
N/A	215 (0x0 0 D7)	SHGetSettings	Not Bound
N/A	229 (0x0 0 E 5)	SHIsFileAvailableOffline	Not Bound
N/A	271 (0x0 1 0 F)	ShellAboutA	Not Bound
N/A	276 (0x0 1 1 4)	ShellExecuteA	Not Bound
N/A	279 (0x0 1 1 7)	ShellExecuteExW	Not Bound
N/A	317 (0x0 1 3 D)	WOWShellExecute	Not Bound

Figure 9

The imports from Advapi32.dll tell us that this program uses the registry. In this case, we don't see any string for registry key which further indicates that the malware is hiding somewhere. ImpersonateLoggedOnUser is another interesting function which can allow the calling thread to impersonate the security context of a logged-on user.

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	120 (0x0078)	CreateProcessAsUserW	Not Bound
	N/A	282 (0x011A)	FreeSid	Not Bound
	N/A	298 (0x012A)	GetFileSecurityW	Not Bound
	N/A	325 (0x0145)	GetSecurityDescriptorOwner	Not Bound
	N/A	365 (0x016D)	ImpersonateLoggedOnUser	Not Bound
	N/A	395 (0x018B)	LookupAccountSidW	Not Bound
	N/A	554 (0x022A)	RegCloseKey	Not Bound
	N/A	563 (0x0233)	RegCreateKeyExW	Not Bound
	N/A	574 (0x023E)	RegDeleteKeyW	Not Bound
	N/A	586 (0x024A)	RegEnumKeyW	Not Bound
	N/A	603 (0x025B)	RegOpenKeyExW	Not Bound
	N/A	606 (0x025E)	RegOpenKeyW	Not Bound
	N/A	616 (0x0268)	RegQueryValueExW	Not Bound
	N/A	617 (0x0269)	RegQueryValueW	Not Bound
	N/A	632 (0x0278)	RegSetValueExW	Not Bound
	N/A	633 (0x0279)	RegSetValueW	Not Bound
	N/A	650 (0x028A)	RevertToSelf	Not Bound
	N/A	651 (0x028B)	SaferCloseLevel	Not Bound
	N/A	652 (0x028C)	SaferComputeTokenFromLevel	Not Bound
	N/A	656 (0x0290)	SaferIdentifyLevel	Not Bound
	N/A	657 (0x0291)	SaferRecordEventLogEntry	Not Bound

Figure 10

The import from advapi32.dll (CreateService) tells us that this program creates a service.

	[illegible]	[illegible]	[illegible]	[illegible]
	1130 (0x046A)	128 (0x0080)	CreateServiceA	0x00042120
	1131 (0x046B)	129 (0x0081)	CreateServiceW	0x0002DBC1
	1132 (0x046C)	130 (0x0082)	CreateTraceInstanceId	ntdll.EtwCreateTraceInstanceId

Figure 11

All of the imports from msvcrt.dll are functions that are included in nearly every executable as part of the wrapper code added by the compiler.

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	394 (0x018A)	_snwprintf	Not Bound
	N/A	427 (0x01AB)	_tell	Not Bound
	N/A	438 (0x01B6)	_ultoa	Not Bound
	N/A	448 (0x01C0)	_vsnwprintf	Not Bound
	N/A	456 (0x01C8)	_wcsicmp	Not Bound
	N/A	458 (0x01CA)	_wcslwr	Not Bound
	N/A	460 (0x01CC)	_wcsnicmp	Not Bound
	N/A	465 (0x01D1)	_wcsupr	Not Bound
	N/A	500 (0x01F4)	_wpopen	Not Bound
	N/A	528 (0x0210)	_wtol	Not Bound
	N/A	547 (0x0223)	calloc	Not Bound
	N/A	556 (0x022C)	exit	Not Bound
	N/A	562 (0x0232)	fflush	Not Bound
	N/A	565 (0x0235)	fgets	Not Bound
	N/A	571 (0x023B)	fprintf	Not Bound
	N/A	577 (0x0241)	free	Not Bound
	N/A	607 (0x025F)	iswalpha	Not Bound
	N/A	611 (0x0263)	iswdigit	Not Bound
	N/A	616 (0x0268)	iswspace	Not Bound
	N/A	618 (0x026A)	iswxdigit	Not Bound
	N/A	627 (0x0273)	longjmp	Not Bound
	N/A	628 (0x0274)	malloc	Not Bound
	N/A	635 (0x027B)	memmove	Not Bound

Figure 12

Shlwapi.dll is a vital component of the Windows operating system, linked to the Windows Shell API. Loaded at startup, it provides functions for file management, user interface, and internet tasks. As an integral part of Windows, it is essential for various applications and processes to perform critical operations.

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	270 (0x010E)	StrChrIA	Not Bound
	N/A	281 (0x0119)	StrCmpNA	Not Bound
	N/A	288 (0x0120)	StrCmpNW	Not Bound
	N/A	321 (0x0141)	StrStrIA	Not Bound
	N/A	322 (0x0142)	StrStrIW	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
	867 (0x0363)	313 (0x0139)	StrRChrW	0x00013AB0
	868 (0x0364)	314 (0x013A)	StrRStrIA	0x0003C92E
	869 (0x0365)	315 (0x013B)	StrRStrIW	0x0002EE72
	870 (0x0366)	316 (0x013C)	StrRetToBSTR	0x00019D74
	871 (0x0367)	317 (0x013D)	StrRetToBufA	0x0003CF00
	872 (0x0368)	318 (0x013E)	StrRetToBufW	0x000194A3
	873 (0x0369)	319 (0x013F)	StrRetToStrA	0x0003CE8D
	874 (0x036A)	320 (0x0140)	StrRetToStrW	0x00018C9A
	875 (0x036B)	321 (0x0141)	StrSpnA	0x0003C7CF
	876 (0x036C)	322 (0x0142)	StrSpnW	0x0003C838
	877 (0x036D)	323 (0x0143)	StrStrA	0x0000CDB6
	878 (0x036E)	324 (0x0144)	StrStrIA	0x0000DAFE
	879 (0x036F)	325 (0x0145)	StrStrIW	0x000149E1
	880 (0x0370)	326 (0x0146)	StrStrNIW	0x0003CD18
	881 (0x0371)	327 (0x0147)	StrStrNW	0x0003C9C6
	882 (0x0372)	328 (0x0148)	StrStrW	0x0000E8C7
	883 (0x0373)	329 (0x0149)	StrToInt64ExA	0x0003C707
	884 (0x0374)	330 (0x014A)	StrToInt64ExW	0x0002E8D9
	885 (0x0375)	331 (0x014B)	StrToIntA	0x0000BF27
	886 (0x0376)	332 (0x014C)	StrToIntExA	0x0003C78A
	887 (0x0377)	333 (0x014D)	StrToIntExW	0x0002E894
	888 (0x0378)	334 (0x014E)	StrToIntW	0x00015201
	889 (0x0379)	335 (0x014F)	StrTrimA	0x0003CB48
	890 (0x037A)	336 (0x0150)	StrTrimW	0x00018C1C

Figure 13

COMCTL32.dll, or Common Controls Library 32-bit, is a system file offering standard controls like buttons and menus for Windows applications. It ensures consistent and visually pleasing interfaces. Located in the System32 folder, it is loaded into memory when needed. Major software like Microsoft Office and Adobe Creative Suite depends on it for a unified user experience.

PI	Ordinal ^	Hint	Function	Entry Point
	N/A	83 (0x0053)	ImageList_Create	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
	2 (0x0002)	107 (0x006B)	MenuHelp	0x000327D5
	3 (0x0003)	114 (0x0072)	ShowHideMenuCtl	0x000329E2
	4 (0x0004)	59 (0x003B)	GetEffectiveClientRect	0x00032AAD
	5 (0x0005)	45 (0x002D)	DrawStatusTextA	0x0002A3EA
	6 (0x0006)	7 (0x0007)	CreateStatusWindowA	0x0002A15C
	7 (0x0007)	9 (0x0009)	CreateToolbar	0x0002A5C1
	8 (0x0008)	2 (0x0002)	CreateMappedBitmap	0x0000AB6E
	9 (0x0009)	24 (0x0018)	DPA_LoadStream	0x0002EA33
	10 (0x000A)	26 (0x001A)	DPA_SaveStream	0x0002E6EC
	11 (0x000B)	25 (0x0019)	DPA_Merge	0x0002EB80
	12 (0x000C)	3 (0x0003)	CreatePropertySheetPage	0x00025086
	13 (0x000D)	106 (0x006A)	MakeDragList	0x0002F752
	14 (0x000E)	105 (0x0069)	LBItemFromPt	0x0002F210
	15 (0x000F)	43 (0x002B)	DrawInsert	0x0002F323
	16 (0x0010)	11 (0x000B)	CreateUpDownControl	0x0002D85D
	17 (0x0011)	101 (0x0065)	InitCommonControls	0x00001739
	18 (0x0012)	4 (0x0004)	CreatePropertySheetPageA	0x00025086
	19 (0x0013)	5 (0x0005)	CreatePropertySheetPageW	0x0002506C
	20 (0x0014)	6 (0x0006)	CreateStatusWindow	0x0002A15C
	21 (0x0015)	8 (0x0008)	CreateStatusWindowW	0x0002A11F
	22 (0x0016)	10 (0x000A)	CreateToolbarEx	0x0002A4DA
	23 (0x0017)	41 (0x0029)	DestroyPropertySheetPage	0x00024B46
	24 (0x0018)	42 (0x002A)	DllGetVersion	0x00013436
	25 (0x0019)	44 (0x002C)	DrawStatusText	0x0002A3EA
	26 (0x001A)	46 (0x002E)	DrawStatusTextW	0x0002A3C7
	27 (0x001B)	48 (0x0030)	FlatSB_EnableScrollBar	0x000320C9
	28 (0x001C)	49 (0x0031)	FlatSB_GetScrollInfo	0x00031F0F
	29 (0x001D)	50 (0x0032)	FlatSB_GetScrollPos	0x00031CCD

Figure 14

Using CFF Explorer

Opening the file in CFF Explorer shows that it is a 7-year-old file (2017).

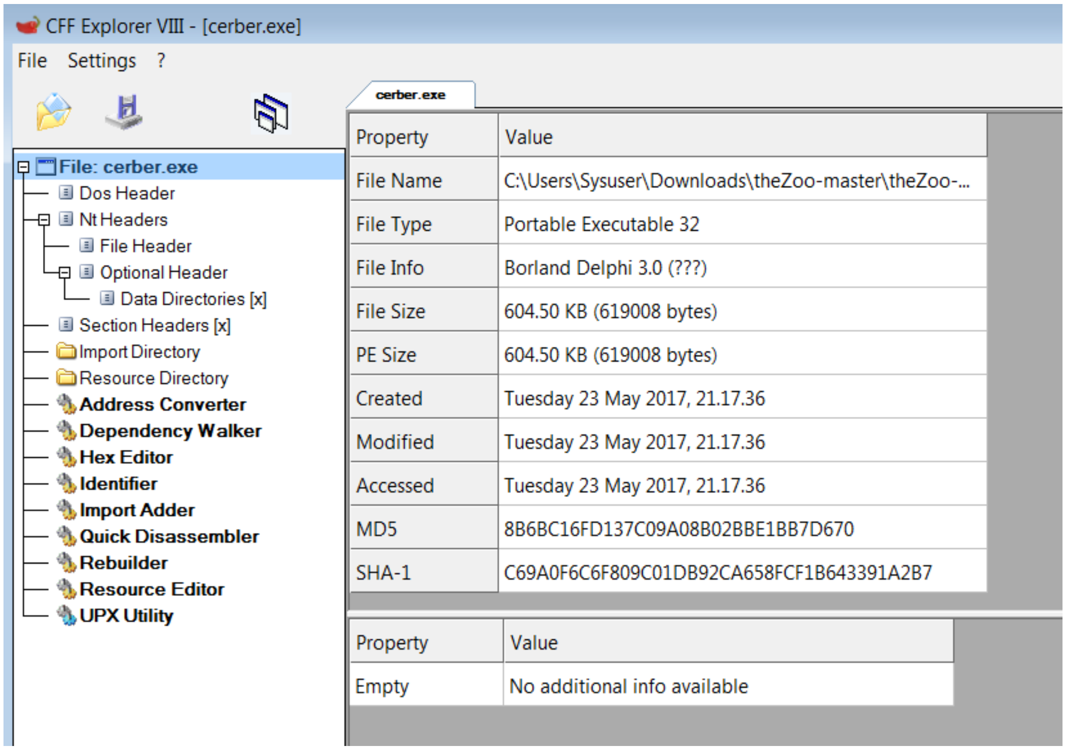


Figure 15

DOS header shows magic = 5A4D which confirms that this program is a Windows executable file (file extension was also .exe).

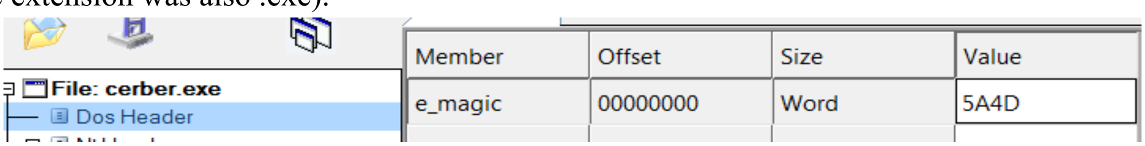


Figure 16

File Header shows this program has 4 sections; TimeDateStamp field tells that this program was compiled on May 24, 2017 and optional header is 224 bytes (E0) long.

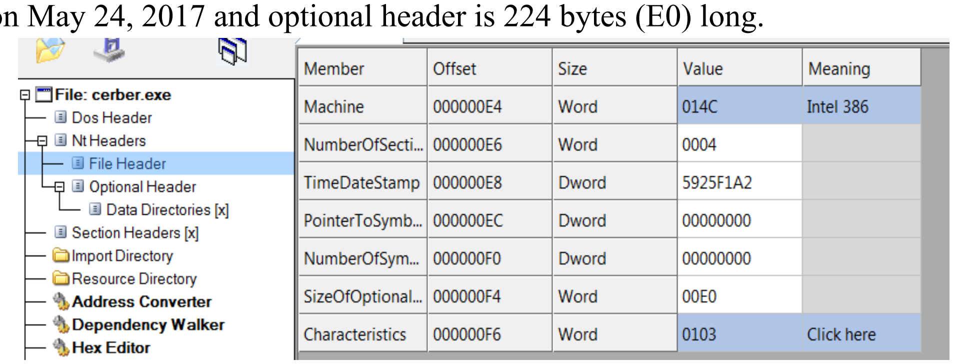


Figure 17

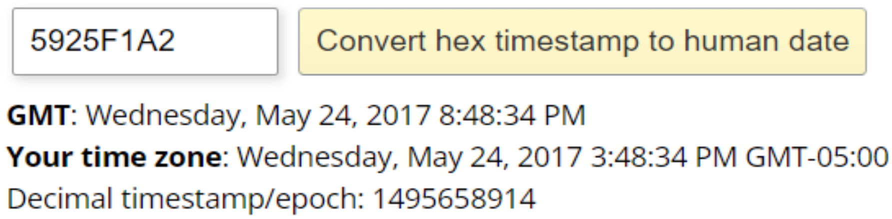


Figure 18

In optional header, subsystem indicates that this program is a GUI program.

Member	Offset	Size	Value	Meaning
Magic	000000F8	Word	010B	PE32
MajorLinkerVersion	000000FA	Byte	09	
MinorLinkerVersion	000000FB	Byte	00	
SizeOfCode	000000FC	Dword	0004EE00	
SizeOfInitializedData	00000100	Dword	00048000	
SizeOfUninitializedData	00000104	Dword	00000000	
AddressOfEntryPoint	00000108	Dword	0004F4E0	.text
BaseOfCode	0000010C	Dword	00001000	
BaseOfData	00000110	Dword	00050000	
ImageBase	00000114	Dword	00400000	
SectionAlignment	00000118	Dword	00001000	
FileAlignment	0000011C	Dword	00000200	
MajorOperatingSystemVersion	00000120	Word	0005	
MinorOperatingSystemVersion	00000122	Word	0000	
MajorImageVersion	00000124	Word	0000	
MinorImageVersion	00000126	Word	0000	
MajorSubsystemVersion	00000128	Word	0005	
MinorSubsystemVersion	0000012A	Word	0000	
Win32VersionValue	0000012C	Dword	00000000	
SizeOfImage	00000130	Dword	0009A000	
SizeOfHeaders	00000134	Dword	00000400	
CheckSum	00000138	Dword	00000000	
Subsystem	0000013C	Word	0002	Windows GUI

Figure 19

Section Header shows that the .text, .rdata, and .rsrc sections each have Virtual Size and Size of Raw Data value of about the same size. It simply shows that it is likely not packed, and that the PE file header was generated by a compiler.

Name	Virtual Size	Virtual Ad...	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	0004ED6E	00001000	0004EE00	00000400	00000000	00000000	0000	0000	60000020
.rdata	0003A87A	00050000	0003AA00	0004F200	00000000	00000000	0000	0000	40000040
.data	000011C0	0008B000	00001200	00089C00	00000000	00000000	0000	0000	C0000040
.rsrc	0000C3A8	0008D000	0000C400	0008AE00	00000000	00000000	0000	0000	40000040

Figure 20

As seen before in Dependency Walker, the Import directory has the same DLLs imported: KERNEL32.dll, USER32.dllm GDI32.dll, ADVAPI32.dll, SHELL32.dll, SHLWAPI.dll, COMCTL32.dll and msvcrt.dll.

Module Name	Imports	OFTs	TimeDateSt...	ForwarderC...	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	143	00088ED8	00000000	00000000	00089DB8	000500C4
USER32.dll	31	00089180	00000000	00000000	00089FF2	0005036C
GDI32.dll	24	00088E74	00000000	00000000	0008A1A2	00050060
ADVAPI32.dll	21	00088E14	00000000	00000000	0008A344	00050000
SHELL32.dll	19	00089118	00000000	00000000	0008A4C0	00050304
SHLWAPI.dll	5	00089168	00000000	00000000	0008A508	00050354
COMCTL32.dll	1	00088E6C	00000000	00000000	0008A528	00050058
msvcrt.dll	73	00089200	00000000	00000000	0008A86E	000503EC

Figure 21

Resource Directory shows that icons with various sizes are present in the resource section of the program.

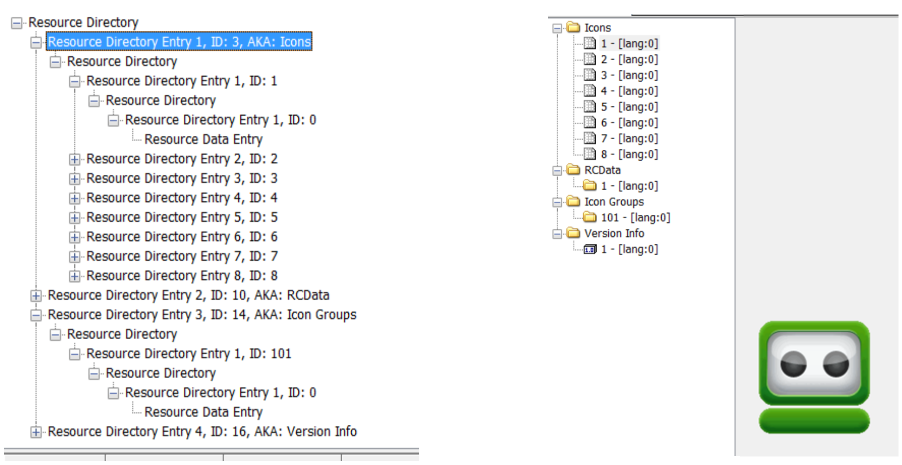
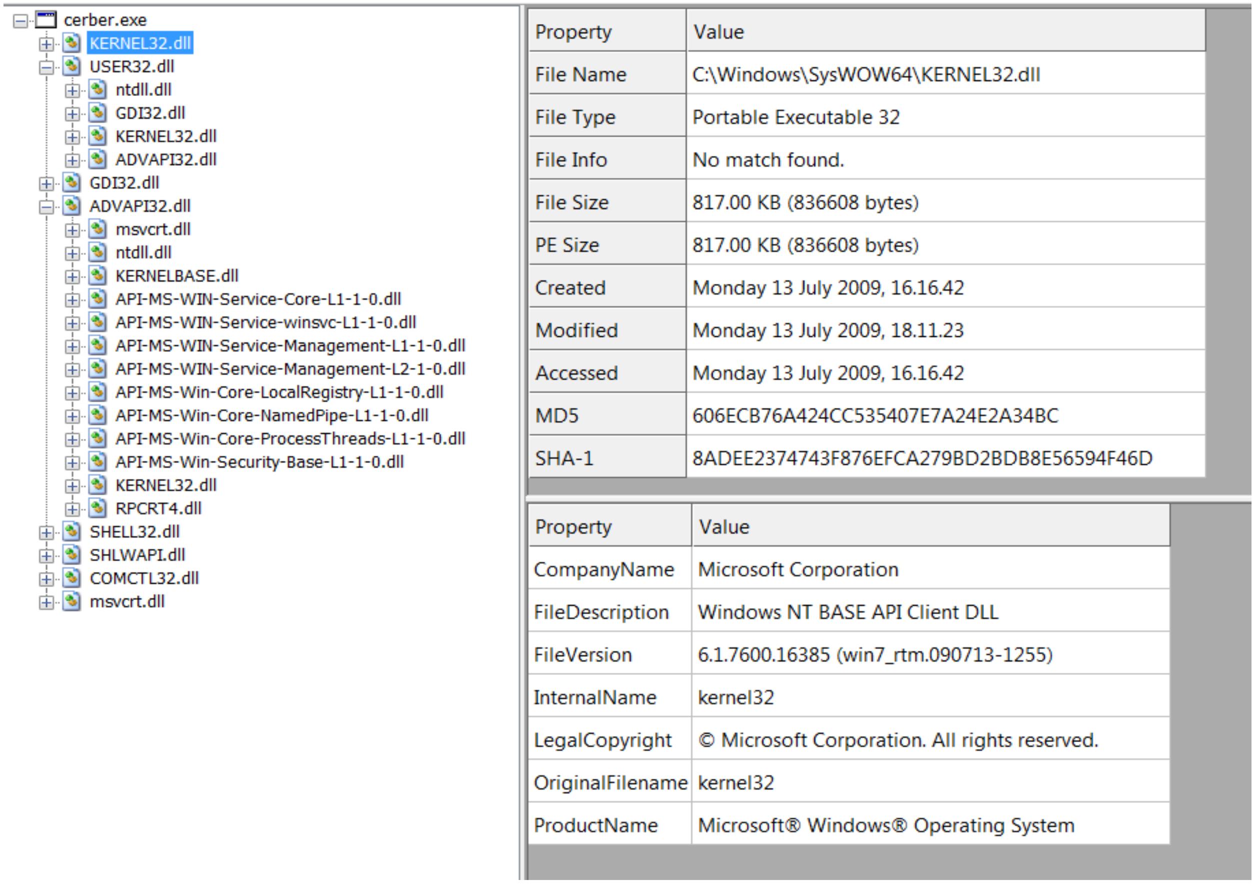


Figure 22

Dependency walker inside CFF Explorer reveals the same information that we saw earlier.



Property	Value
File Name	C:\Windows\SysWOW64\KERNEL32.dll
File Type	Portable Executable 32
File Info	No match found.
File Size	817.00 KB (836608 bytes)
PE Size	817.00 KB (836608 bytes)
Created	Monday 13 July 2009, 16.16.42
Modified	Monday 13 July 2009, 18.11.23
Accessed	Monday 13 July 2009, 16.16.42
MD5	606ECB76A424CC535407E7A24E2A34BC
SHA-1	8ADEE2374743F876EFCA279BD2BDB8E56594F46D

Property	Value
CompanyName	Microsoft Corporation
FileDescription	Windows NT BASE API Client DLL
FileVersion	6.1.7600.16385 (win7_rtm.090713-1255)
InternalName	kernel32
LegalCopyright	© Microsoft Corporation. All rights reserved.
OriginalFilename	kernel32
ProductName	Microsoft® Windows® Operating System

Figure 23

Basic Dynamic Analysis

To understand the behavior of this program, we will use Procmon, Process Explorer, Wireshark, Inetsim and RegShot.
For Procmon, we will use the filter **Process name contains cerber**.

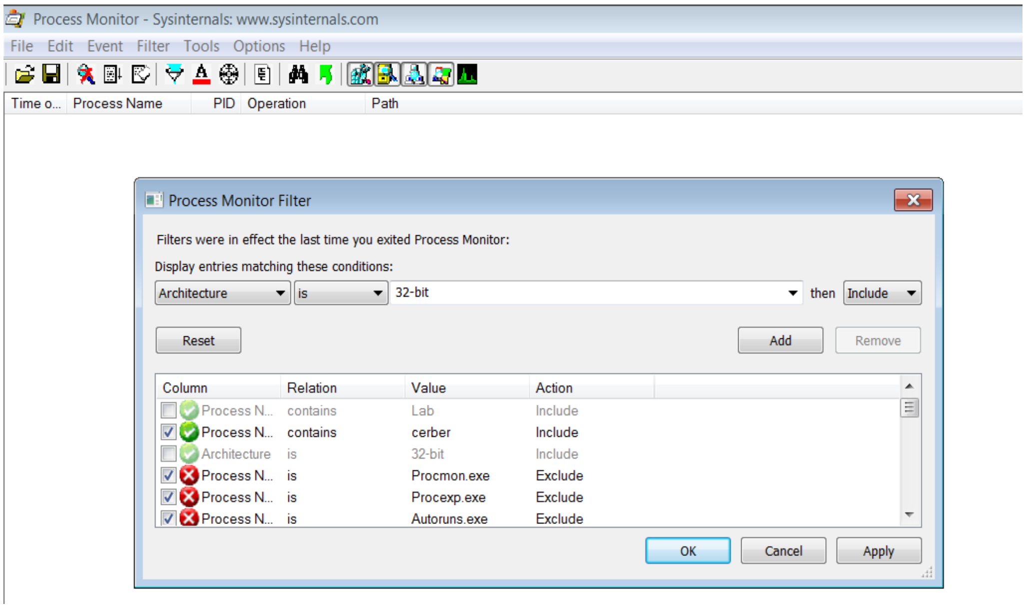


Figure 24

Initially, Process Explorer looks like this:

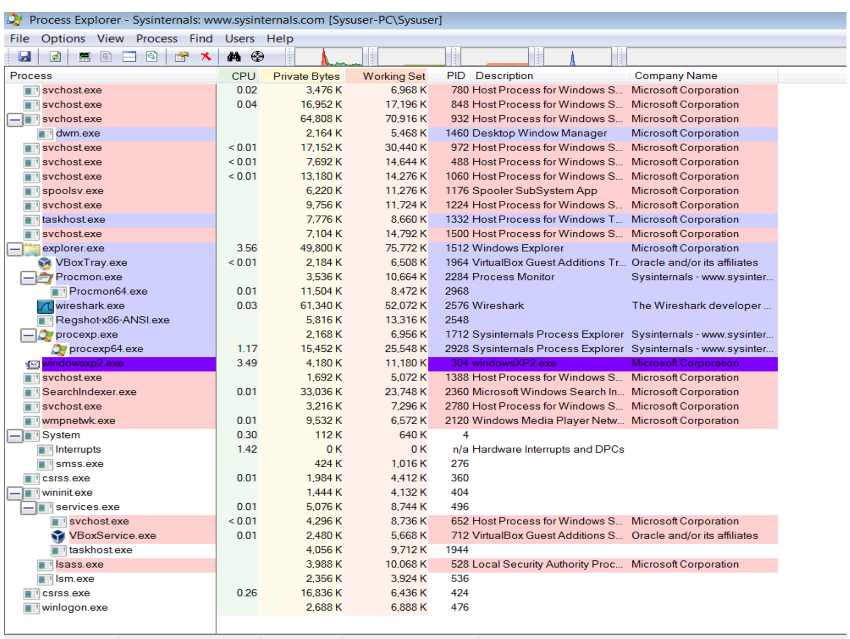


Figure 25

For Wireshark, we will start capturing network traffic on the shown interface.

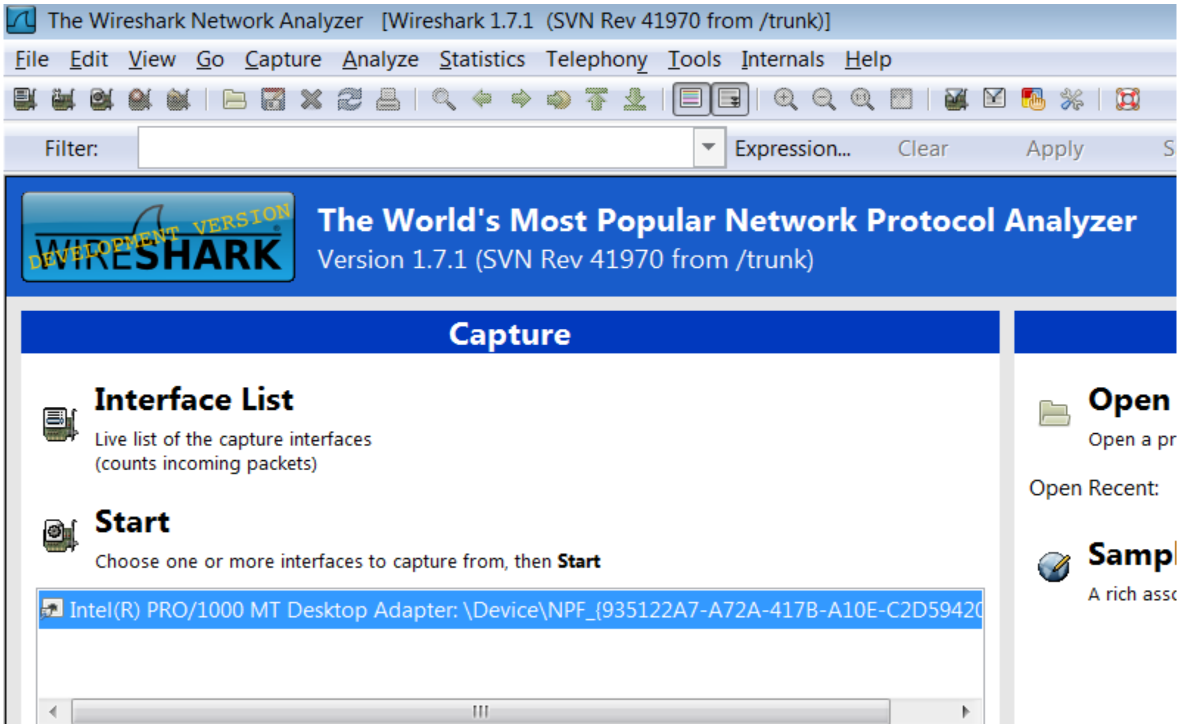


Figure 26

Inetsim is also started on Remnux machine.

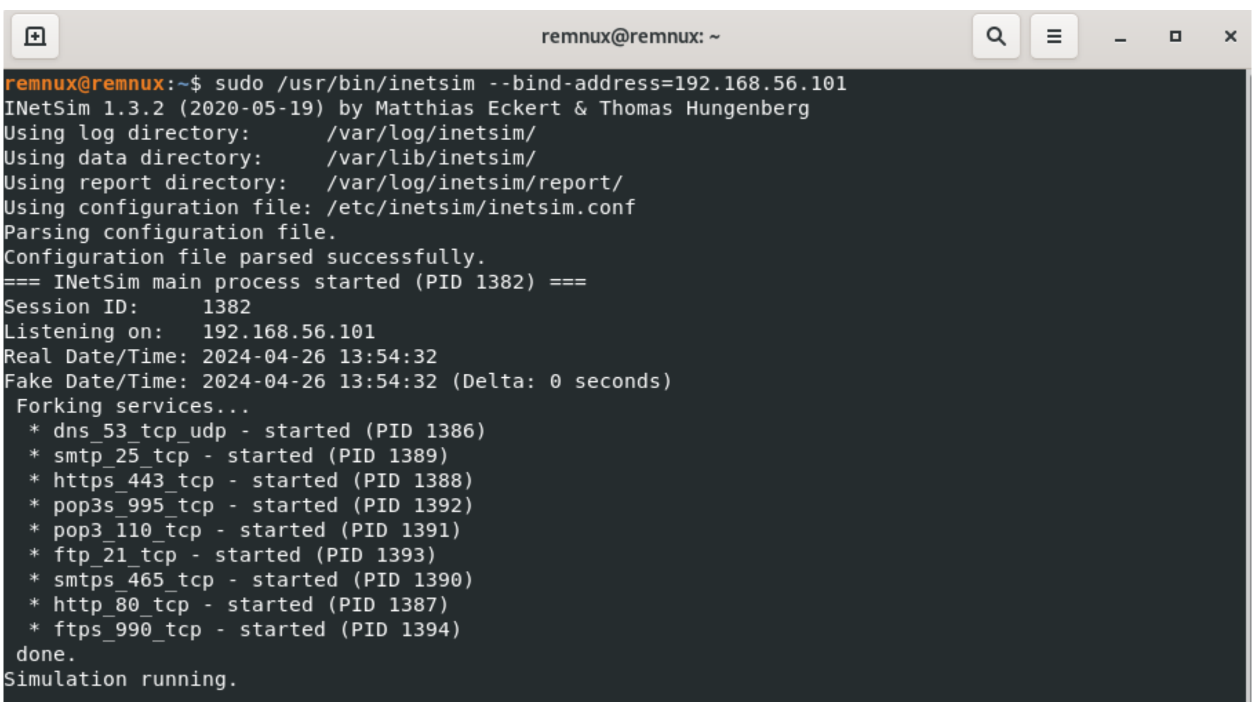


Figure 27

With RegShot, we will take the 1st shot of current registry entries.

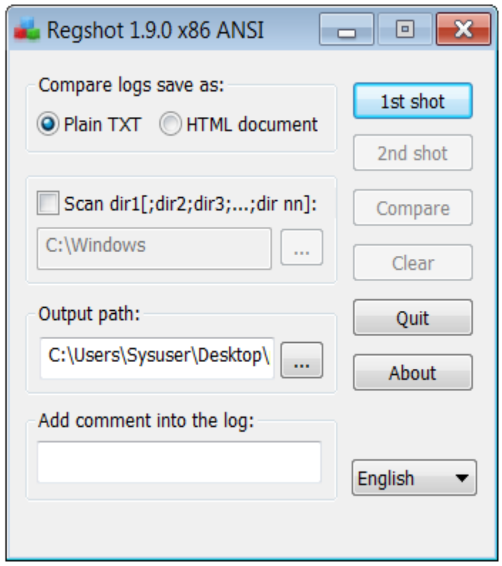


Figure 28

The next step is to run "cerber.exe" file in the virtual machine (after saving a snapshot). Within small amount of time, we see a lot of activities happening in the VM. Below is the screenshot of changes observed in ProcMon, Wireshark and Process Explorer. ProcMon shows that cerber.exe performed a lot of file and registry operations. Multiple network messages were sent through User Datagram Protocol (UDP) as seen in Wireshark. The process id of cerber.exe is 1944 as seen in Process Explorer.

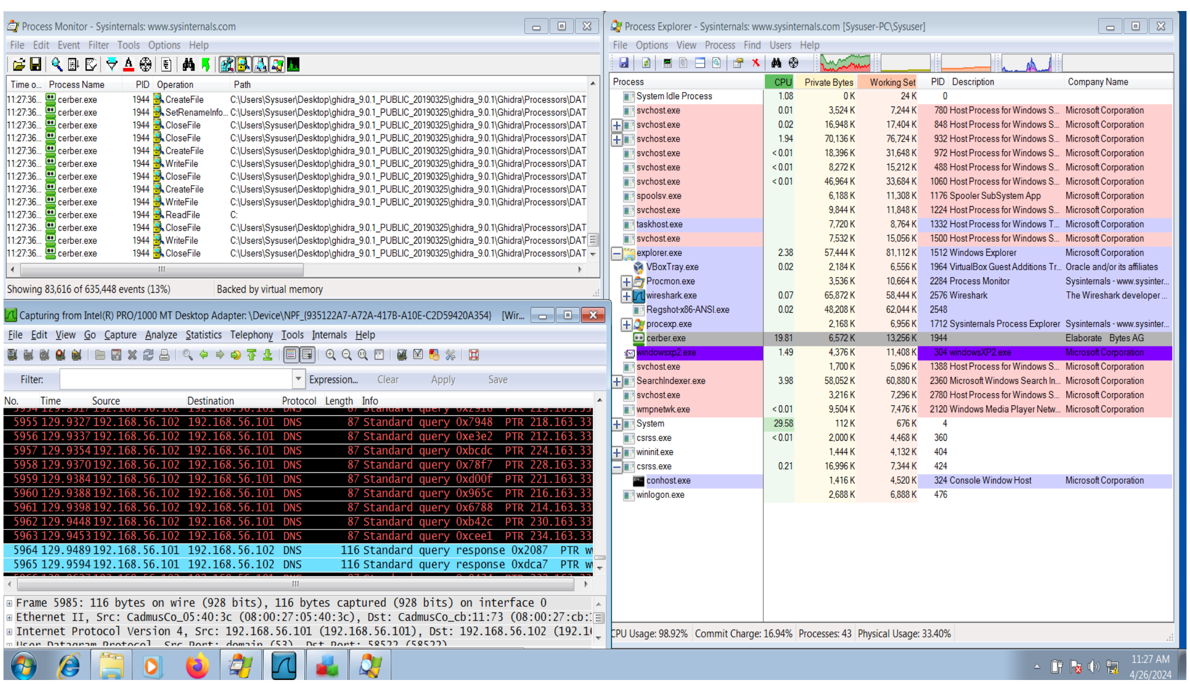
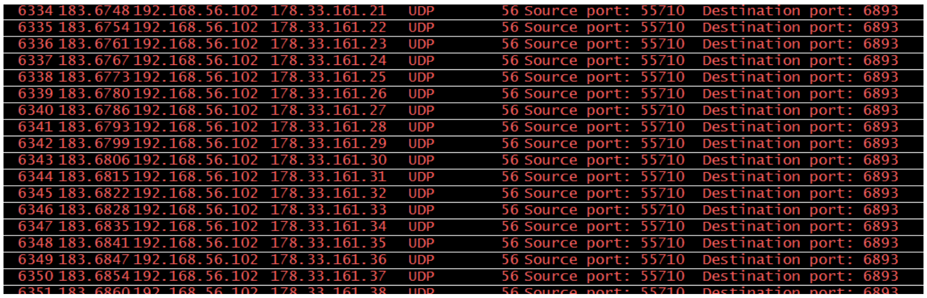


Figure 29

Wireshark logs:



6334	183.6748	192.168.56.102	178.33.161.21	UDP	56	Source port: 55710 Destination port: 6893
6335	183.6754	192.168.56.102	178.33.161.22	UDP	56	Source port: 55710 Destination port: 6893
6336	183.6761	192.168.56.102	178.33.161.23	UDP	56	Source port: 55710 Destination port: 6893
6337	183.6767	192.168.56.102	178.33.161.24	UDP	56	Source port: 55710 Destination port: 6893
6338	183.6773	192.168.56.102	178.33.161.25	UDP	56	Source port: 55710 Destination port: 6893
6339	183.6780	192.168.56.102	178.33.161.26	UDP	56	Source port: 55710 Destination port: 6893
6340	183.6786	192.168.56.102	178.33.161.27	UDP	56	Source port: 55710 Destination port: 6893
6341	183.6793	192.168.56.102	178.33.161.28	UDP	56	Source port: 55710 Destination port: 6893
6342	183.6799	192.168.56.102	178.33.161.29	UDP	56	Source port: 55710 Destination port: 6893
6343	183.6806	192.168.56.102	178.33.161.30	UDP	56	Source port: 55710 Destination port: 6893
6344	183.6815	192.168.56.102	178.33.161.31	UDP	56	Source port: 55710 Destination port: 6893
6345	183.6822	192.168.56.102	178.33.161.32	UDP	56	Source port: 55710 Destination port: 6893
6346	183.6828	192.168.56.102	178.33.161.33	UDP	56	Source port: 55710 Destination port: 6893
6347	183.6835	192.168.56.102	178.33.161.34	UDP	56	Source port: 55710 Destination port: 6893
6348	183.6841	192.168.56.102	178.33.161.35	UDP	56	Source port: 55710 Destination port: 6893
6349	183.6847	192.168.56.102	178.33.161.36	UDP	56	Source port: 55710 Destination port: 6893
6350	183.6854	192.168.56.102	178.33.161.37	UDP	56	Source port: 55710 Destination port: 6893
6351	183.6860	192.168.56.102	178.33.161.38	UDP	56	Source port: 55710 Destination port: 6893

Figure 30

Example UDP messages:

The program sends multiple UDP requests (25 bytes data) from port 51909 to 178.33.158.x at port 6893. Message content is aa9df958a4d50446 and 97100015d.

No.	Time	Source	Destination	Protocol	Length	Info
32	116.387863000	192.168.56.102	178.33.158.0	UDP	67	Source port: 51909 Destination port: 6893

Frame 32: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: CadmusCo_cb:11:73 (08:00:27:cb:11:73), Dst: CadmusCo_05:40:3c (08:00:27:05:40:3c)
Internet Protocol Version 4, Src: 192.168.56.102 (192.168.56.102), Dst: 178.33.158.0 (178.33.158.0)
User Datagram Protocol, Src Port: 51909 (51909), Dst Port: 6893 (6893)
Data (25 bytes)

```
0000  61 61 39 64 66 39 35 38 61 34 64 35 30 34 34 36   aa9df958a4d50446
0010  39 37 31 30 30 30 31 35 64                        97100015d
```

(A)

No.	Time	Source	Destination	Protocol	Length	Info
33	116.389353000	192.168.56.102	178.33.158.1	UDP	67	Source port: 51909 Destination port: 6893

Frame 33: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
Ethernet II, Src: CadmusCo_cb:11:73 (08:00:27:cb:11:73), Dst: CadmusCo_05:40:3c (08:00:27:05:40:3c)
Internet Protocol Version 4, Src: 192.168.56.102 (192.168.56.102), Dst: 178.33.158.1 (178.33.158.1)
User Datagram Protocol, Src Port: 51909 (51909), Dst Port: 6893 (6893)
Data (25 bytes)

```
0000  61 61 39 64 66 39 35 38 61 34 64 35 30 34 34 36   aa9df958a4d50446
0010  39 37 31 30 30 30 31 35 64                        97100015d
```

(B)

Figure 31

Later, it sends multiple UDP requests (14 bytes data) to the same destinations and port 6893 from another source port 55710. Message content is aa9df958a4d5a2. It looks like it is sending these messages to its control server.

No.	Time	Source	Destination	Protocol	Length	Info
6019	182.130470000	192.168.56.102	178.33.158.26	UDP	56	Source port: 55710 Destination port: 6893

Frame 6019: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
Ethernet II, Src: CadmusCo_cb:11:73 (08:00:27:cb:11:73), Dst: CadmusCo_05:40:3c (08:00:27:05:40:3c)
Internet Protocol Version 4, Src: 192.168.56.102 (192.168.56.102), Dst: 178.33.158.26 (178.33.158.26)
User Datagram Protocol, Src Port: 55710 (55710), Dst Port: 6893 (6893)
Data (14 bytes)

0000 61 61 39 64 66 39 35 38 61 34 64 35 61 32   aa9df958a4d5a2

(A)

No.	Time	Source	Destination	Protocol	Length	Info
6020	182.134896000	192.168.56.102	178.33.158.27	UDP	56	Source port: 55710 Destination port: 6893

Frame 6020: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
Ethernet II, Src: CadmusCo_cb:11:73 (08:00:27:cb:11:73), Dst: CadmusCo_05:40:3c (08:00:27:05:40:3c)
Internet Protocol Version 4, Src: 192.168.56.102 (192.168.56.102), Dst: 178.33.158.27 (178.33.158.27)
User Datagram Protocol, Src Port: 55710 (55710), Dst Port: 6893 (6893)
Data (14 bytes)

0000 61 61 39 64 66 39 35 38 61 34 64 35 61 32   aa9df958a4d5a2

(B)

Figure 32

Though there are multiple entries in ProcMon network logs, only two of them are unique and confirm our observation:

Operation	Path	Result	Detail
UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
UDP Send	Sysuser-PC:55710 -> www.inetsim.org:6893	SUCCESS	Length: 14, seqnum: 0, connid: 0

Figure 33

Inetsim logs indicate that after the UDP messages, some websites are called:

- api.blockcypher.com: http://api.blockcypher.com/v1/btc/main/addrs/17gd1mspFnMcEMF1MitTNSsYs7w7AQyct?_=1714156121538
- btc.blockr.io: http://btc.blockr.io/api/v1/address/txs/17gd1mspFnMcEMF1MitTNSsYs7w7AQyct?_=1714156121538
- bitaps.com
- chain.so

```
2024-04-26 14:29:12  DNS connection, type: PTR, class: IN, requested name: 234.163.33.178.in-addr.arpa
2024-04-26 14:29:12  DNS connection, type: PTR, class: IN, requested name: 232.163.33.178.in-addr.arpa
2024-04-26 14:30:11  DNS connection, type: A, class: IN, requested name: api.blockcypher.com
2024-04-26 14:30:11  HTTP connection, method: GET, URL: http://api.blockcypher.com/v1/btc/main/addrs/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt?_=1714156121538, file name:
/var/lib/inetsim/http/fakefiles/sample.html
2024-04-26 14:30:11  DNS connection, type: A, class: IN, requested name: btc.blockr.io
2024-04-26 14:30:11  HTTP connection, method: GET, URL: http://btc.blockr.io/api/v1/address/txs/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt?_=1714156122077, file name:
/var/lib/inetsim/http/fakefiles/sample.html
2024-04-26 14:30:11  DNS connection, type: A, class: IN, requested name: bitaps.com
2024-04-26 14:30:11  DNS connection, type: A, class: IN, requested name: chain.so
```

Figure 34

Similar logs are observed in Wireshark:

```
No.     Time          Source             Destination         Protocol Length Info
   7098 189.293822000 192.168.56.102     192.168.56.101      HTTP     403    GET /api/v1/address/txs/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt?_=1714156122077 HTTP/1.1

Frame 7098: 403 bytes on wire (3224 bits), 403 bytes captured (3224 bits) on interface 0
Ethernet II, Src: CadmusCo_cb:11:73 (08:00:27:cb:11:73), Dst: CadmusCo_05:40:3c (08:00:27:05:40:3c)
Internet Protocol Version 4, Src: 192.168.56.102 (192.168.56.102), Dst: 192.168.56.101 (192.168.56.101)
Transmission Control Protocol, Src Port: 49225 (49225), Dst Port: http (80), Seq: 1, Ack: 1, Len: 349
Hypertext Transfer Protocol
```

```
No.     Time          Source             Destination         Protocol Length Info
   7086 189.239018000 192.168.56.102     192.168.56.101      HTTP     408    GET /v1/btc/main/addrs/17gd1msp5FnMcEMF1MitTNSsYs7w7AQyCt?_=1714156121538 HTTP/1.1

Frame 7086: 408 bytes on wire (3264 bits), 408 bytes captured (3264 bits) on interface 0
Ethernet II, Src: CadmusCo_cb:11:73 (08:00:27:cb:11:73), Dst: CadmusCo_05:40:3c (08:00:27:05:40:3c)
Internet Protocol Version 4, Src: 192.168.56.102 (192.168.56.102), Dst: 192.168.56.101 (192.168.56.101)
Transmission Control Protocol, Src Port: 49224 (49224), Dst Port: http (80), Seq: 1, Ack: 1, Len: 354
Hypertext Transfer Protocol
```

Figure 35

1714156121538: This number is the current UNIX time stamp of the infected system.

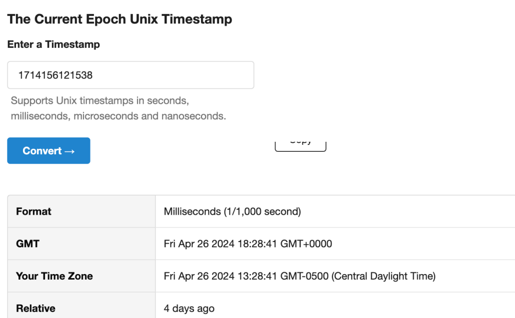


Figure 36

After the program finishes, we see that a notepad document and a .hta page opens.

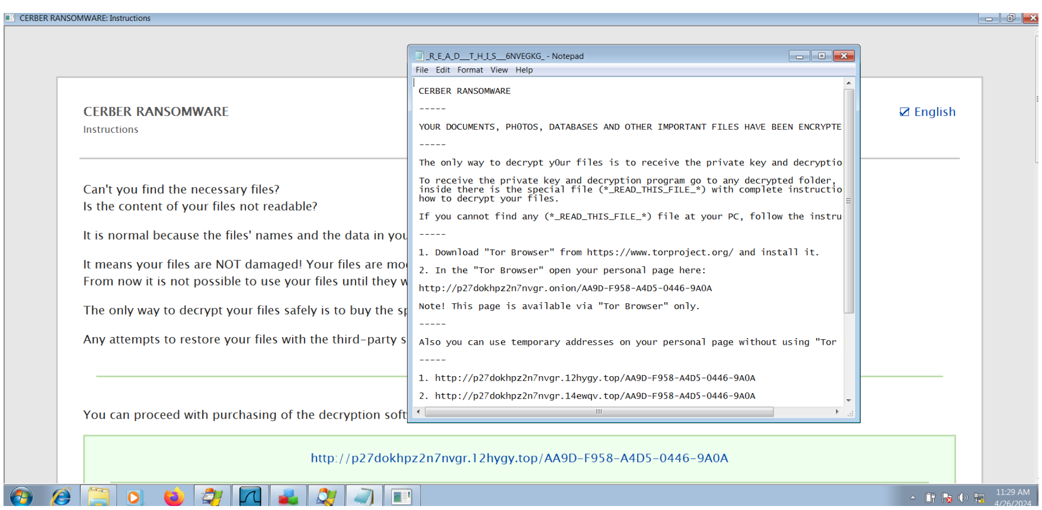
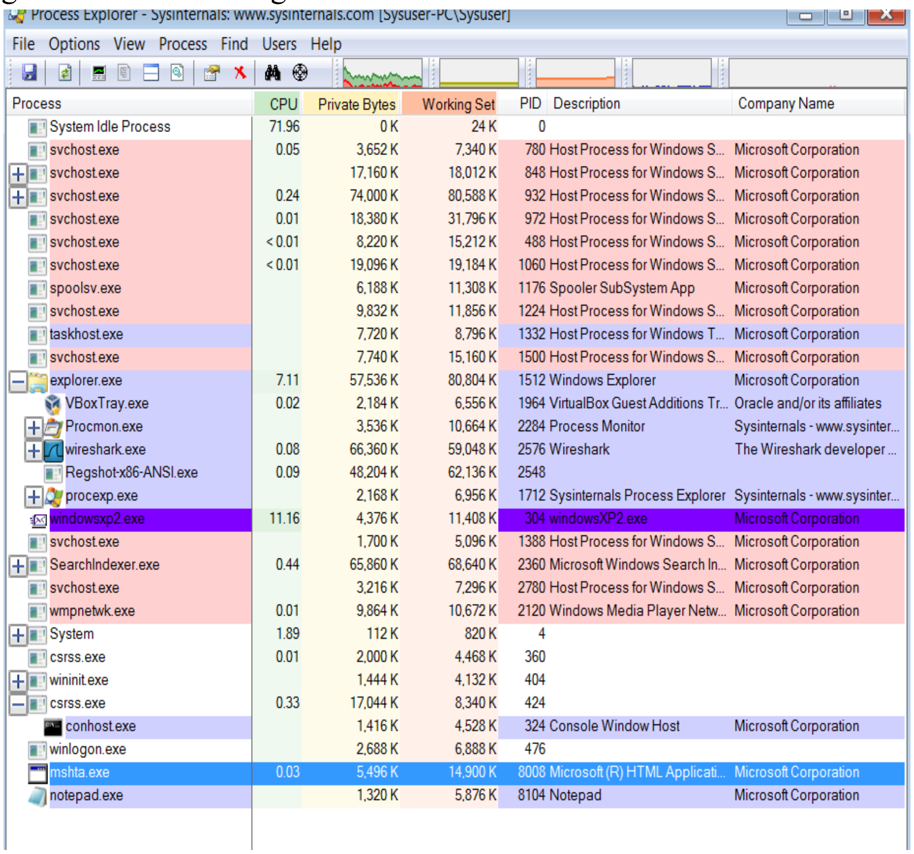


Figure 37

Process Explorer shows that two new processes started – mshta.exe and notepad.exe. The desktop background has also changed.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	71.96	0 K	24 K	0		
svchost.exe	0.05	3,652 K	7,340 K	780	Host Process for Windows S...	Microsoft Corporation
svchost.exe		17,160 K	18,012 K	848	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.24	74,000 K	80,588 K	932	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	18,380 K	31,796 K	972	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	8,220 K	15,212 K	488	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	19,096 K	19,184 K	1060	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		6,188 K	11,308 K	1176	Spooler SubSystem App	Microsoft Corporation
svchost.exe		9,832 K	11,856 K	1224	Host Process for Windows S...	Microsoft Corporation
taskhost.exe		7,720 K	8,796 K	1332	Host Process for Windows T...	Microsoft Corporation
svchost.exe		7,740 K	15,160 K	1500	Host Process for Windows S...	Microsoft Corporation
explorer.exe	7.11	57,536 K	80,804 K	1512	Windows Explorer	Microsoft Corporation
VBoxTray.exe	0.02	2,184 K	6,556 K	1964	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
Procmon.exe		3,536 K	10,664 K	2284	Process Monitor	Sysinternals - www.sysinter...
wireshark.exe	0.08	66,360 K	59,048 K	2576	Wireshark	The Wireshark developer ...
Regshot-x86-ANSI.exe	0.09	48,204 K	62,136 K	2548		
procexp.exe		2,168 K	6,956 K	1712	Sysinternals Process Explorer	Sysinternals - www.sysinter...
windowsxp2.exe	11.16	4,376 K	11,408 K	304	windowsXP2.exe	Microsoft Corporation
svchost.exe		1,700 K	5,096 K	1388	Host Process for Windows S...	Microsoft Corporation
SearchIndexer.exe	0.44	65,860 K	68,640 K	2360	Microsoft Windows Search In...	Microsoft Corporation
svchost.exe		3,216 K	7,296 K	2780	Host Process for Windows S...	Microsoft Corporation
wmpnetwk.exe	0.01	9,864 K	10,672 K	2120	Windows Media Player Netw...	Microsoft Corporation
System	1.89	112 K	820 K	4		
csrss.exe	0.01	2,000 K	4,468 K	360		
wininit.exe		1,444 K	4,132 K	404		
csrss.exe	0.33	17,044 K	8,340 K	424		
conhost.exe		1,416 K	4,528 K	324	Console Window Host	Microsoft Corporation
winlogon.exe		2,688 K	6,888 K	476		
mshta.exe	0.03	5,496 K	14,900 K	8008	Microsoft (R) HTML Applicati...	Microsoft Corporation
notepad.exe		1,320 K	5,876 K	8104	Notepad	Microsoft Corporation

Figure 38

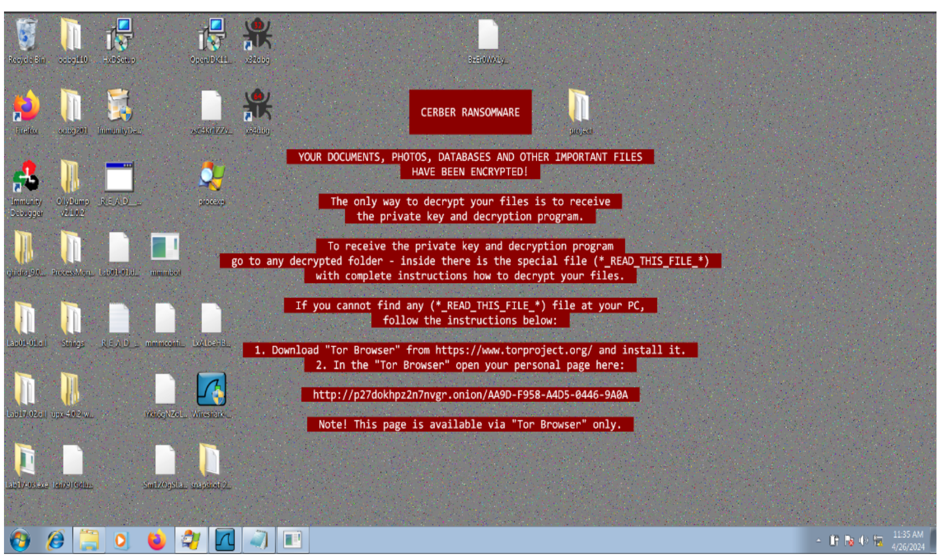


Figure 39

Files have been encrypted and have weird extensions:

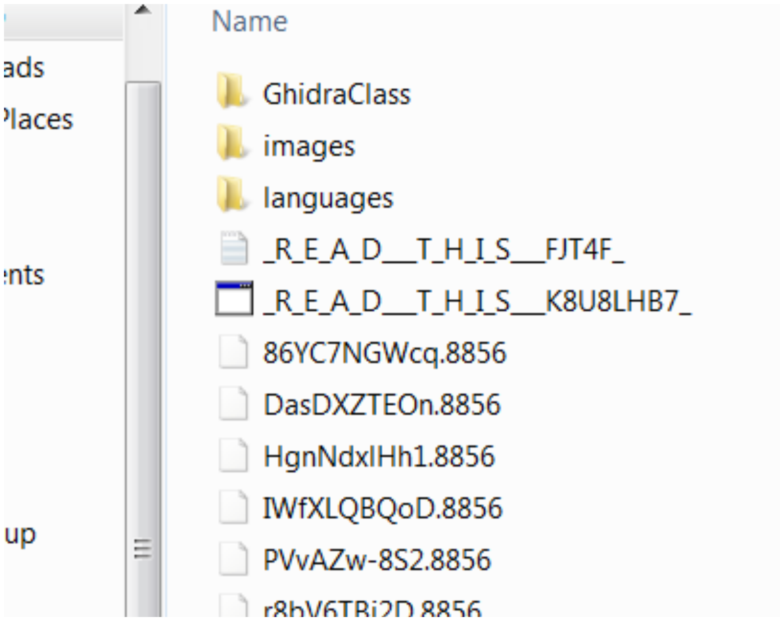


Figure 40

The file cerber.exe is no longer present in its original location.

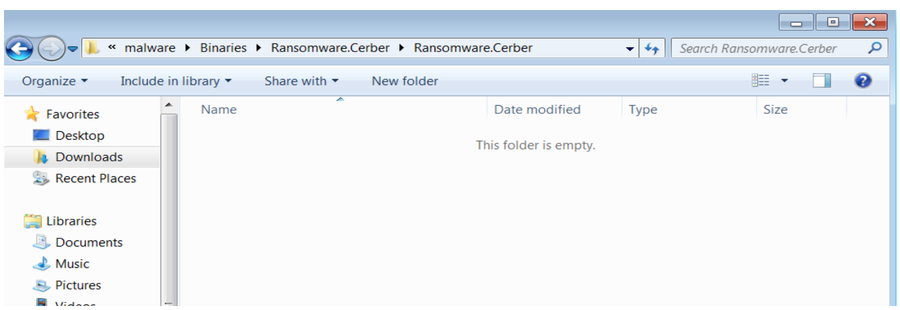


Figure 41

Registry changes

Regshot comparison shows that 10 keys are added, 43 values are added, 31 values are modified, a total of 84 changes are made.

```
----------------------------------
Keys added: 10
----------------------------------
HKLM\SOFTWARE\Microsoft\Tracing\mshta_RASAPI32
HKLM\SOFTWARE\Microsoft\Tracing\mshta_RASMANCS
HKU\S-1-5-21-4256571159-2166413623-464567181-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMRU\hiv
HKU\S-1-5-21-4256571159-2166413623-464567181-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv
HKU\S-1-5-21-4256571159-2166413623-464567181-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.hiv\OpenWithList
HKU\S-1-5-21-4256571159-2166413623-464567181-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.hiv
HKU\S-1-5-21-4256571159-2166413623-464567181-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\149\ComDlg
HKU\S-1-5-21-4256571159-2166413623-464567181-1000\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\149\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
HKU\S-1-5-21-4256571159-2166413623-464567181-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\149\ComDlg
HKU\S-1-5-21-4256571159-2166413623-464567181-1000_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\149\ComDlg\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}
```

Figure 42

The first two registry keys are tracing settings which are created the first time an application interacts with Remote Access API (rasapi32.dll) and has attempted network connections. Note that this DLL was not found in our basic static analysis which confirms that the actual malware is hiding somewhere. The next 4 keys are related to .hiv files (created when we saved 1st shot backup). The remaining registry keys are related to shell bags which are used to store information about view settings of a folder for a specific user profile. Overall, it doesn't look like our program cerber.exe is creating any significant registry key.

Out of the 43 values added, two interesting ones are

- HKU\.DEFAULT\Software\Classes\Local Settings\MuiCache\3\52C64B7E\@C:\Windows\System32\mshta.exe
- HKU\S-1-5-18\Software\Classes\Local Settings\MuiCache\3\52C64B7E\@C:\Windows\System32\mshta.exe

These likely contain information related to the Multi-Language User Interface cache for the "mshta.exe" file, which is a component of the Windows operating system used to execute HTML applications. This application was started after cerber.exe was executed as we saw earlier.

There are two values which are unusual:

```
HKU\S-1-5-21-4256571159-2166413623-464567181-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Flfhfre\Qbjaybnqf\gurMbb-znfgre\gurMbb-znfgre\znyjner\Ovanevrf\Enafbzjner.Preore\Enafbzjner.Preore\preore.rkr:    00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 60 40 53 4F 07 98 DA 01 00 00 00 00
```

HKU\S-1-5-21-4256571159-2166413623-464567181-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\{Q65231O0-O2S1-4857-N4PR-N8R7P6RN7Q27}\abgrcnq.rkr: 00 00 00 00 00 00 00 00 01 00 00 00 B3 74 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00

The paths P:\Hfref\Flfhfre\Qbjaybnqf\gurMbb-znfgre\gurMbb-znfgre\znyjner\Ovanevrf\Enafbzjner.Preore\Enafbzjner.Preore\preore.rkr and abgrcnq.rkr are obfuscated. Noting the pattern, the first path looks like a cipher for C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master\malware\Binaries\Ransomware.Cerber\Ransomware.Cerber\cerber.exe and second looks like a cipher for notepad.exe. The other registry values do not seem important.

Original:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Encrypted:	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

Figure 43

ProcMon

Below is a summary of registry logs obtained from ProcMon. Screenshots present in Appendix A:

Count of Operation	Column Labels							
Row Labels	ACCESS DENIED	BUFFER OVERFLOW	BUFFER TOO SMALL	NAME NOT FOUND	NO MORE ENTRIES	REPARSE	SUCCESS	Grand Total
RegCloseKey							908	908
RegCreateKey	2					2		4
RegDeleteValue	4			4				8
RegEnumKey					14		44	58
RegEnumValue					27		47	74
RegOpenKey	1			1763		152	908	2824
RegQueryKey			15				3723	3738
RegQueryKeySecurity			1				1	2
RegQueryValue		49		799			874	1722
RegSetInfoKey							587	587
RegSetValue							8	8
Grand Total	**7**	**49**	**16**	**2566**	**41**	**154**	**7100**	**9933**

Figure 44

It looks like the program performs query, open, close, and set operations on multiple registry keys. It also tries to create key in path HKLM\System\CurrentControlSet\Control\Session Manager but gets Access Denied error. It tries to delete some values related to Internet settings but either gets access denied error or name not found error.

Time of Day	Process Name	PID	Operation	Path	Result	Detail
11:28:04	cerber.exe	1944	RegCreateKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Read/Write
11:28:04	cerber.exe	1944	RegCreateKey	HKLM\System\CurrentControlSet\Control\Session Manager	ACCESS DENIE	Desired Access: Read/Write
11:28:04	cerber.exe	1944	RegCreateKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Read/Write
11:28:04	cerber.exe	1944	RegCreateKey	HKLM\System\CurrentControlSet\Control\Session Manager	ACCESS DENIE	Desired Access: Read/Write

Operation	Path	Result
RegDeleteValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	NAME NOT FOUND
RegDeleteValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	ACCESS DENIED
RegDeleteValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	NAME NOT FOUND
RegDeleteValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	ACCESS DENIED
RegDeleteValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	NAME NOT FOUND
RegDeleteValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass	ACCESS DENIED
RegDeleteValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	NAME NOT FOUND
RegDeleteValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName	ACCESS DENIED

Figure 45

The program also enumerates registry keys under certain paths to gather information:

Operation	Path
RegEnumKey	HKLM\System\CurrentControlSet\Control\MUI\UILanguages
RegEnumKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\ProfileList
RegEnumKey	HKCR\Drive\shellex\FolderExtensions
RegEnumKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderTypes\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\TopViews
RegEnumKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderTypes\{7FDE1A1E-8B31-49A5-93B8-6BE14CFA4943}\TopViews
RegEnumKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderTypes\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\TopViews
RegEnumKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderTypes\{FBB3477E-C9E4-4B3B-A2BA-D3F5D3CD46F9}\TopViews
RegEnumKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback
RegEnumKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
RegEnumKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown_Zones

Figure 46

It also enumerates registry values under certain paths to gather information related to file associations, language settings and explorer configurations.

Operation	Path
RegEnumValue	HKLM\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration
RegEnumValue	HKCU\Control Panel\Desktop\LanguageConfiguration
RegEnumValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderTypes\{5C4F28B5-F869-4E84-8E60-F11DB97C5CC7}\Modifiers
RegEnumValue	HKCU\Software\Classes\.pdf\OpenWithProgids
RegEnumValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.pdf\OpenWithProgids
RegEnumValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt\OpenWithProgids
RegEnumValue	HKCR\.zip\OpenWithProgids
RegEnumValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.zip\OpenWithProgids
RegEnumValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.dll\OpenWithProgids
RegEnumValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.ini\OpenWithProgids
RegEnumValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderTypes\{7D49D726-3C21-4F05-99AA-FDC2C9474656}\Modifiers
RegEnumValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.msu\OpenWithProgids
RegEnumValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProtocolDefaults

Figure 47

The first attempt to query the security descriptor of the HKCU\Network registry key failed due to insufficient buffer size while the second attempt to query the security descriptor of the HKCU\Control Panel\Desktop registry key was successful.

Operation	Path	Result
RegQueryKeySecurity	HKCU\Network	BUFFER TOO SMALL
RegQueryKeySecurity	HKCU\Control Panel\Desktop	SUCCESS

Figure 47

Using the RegSetInfoKey operation, the program sets information about various registry keys related to file extensions and explorer settings.

RegSetInfoKey	HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Policies\Explorer	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Policies\Explorer	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\Drive\shellex\FolderExtensions	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Policies\Explorer	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Policies\Explorer	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.hta	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.hta	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\htafile	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\Explorer\KindMap	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.hta	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.hta	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\htafile	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.hta	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.asp	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.bas	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.bat	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.cer	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.chm	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.cmd	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.com	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.cpl	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.crt	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.exe	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.gadget	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.grp	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\.hlp	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCR\Wow6432Node\CLSID\{7B8A2D94-0AC9-11D1-896C-00C04FB6BFC4}	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegSetInfoKey	HKCU\Software\Classes	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0

Figure 48

It also uses RegSetValue operation to modify language settings, security zone settings for intranet resources accessed via UNC paths and AutoDetect internet settings. It also sets the desktop wallpaper registry value to a file located in "C:\Users\Sysuser\AppData\Local\Temp\tmpE33C.bmp" path (we saw the desktop wallpaper change earlier).

Operation	Path	Result	Detail
RegSetValue	HKCU\Software\Classes\Local Settings\MuiCache\3\52C64B7E\LanguageList	SUCCESS	Type: REG_MULTI_SZ, Length: 20, Data: en-US, en
RegSetValue	HKCU\Software\Classes\Local Settings\MuiCache\3\52C64B7E\LanguageList	SUCCESS	Type: REG_MULTI_SZ, Length: 20, Data: en-US, en
RegSetValue	HKCU\Software\Classes\Local Settings\MuiCache\3\52C64B7E\LanguageList	SUCCESS	Type: REG_MULTI_SZ, Length: 20, Data: en-US, en
RegSetValue	HKCU\Control Panel\Desktop\Wallpaper	SUCCESS	Type: REG_SZ, Length: 96, Data: C:\Users\Sysuser\AppData\Local\Temp\tmpE33C.bmp
RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1

Figure 49

ProcMon logs for processes show that total 85 DLLs are loaded by cerber.exe which is quite high from the number of DLLs that we saw during static analysis.

Table 2

C:\Windows\System32\kernel32.dll	*C:\Windows\SysWOW64\cscapi.dll*	*C:\Windows\SysWOW64\msasn1.dll*
C:\Windows\System32\ntdll.dll	*C:\Windows\SysWOW64\davclnt.dll*	*C:\Windows\SysWOW64\msctf.dll*
C:\Windows\System32\user32.dll	*C:\Windows\SysWOW64\davhlpr.dll*	*C:\Windows\SysWOW64\mshta.exe*
C:\Windows\System32\wow64.dll	*C:\Windows\SysWOW64\devobj.dll*	*C:\Windows\SysWOW64\msvcrt.dll*
C:\Windows\System32\wow64cpu.dll	*C:\Windows\SysWOW64\drprov.dll*	*C:\Windows\SysWOW64\mswsock.dll*
C:\Windows\System32\wow64win.dll	*C:\Windows\SysWOW64\dwmapi.dll*	*C:\Windows\SysWOW64\netapi32.dll*
C:\Windows\SysWOW64\advapi32.dll	*C:\Windows\SysWOW64\gdi32.dll*	*C:\Windows\SysWOW64\netutils.dll*
C:\Windows\SysWOW64\apphelp.dll	*C:\Windows\SysWOW64\IconCodecService.dll*	*C:\Windows\SysWOW64\notepad.exe*
C:\Windows\SysWOW64\browcli.dll		*C:\Windows\SysWOW64\nsi.dll*
C:\Windows\SysWOW64\cfgmgr32.dll	*C:\Windows\SysWOW64\iertutil.dll*	*C:\Windows\SysWOW64\ntdll.dll*
C:\Windows\SysWOW64\clbcatq.dll	*C:\Windows\SysWOW64\imm32.dll*	*C:\Windows\SysWOW64\ntlanman.dll*
C:\Windows\SysWOW64\cmd.exe	*C:\Windows\SysWOW64\kernel32.dll*	*C:\Windows\SysWOW64\ntmarta.dll*
C:\Windows\SysWOW64\comctl32.dll	*C:\Windows\SysWOW64\KernelBase.dll*	*C:\Windows\SysWOW64\ole32.dll*
C:\Windows\SysWOW64\crypt32.dll	*C:\Windows\SysWOW64\linkinfo.dll*	*C:\Windows\SysWOW64\oleaut32.dll*
C:\Windows\SysWOW64\cryptbase.dll	*C:\Windows\SysWOW64\lpk.dll*	*C:\Windows\SysWOW64\powrprof.dll*
C:\Windows\SysWOW64\cryptsp.dll	*C:\Windows\SysWOW64\mpr.dll*	*C:\Windows\SysWOW64\profapi.dll*

C:\Windows\SysWOW64\propsys.dll	*C:\Windows\SysWOW64\shell32.dll*	*C:\Windows\SysWOW64\version.dll*
C:\Windows\SysWOW64\rpcrt4.dll	*C:\Windows\SysWOW64\shlwapi.dll*	*C:\Windows\SysWOW64\WindowsCodecs.dll*
C:\Windows\SysWOW64\RpcRtRemote.dll	*C:\Windows\SysWOW64\srvcli.dll*	*C:\Windows\SysWOW64\winsta.dll*
C:\Windows\SysWOW64\rsaenh.dll	*C:\Windows\SysWOW64\sspicli.dll*	*C:\Windows\SysWOW64\wkscli.dll*
C:\Windows\SysWOW64\samcli.dll	*C:\Windows\SysWOW64\urlmon.dll*	*C:\Windows\SysWOW64\Wldap32.dll*
C:\Windows\SysWOW64\SearchFolder.dll	*C:\Windows\SysWOW64\user32.dll*	*C:\Windows\SysWOW64\ws2_32.dll*
C:\Windows\SysWOW64\sechost.dll	*C:\Windows\SysWOW64\usp10.dll*	*C:\Windows\SysWOW64\WSHTCPIP.DLL*
C:\Windows\SysWOW64\setupapi.dll	*C:\Windows\SysWOW64\uxtheme.dll*	
C:\Windows\SysWOW64\shdocvw.dll	*C:\Windows\SysWOW64\VBoxMRXNP.dll*	
C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master\malware\Binaries\Ransomware.Cerber\Ransomware.Cerber\cerber.exe		
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll		
C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf861225ca\GdiPlus.dll		

ProcMon process logs further show that three processes are created by cerber.exe, this matches our observation in ProcExplorer. mshta.exe displays the .hta file and notepad.exe displays the ransom note after execution completes. cmd.exe is also created but the reasons are not clear.

Operation	Path	Result	Detail
Process Create	C:\Windows\SysWOW64\mshta.exe	SUCCESS	PID: 8008, Command line: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\Sysuser\Desktop_R_E_A_D___T_H_I_S___0078DKZV_.hta"
Process Create	C:\Windows\SysWOW64\NOTEPAD.EXE	SUCCESS	PID: 8104, Command line: "C:\Windows\system32\NOTEPAD.EXE" C:\Users\Sysuser\Desktop_R_E_A_D___T_H_I_S___6NVEGKG_.txt
Process Create	C:\Windows\SysWOW64\cmd.exe	SUCCESS	PID: 5616, Command line: "C:\Windows\system32\cmd.exe"

Figure 50

The program exit status is 0 (no error) and it took only 1.18 seconds of user time and 7.04 seconds of kernel time to encrypt the entire file system.

Process Name	PID	Operation	Result	Detail
cerber.exe	1944	Process Exit	SUCCESS	Exit Status: 0, User Time: 1.1875000 seconds, Kernel Time: 7.0468750 seconds, Private Bytes: 6,656,000, Peak Private Bytes: 28,659,712, Working Set: 14,622,720, Peak Working Set: 36,003,840

Figure 51

The program creates 18 threads in total and successfully exits from all the threads within a very less amount of time:

Operation	Path	Result	Detail
Thread Create		SUCCESS	Thread ID: 2876
Thread Create		SUCCESS	Thread ID: 1612
Thread Create		SUCCESS	Thread ID: 8084
Thread Create		SUCCESS	Thread ID: 8092
Thread Create		SUCCESS	Thread ID: 8100
Thread Create		SUCCESS	Thread ID: 8108
Thread Create		SUCCESS	Thread ID: 8116
Thread Create		SUCCESS	Thread ID: 8124
Thread Create		SUCCESS	Thread ID: 4804
Thread Create		SUCCESS	Thread ID: 7872
Thread Create		SUCCESS	Thread ID: 7888
Thread Create		SUCCESS	Thread ID: 4708
Thread Create		SUCCESS	Thread ID: 3136
Thread Create		SUCCESS	Thread ID: 8096
Thread Create		SUCCESS	Thread ID: 4816
Thread Create		SUCCESS	Thread ID: 4860
Thread Create		SUCCESS	Thread ID: 8120
Thread Create		SUCCESS	Thread ID: 5592

(A)

Operation	Path	Result	Detail
Thread Exit		SUCCESS	Thread ID: 4804, User Time: 0.0156250, Kernel Time: 0.1093750
Thread Exit		SUCCESS	Thread ID: 7888, User Time: 0.2187500, Kernel Time: 2.0937500
Thread Exit		SUCCESS	Thread ID: 4708, User Time: 0.2656250, Kernel Time: 1.5156250
Thread Exit		SUCCESS	Thread ID: 3136, User Time: 0.0000000, Kernel Time: 0.0312500
Thread Exit		SUCCESS	Thread ID: 8096, User Time: 0.0000000, Kernel Time: 0.0156250
Thread Exit		SUCCESS	Thread ID: 4816, User Time: 0.0000000, Kernel Time: 0.0000000
Thread Exit		SUCCESS	Thread ID: 8092, User Time: 0.0000000, Kernel Time: 0.0000000
Thread Exit		SUCCESS	Thread ID: 8108, User Time: 0.0000000, Kernel Time: 0.0000000
Thread Exit		SUCCESS	Thread ID: 4860, User Time: 0.0000000, Kernel Time: 0.0781250
Thread Exit		SUCCESS	Thread ID: 8120, User Time: 0.0000000, Kernel Time: 0.0000000
Thread Exit		SUCCESS	Thread ID: 5592, User Time: 0.0000000, Kernel Time: 0.0156250
Thread Exit		SUCCESS	Thread ID: 1612, User Time: 0.0000000, Kernel Time: 0.0156250
Thread Exit		SUCCESS	Thread ID: 8084, User Time: 0.0000000, Kernel Time: 0.0000000
Thread Exit		SUCCESS	Thread ID: 8100, User Time: 0.0000000, Kernel Time: 0.0000000
Thread Exit		SUCCESS	Thread ID: 8116, User Time: 0.0000000, Kernel Time: 0.0000000
Thread Exit		SUCCESS	Thread ID: 8124, User Time: 0.0000000, Kernel Time: 0.0000000
Thread Exit		SUCCESS	Thread ID: 2876, User Time: 0.6875000, Kernel Time: 3.1562500
Thread Exit		SUCCESS	Thread ID: 7872, User Time: 0.0000000, Kernel Time: 0.0000000

(B)

Figure 52 A) Thread Create; B) Thread Exit

Below is the summary of ProcMon logs for file system files. Clearly, a lot of file operations are performed.

Row Labels	Count of Operation
CloseFile	15277
CreateFile	22404
CreateFileMapping	402
FileSystemControl	40
LockFile	13
QueryAllInformationFile	24
QueryAttributeInformationVolume	2
QueryAttributeTagFile	2433
QueryBasicInformationFile	6768
QueryDirectory	3062
QueryFileInternalInformationFile	39
QueryFullSizeInformationVolume	1
QueryInformationVolume	25
QueryNameInformationFile	74
QueryNetworkOpenInformationFile	8
QuerySecurityFile	910
QueryStandardInformationFile	5067
ReadFile	22998
SetBasicInformationFile	3333
SetRenameInformationFile	2405
UnlockFileSingle	13
WriteFile	14046
Grand Total	**99344**

Figure 53

All CloseFile operations are successful (not much important for our analysis). Some of the CreateFile operations result in Access Denied error:

Operation	Path	Result
CreateFile	C:\PerfLogs	ACCESS DENIED
CreateFile	C:\PerfLogs	ACCESS DENIED
CreateFile	C:\Users	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\LocalService\Documents	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\LocalService\Documents	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\LocalService\Documents	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\NetworkService\Documents	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\NetworkService\Documents	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\NetworkService\Documents	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\LocalService\Desktop	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\LocalService\Desktop	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\LocalService\Desktop	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\NetworkService\Desktop	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\NetworkService\Desktop	ACCESS DENIED
CreateFile	C:\Windows\ServiceProfiles\NetworkService\Desktop	ACCESS DENIED
CreateFile	C:\Users\Sysuser\Desktop\odbg110\plugins\.git\objects\pack\pack-f06c35d4149c2c6d38beae81fa061ca92eefce80.idx	ACCESS DENIED
CreateFile	C:\Users\Sysuser\Desktop\odbg201\plugins\ollydbg-script\.git\objects\pack\pack-f06c35d4149c2c6d38beae81fa061ca92eefce80.idx	ACCESS DENIED
CreateFile	\\sysuser-pc\users\	ACCESS DENIED

Figure 54

Some CreateFile operation result in Path Not Found error (e.g. C:\test\cerber_debug2.txt, C:\Windows\System32\DriverStore\FileRepository\tkbtnpn.inf_061cd165\lencins.dll, etc.). Some result in Name Not Found error and Name Collision errors.

CreateFile	**22404**
ACCESS DENIED	18
NAME COLLISION	4107
NAME NOT FOUND	2963
PATH NOT FOUND	27
REPARSE	3
SUCCESS	15286

Figure 55

Many files are successfully written. We see that .hta and .txt files are created by the ransomware in each directory (total 356) where it encrypted files.

Operation	Path	Result
CreateFile	C:\Users\Public\Documents_R_E_A_D___T_H_I_S___5FLKEUR6_.hta	SUCCESS
CreateFile	C:\Users\Public\Documents_R_E_A_D___T_H_I_S___SG5J_.txt	SUCCESS
CreateFile	C:\Users\Public\Documents\Explorer Suite Signatures_R_E_A_D___T_H_I_S___AWKA9C9_.hta	SUCCESS
CreateFile	C:\Users\Public\Documents\Explorer Suite Signatures_R_E_A_D___T_H_I_S___QL979X0_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Documents_R_E_A_D___T_H_I_S___59YJ_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Documents_R_E_A_D___T_H_I_S___H7WV_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Documents\depends22_x86_R_E_A_D___T_H_I_S___AIGHOB_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Documents\depends22_x86_R_E_A_D___T_H_I_S___CVLREUDA_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Documents\Regshot-1.9.0_R_E_A_D___T_H_I_S___KI5X6PD_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Documents\Regshot-1.9.0_R_E_A_D___T_H_I_S___QRRH07_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop_R_E_A_D___T_H_I_S___0078DKZV_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop_R_E_A_D___T_H_I_S___6NVEGKG_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs_R_E_A_D___T_H_I_S___VYEYK_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs_R_E_A_D___T_H_I_S___YF3ANUU_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\Advanced\Examples_R_E_A_D___T_H_I_S___XFTBLY1B_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\Advanced\Examples_R_E_A_D___T_H_I_S___XIIXPCAQ_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\Advanced_R_E_A_D___T_H_I_S___RB1UAT_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\Advanced_R_E_A_D___T_H_I_S___XVBGDE_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\AdvancedDevelopment\ghidra-format_R_E_A_D___T_H_I_S___JOXEGDN_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\AdvancedDevelopment\ghidra-format_R_E_A_D___T_H_I_S___JIXTSHJV_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\AdvancedDevelopment_R_E_A_D___T_H_I_S___II5F3K_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\AdvancedDevelopment_R_E_A_D___T_H_I_S___O8GPIXM_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\AdvancedDevelopment\Images_R_E_A_D___T_H_I_S___4LSTHO0B_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\AdvancedDevelopment\Images_R_E_A_D___T_H_I_S___1KA1_.txt	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\Beginner\Images_R_E_A_D___T_H_I_S___VOKLWM_.hta	SUCCESS
CreateFile	C:\Users\Sysuser\Desktop\ghidra_9.0.1_PUBLIC_20190325\ghidra_9.0.1\docs\GhidraClass\Beginner\Images_R_E_A_D___T_H_I_S___EQDS_.txt	SUCCESS

Figure 56

CreateFileMapping operations are performed to create or open file mapping objects for the specified files.

CreateFileMapping	**402**
FILE LOCKED WITH ONLY READERS	201
SUCCESS	201

Figure 57

FileSystemControl operations are also performed to get these controls:
FSCTL_FILE_PREFETCH, FSCTL_LMR_QUERY_DEBUG_INFO,
CSC_FSCTL_OPERATION_QUERY_HANDLE,
FSCTL_DFS_GET_REFERRALS,
FSCTL_NETWORK_DELETE_CONNECTION.

FileSystemControl	**40**
END OF FILE	9
FS DRIVER REQUIRED	1
INVALID DEVICE REQUEST	19
SUCCESS	11

Figure 58

Multiple LockFile operations are performed on two unique files:

Operation	Path	Result
LockFile	C:\Users\Sysuser\Desktop\desktop.ini	SUCCESS
LockFile	C:\Users\Sysuser\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini	SUCCESS

Figure 59

Other operations are also performed to get more information about files and directories, read and write files and to set information about files and directories (shown below with result status).

QueryAllInformationFile	**24**
BUFFER OVERFLOW	24
QueryAttributeInformationVolume	**2**
SUCCESS	2
QueryAttributeTagFile	**2433**
SUCCESS	2433
QueryBasicInformationFile	**6768**
SUCCESS	6768
QueryDirectory	**3062**
NO MORE FILES	891
NO SUCH FILE	1
SUCCESS	2170
QueryFileInternalInformationFile	**39**
SUCCESS	39
QueryFullSizeInformationVolume	**1**
SUCCESS	1
QueryInformationVolume	**25**
SUCCESS	25
QueryNameInformationFile	**74**
SUCCESS	74
QueryNetworkOpenInformationFile	**8**
SUCCESS	8
QuerySecurityFile	**910**
BUFFER OVERFLOW	1
SUCCESS	909
QueryStandardInformationFile	**5067**
SUCCESS	5067

(A)

ReadFile	**22998**
END OF FILE	1
SUCCESS	22997
SetBasicInformationFile	**3333**
SUCCESS	3333
SetRenameInformationFile	**2405**
SUCCESS	2405
UnlockFileSingle	**13**
SUCCESS	13
WriteFile	**14046**
SUCCESS	14046

(B)

Figure 60

Example of file encryption:

This sequence of operations performed on the file `C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml` indicates a series of file manipulation actions.

Operation	Path	Result	Detail
CreateFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Desired Access: Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
SetBasicInformationFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	CreationTime: 0, LastAccessTime: 0, LastWriteTime: 0, ChangeTime: 0, FileAttributes: ANNCI
CloseFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	
CreateFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Desired Access: Generic Read/Write, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/a, ShareMode: None, AllocationSize: n/a, OpenResult: Opened
QueryStandardInformationFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	AllocationSize: 757,760, EndOfFile: 754,095, NumberOfLinks: 1, DeletePending: False, Directory: False
QueryBasicInformationFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	CreationTime: 7/27/2023 7:49:33 AM, LastAccessTime: 7/27/2023 7:49:33 AM, LastWriteTime: 7/1/2007 1:46:24 AM, ChangeTime: 4/26/2024 11:27:30 AM, FileAttributes: ANCI
ReadFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 1,792, Length: 60, Priority: Normal
ReadFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 1,852, Length: 262,144
WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 1,852, Length: 262,144, Priority: Normal
ReadFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 263,996, Length: 262,144
WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 263,996, Length: 262,144
ReadFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 526,140, Length: 227,955
WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 526,140, Length: 227,955
WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 1,792, Length: 60
QueryStandardInformationFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	AllocationSize: 757,760, EndOfFile: 754,095, NumberOfLinks: 1, DeletePending: False, Directory: False
WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 754,095, Length: 86, Priority: Normal
WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 754,181, Length: 110
WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 754,291, Length: 256
CloseFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	
CreateFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Desired Access: Read Attributes, Delete, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Open Reparse Point, Attributes: n/a, ShareMode: Read, Write, Delete, AllocationSize: n/a, OpenResult: Opened
QueryAttributeTagFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Attributes: ANCI, ReparseTag: 0x0
QueryBasicInformationFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	CreationTime: 7/27/2023 7:49:33 AM, LastAccessTime: 7/27/2023 7:49:33 AM, LastWriteTime: 4/26/2024 11:27:30 AM, ChangeTime: 4/26/2024 11:27:30 AM, FileAttributes: ANCI
SetRenameInformationFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	ReplaceIfExists: False, FileName: C:\Users\Public\Documents\Explorer Suite Signatures\1Z8hwJ1dyA.8856

Figure 61

1. CreateFile: The file is successfully opened with the desired access to write attributes. The file's attributes are set to ANNCI, and it is opened for writing.
2. SetBasicInformationFile: The basic information of the file is successfully set.

3. CloseFile: The file is successfully closed after the operations.
4. CreateFile (2nd): The file is successfully reopened with generic read/write access. It is opened for non-directory files, and sharing mode is None.
5. QueryStandardInformationFile: The standard information of file is queried successfully.
6. QueryBasicInformationFile: The basic information of file is queried successfully.
7. ReadFile (Multiple times): The file is successfully read at different offsets and lengths.
8. WriteFile (Multiple times): The file is successfully written to at different offsets and lengths (encrypted data is getting written).
9. QueryStandardInformationFile (2nd): The standard information of file is queried again.
10. WriteFile (Multiple times): Additional writes are performed on the file.
11. CloseFile (2nd): The file is closed again after the operations.
12. CreateFile (3rd): The file is opened again, this time with desired access to read attributes, delete, and synchronize. It is opened with the intent to rename.
13. QueryAttributeTagFile: Attributes and reparse tag of file are queried successfully.
14. QueryBasicInformationFile (2nd): Basic information of file is queried again.
15. SetRenameInformationFile: The file is successfully renamed to: 'C:\Users\Public\Documents\Explorer Suite Signatures\1Z8hwJ1dyA.8856'. This is the encrypted file finally found in our system.

Advanced Static Analysis

As the next step, we will use Ghidra to learn more about the program code. The function call graph indicates that entry function calls multiple functions.

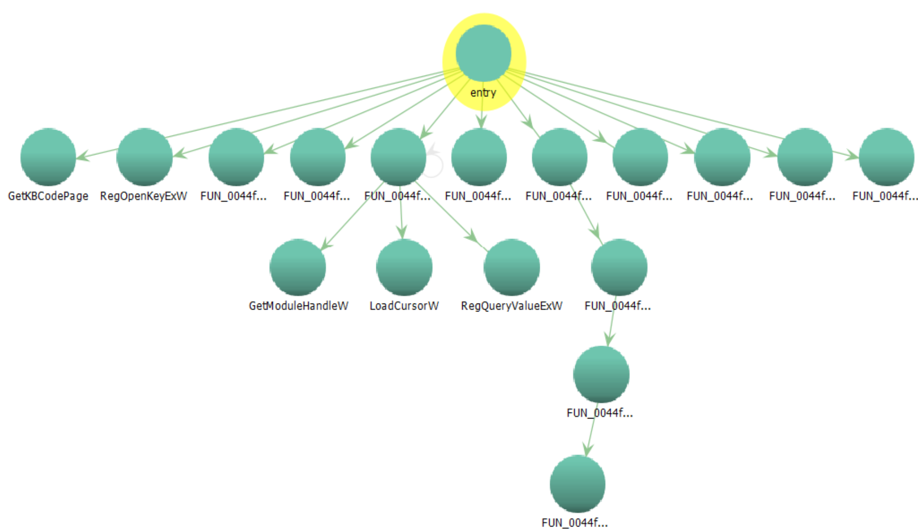


Figure 62

The function `entry` begins with some initialization and setting of global variables. The do while loop calls `RegOpenKeyExW` on the data stored at 0040c0c8 (u_11111kicu4p3050f55f298b5211cf2bb) and

0040c0b0 while updating 0040c0b0 repeatedly until it returns a zero value, indicating that something was found. Various functions are called throughout the entry function, performing different tasks. There are several assignments to global variables (`DAT_0048c184`, `DAT_0048c144`, `DAT_0048c188`, etc.) within the function. There is another do while loop which iterates based on the value of `DAT_0048c188`. It seems to be performing some kind of initialization. FUN_0044f810 appears to be performing some sort of memory allocation operation using the Windows API function VirtualAlloc. FUN_0044f9d0 iterates over a range of memory addresses and modifies them. FUN_0044f1e0 prepares data for processing and calls FUN_0044fad0 which performs XOR operation on the data. FUN_0044f890 calls another function through a function pointer stored in DAT_0048c19c. It appears that all these functions will decode some memory locations which will then be called while executing.

After examining the decompiled code, we have managed to identify most of the functions and renamed them accordingly (shown in figure below):
RegOpenKeyExW, MaxFunction, SomeModuleRelatedFunction, VirtualAllocationFunction, MemoryAllocationFunction, MemoryManipulationFunction, UnpackingFunction, CallXorFunction, XORFunction, etc. These indicate that the program is going to unpack or decrypt some parts of its memory at run time and thus manipulate memory using a XOR function. It will also open registry keys (probably all of them).

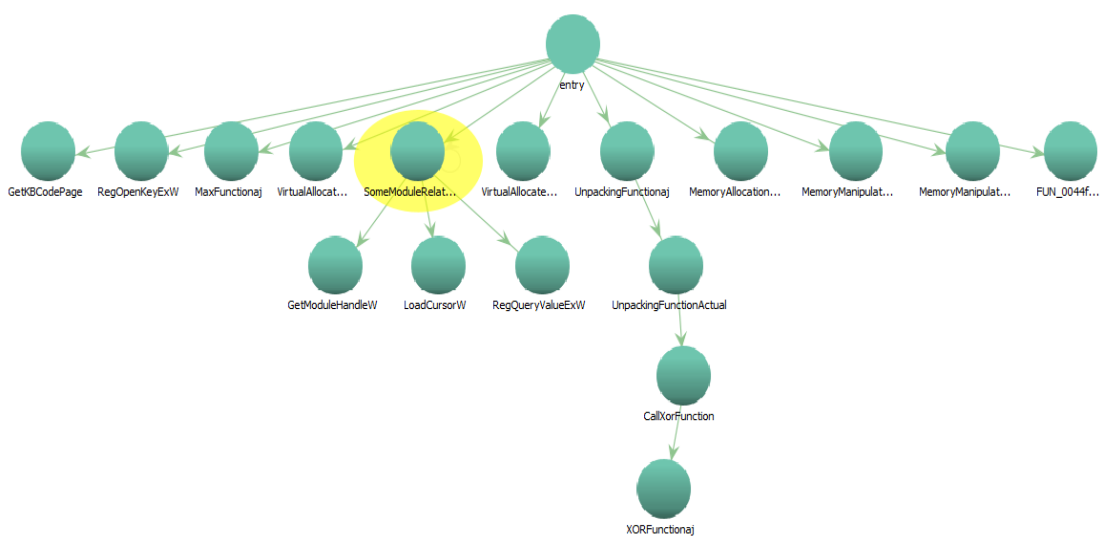


Figure 63

Advanced Dynamic Analysis

As the next step of analysis, we will load the program in OllyDbg 2 while setting the debugging options as break on new module (DLL) loading and unloading. We reach 004F4E0 which is the entry point of the program. We also get a warning that code section is either compressed or encrypted.

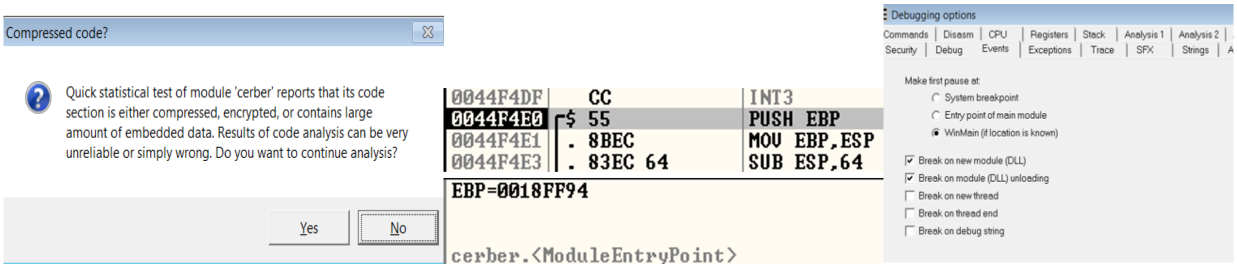


Figure 64

As we step-in the entry function, we see that the gibberish string "u_11111kicu4p3050f55f298b5211cf2bb" at 0048c0c8 is modified to interface\{3050f55f-98b5-11cf-bb82-00aa00bdce0b}. This makes the first do while loop returns a zero value since now the program is able to open the registry key.

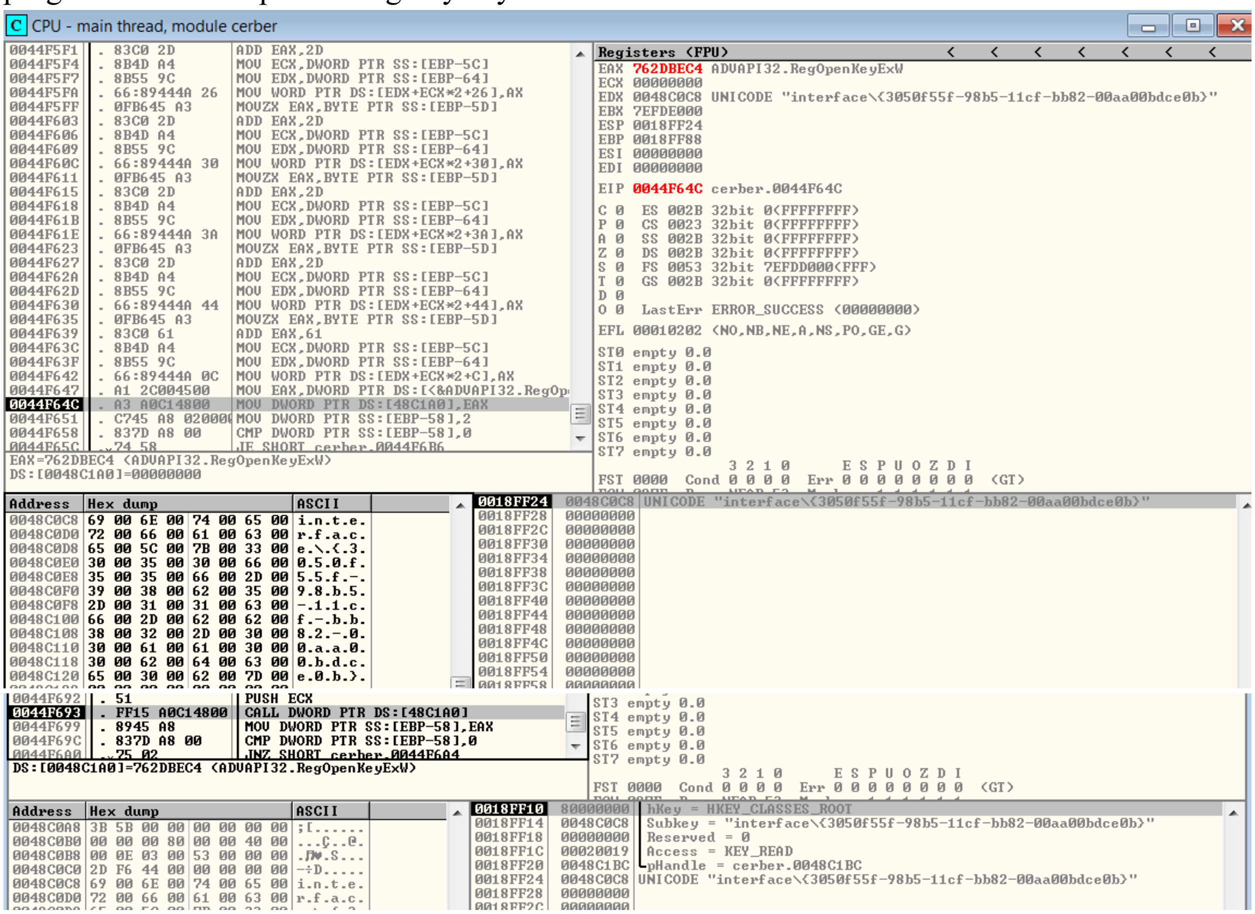


Figure 65

Upon checking in regedit, we see that this registry key is related to display html document (probably the final ransom note).

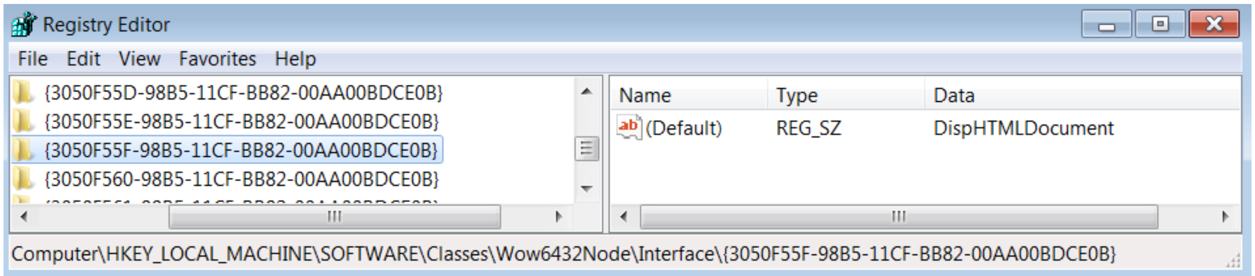


Figure 66

After stepping in and stepping over instructions, we see that 4 new sections are added in the memory.

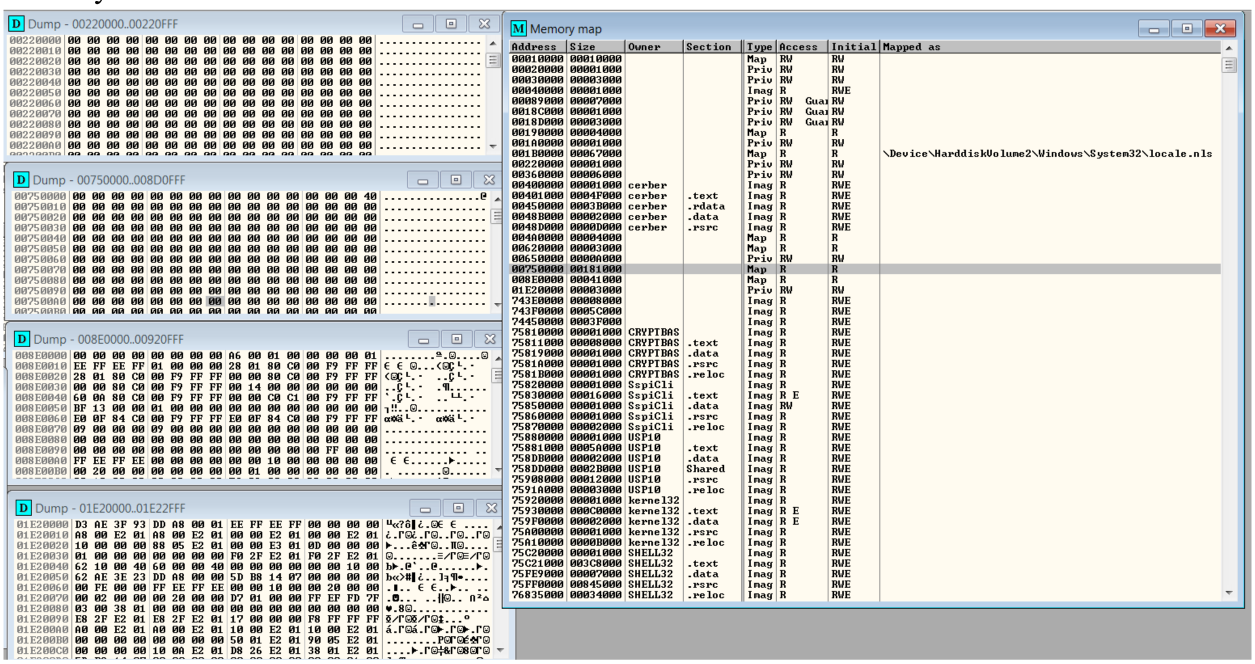


Figure 67

This is the list of initial modules:

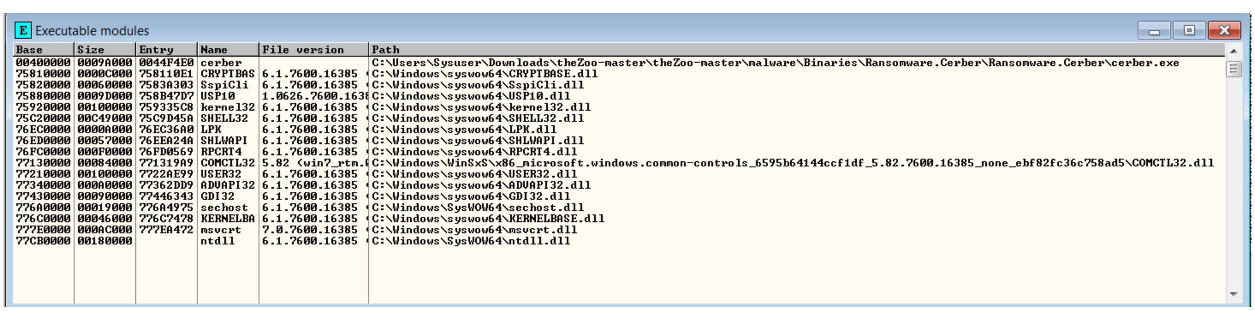


Figure 68

Since we have set a breakpoint on the new DLL load, we can use F9 to play the program further. We see that multiple new modules are loaded by the program including crypt32.dll, CRYPTSP.dll, CLBCatQ.dll and many more. Simultaneously, more sections are created in the memory map. Final executable modules window:

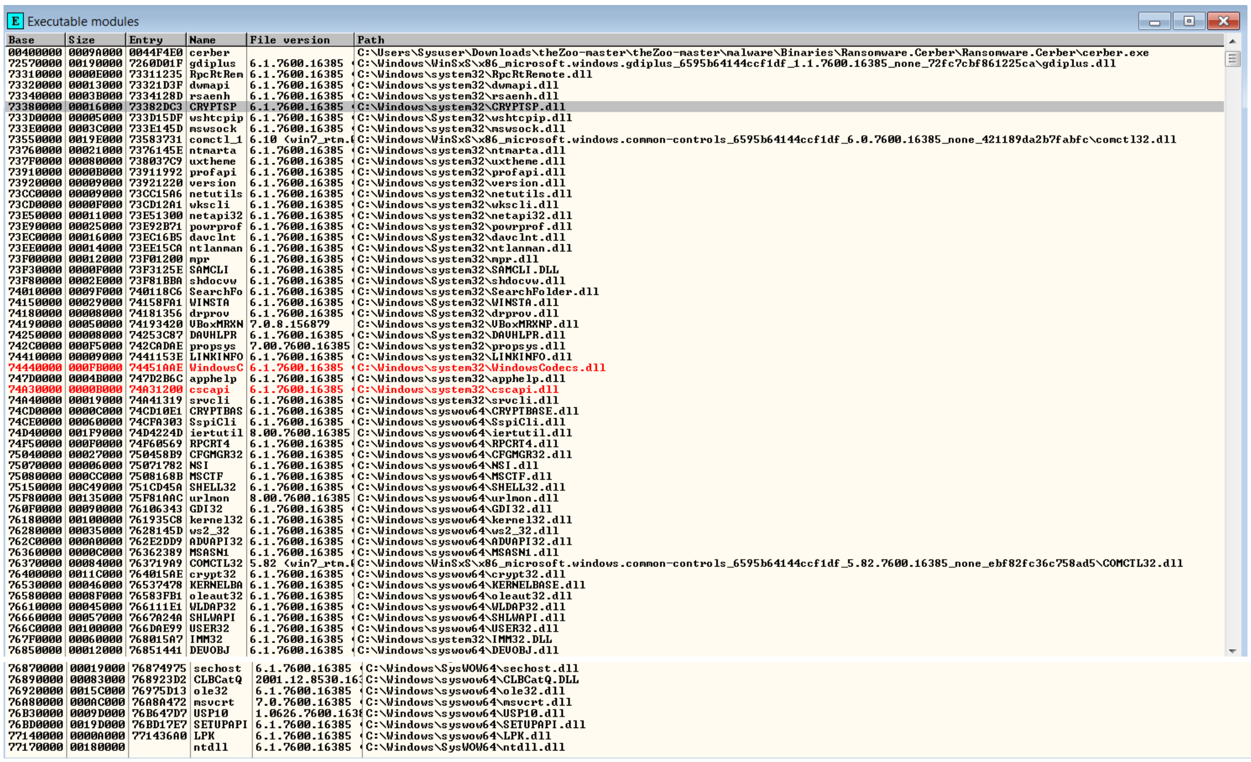


Figure 69

As we move forward, we see that functions of ntdll are called like RtlEnterCriticalSection, RtlRunOnceExecuteOnce, RtlGetCurrentTransaction, RtlRunOnceBeginIntialize – it seems that only one instance of cerber.exe is allowed to run at a time. RtlAllocateHeap, RtlCreateAcl, RtlFreSid, RtlSetDaclSecurityDescriptor, RtlCreateSecurityDescriptor and RtlAddAccessAllowedAce are also called. Then, at address 44F860, VirtualAlloc function of kernel32.dll is called.

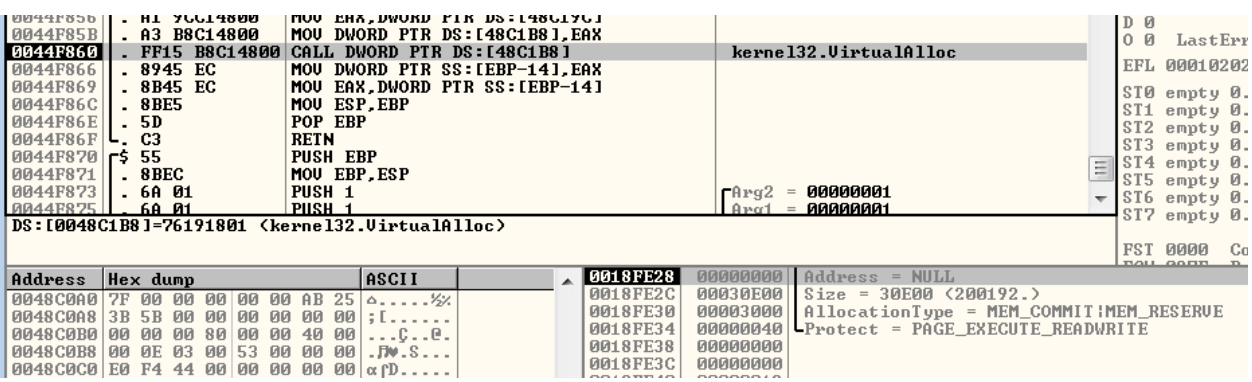


Figure 70

At this point, we see that memory is getting modified starting from 0x2300000.

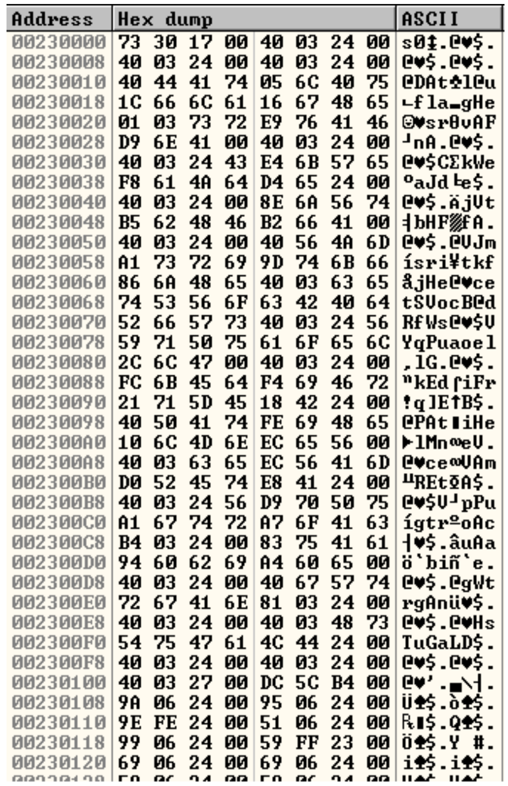


Figure 71

After few step-in and step-over operations, we observe that data changes in the function XXX returning at 0044FBE5. Setting a breakpoint at 0x44FBE3, we will use F9 to move ahead. An example of data change is shown below (memory in figure at left changes to memory in figure at right).

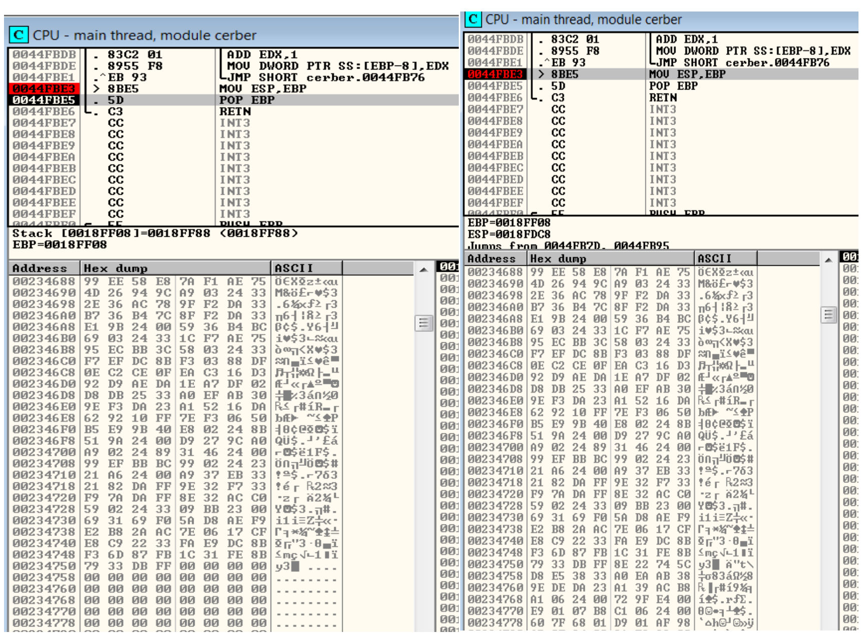


Figure 72

It is worth mentioning that 83 bytes are modified in one function execution until memory at address 00260DFF is modified.

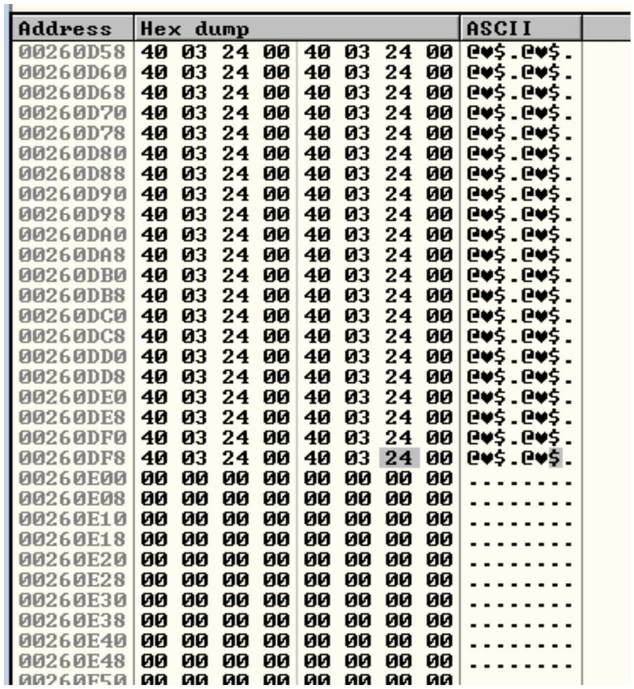


Figure 73

Moving ahead with step-in, we enter another function 0x44F900 which and see that data starting at 0x230000 is again getting modified. This time, we set a breakpoint at 0044FB12 and observe that data is modified for the same memory block (0x230000 to 0x260DFF) using XOR.

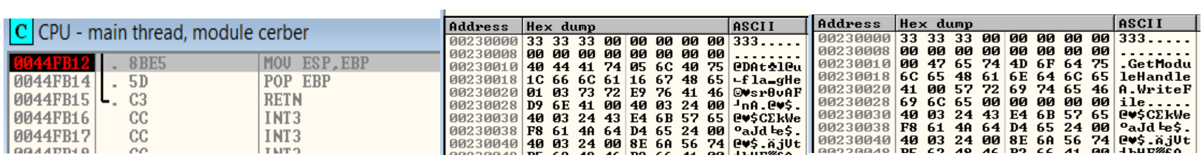


Figure 74

Here, 4 bytes are modified during one function execution. An example of data change is shown below (memory in figure at left changes to memory in figure at right).

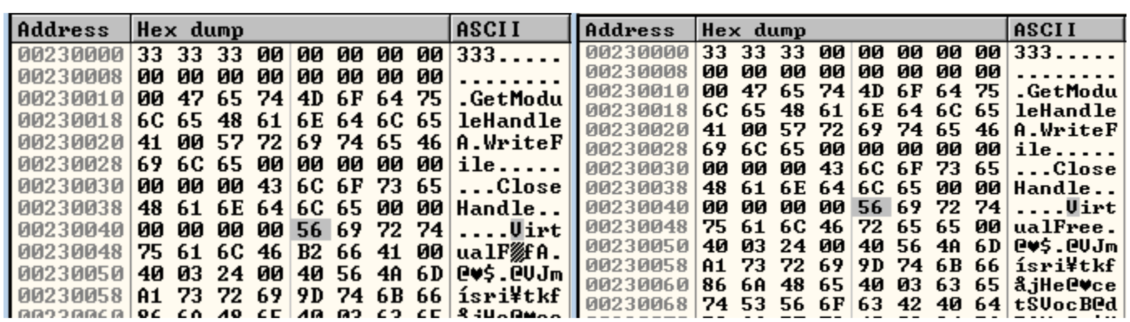


Figure 75

This observation matches our static analysis of FUN_0044f900 using Ghidra.

```
void FUN_0044f900(void)

{
  DAT_0048c158 = 0;
  while (DAT_0048c158 < DAT_0048c144) {
    DAT_0048c1ac = (int *)(DAT_0048c188 + DAT_0048c158);
    *DAT_0048c1ac = *DAT_0048c1ac + DAT_0048c158;
    DAT_0048c198 = DAT_0048c158 + 0x240340;
    FUN_0044f1e0();
    DAT_0048c158 = DAT_0048c158 + 4;
  }
  return;
}
```

```
Registers (FPU)
EAX 0018FF18
ECX 00030E00
EDX 00260B20
EBX 7EFDE000
ESP 0018FEF8
EBP 0018FF80
ESI 00000000
EDI 00000000
```

Figure 76

As we move further in the program, we see that function at 0x44f890 is called which starts to call other functions (not present earlier but present now in memory) using function pointers. It calls a function defined at 0x2600B20 (address loaded in EDX register).

```
00260B20  55               PUSH EBP
00260B21  8BEC             MOV EBP,ESP
00260B23  81EC 80000000    SUB ESP,80
00260B29  C745 F4 00000000 MOV DWORD PTR SS:[EBP-C],0
00260B30  6A 58            PUSH 58
00260B32  6A 00            PUSH 0
00260B34  8D45 98          LEA EAX,DWORD PTR SS:[EBP-68]
00260B37  50               PUSH EAX
00260B38  E8 33F9FFFF      CALL 00260470
00260B3D  83C4 0C          ADD ESP,0C
00260B40  8B45 04          MOV EAX,DWORD PTR SS:[EBP+4]
00260B43  8945 F8          MOV DWORD PTR SS:[EBP-8],EAX
00260B46  8B45 08          MOV EAX,DWORD PTR SS:[EBP+8]
00260B49  8945 8C          MOV DWORD PTR SS:[EBP-74],EAX
00260B4C  896D 98          MOV DWORD PTR SS:[EBP-68],EBP
00260B4F  8D4D 98          LEA ECX,DWORD PTR SS:[EBP-68]
00260B52  51               PUSH ECX
00260B53  E8 B8F6FFFF      CALL 00260210
00260B58  83C4 04          ADD ESP,4
00260B5B  E8 B0F5FFFF      CALL 00260110
00260B60  8945 84          MOV DWORD PTR SS:[EBP-7C],EAX
00260B63  8B55 F8          MOV EDX,DWORD PTR SS:[EBP-8]
00260B66  8955 A0          MOV DWORD PTR SS:[EBP-60],EDX
00260B69  8B45 8C          MOV EAX,DWORD PTR SS:[EBP-74]
00260B6C  8945 AC          MOV DWORD PTR SS:[EBP-54],EAX
00260B6F  8B4D AC          MOV ECX,DWORD PTR SS:[EBP-54]
00260B72  894D F0          MOV DWORD PTR SS:[EBP-10],ECX
00260B75  8B55 AC          MOV EDX,DWORD PTR SS:[EBP-54]
00260B78  8B45 F0          MOV EAX,DWORD PTR SS:[EBP-10]
00260B7B  0342 3C          ADD EAX,DWORD PTR DS:[EDX+3C]
00260B7E  8945 F0          MOV DWORD PTR SS:[EBP-10],EAX
00260B81  8B4D F0          MOV ECX,DWORD PTR SS:[EBP-10]
00260B84  894D 90          MOV DWORD PTR SS:[EBP-70],ECX
00260B87  8B55 90          MOV EDX,DWORD PTR SS:[EBP-70]
00260B8A  0FB742 16        MOVZX EAX,WORD PTR DS:[EDX+16]
00260B8E  8945 A4          MOV DWORD PTR SS:[EBP-5C],EAX
00260B91  E8 7AF5FFFF      CALL 00260110
00260B96  05 00114000      ADD EAX,401100
00260B9B  8945 88          MOV DWORD PTR SS:[EBP-78],EAX
00260B9E  8B4D 88          MOV ECX,DWORD PTR SS:[EBP-78]
00260BA1  8B11             MOV EDX,DWORD PTR DS:[ECX]
00260BA3  8955 80          MOV DWORD PTR SS:[EBP-80],EDX
00260BA6  E8 65F5FFFF      CALL 00260110
00260BAB  05 04114000      ADD EAX,401104
00260BB0  8945 88          MOV DWORD PTR SS:[EBP-78],EAX
00260BB3  8B45 80          MOV EAX,DWORD PTR SS:[EBP-80]
00260BB6  50               PUSH EAX
00260BB7  E8 64F7FFFF      CALL 00260320
00260BBC  83C4 04          ADD ESP,4
00260BBF  8945 94          MOV DWORD PTR SS:[EBP-6C],EAX
00260BC2  8B4D 80          MOV ECX,DWORD PTR SS:[EBP-80]
00260BC5  51               PUSH ECX
00260BC6  8B55 88          MOV EDX,DWORD PTR SS:[EBP-78]
00260BC9  52               PUSH EDX
00260BCA  8B45 94          MOV EAX,DWORD PTR SS:[EBP-6C]
00260BCD  50               PUSH EAX
00260BCE  E8 DDF8FFFF      CALL 002604B0
00260BD3  83C4 0C          ADD ESP,0C
00260BD6  8B4D 80          MOV ECX,DWORD PTR SS:[EBP-80]
00260BD9  51               PUSH ECX
00260BDA  8B55 94          MOV EDX,DWORD PTR SS:[EBP-6C]
00260BDD  52               PUSH EDX
00260BDE  E8 EDFEFFFF      CALL 00260AD0
00260BE3  83C4 08          ADD ESP,8
00260BE6  8B45 94          MOV EAX,DWORD PTR SS:[EBP-6C]
00260BE9  50               PUSH EAX
00260BEA  8D4D 98          LEA ECX,DWORD PTR SS:[EBP-68]
00260BED  51               PUSH ECX
00260BEE  E8 7DFCFFFF      CALL 00260870
00260BF3  85C0             TEST EAX,EAX
00260BF5  75 04            JNZ SHORT 00260BFB
00260BF7  33C0             XOR EAX,EAX
00260BF9  EB 1A            JMP SHORT 00260C15
00260BFB  837D A0 00       CMP DWORD PTR SS:[EBP-60],0
00260BFF  74 09            JE SHORT 00260C0A
00260C01  8B45 B0          MOV EAX,DWORD PTR SS:[EBP-50]
00260C04  8B4D 98          MOV ECX,DWORD PTR SS:[EBP-68]
00260C07  8941 10          MOV DWORD PTR DS:[ECX+10],EAX
00260C0A  8B55 A8          MOV EDX,DWORD PTR SS:[EBP-58]
00260C0D  8B65 98          MOV ESP,DWORD PTR SS:[EBP-68]
00260C10  5D               POP EBP
00260C11  58               POP EAX
00260C12  58               POP EAX
00260C13  52               PUSH EDX
00260C14  C3               RETN
00260C15  8BE5             MOV ESP,EBP
00260C17  5D               POP EBP
00260C18  C3               RETN
```

Figure 77

The function at 0x260B20 calls another function at 0x260470 with three arguments.

Figure 78

Value at 0x18FF80 is:

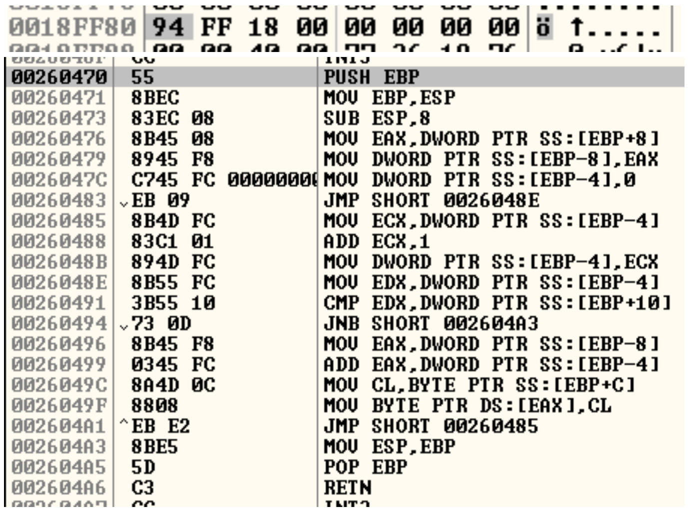


Figure 79

This function looks like it is copying bytes from source to destination until some terminator is found. We see that a new module MSCTF is loaded into the program now.

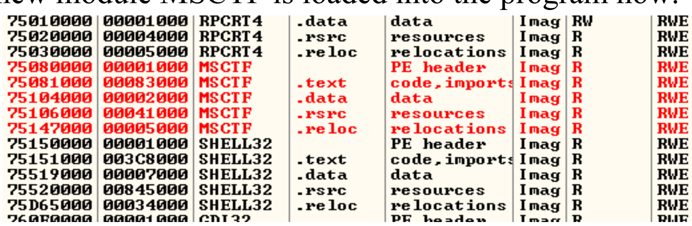


Figure 80

Next, function at 0x260210 is called.

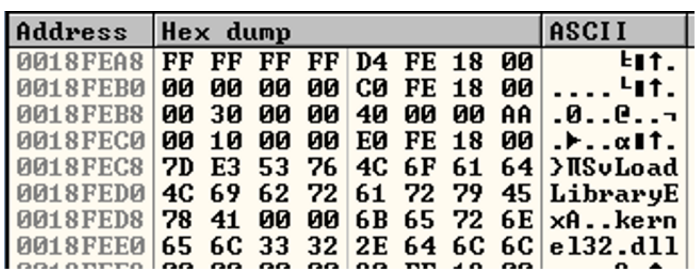
```
00260210  55              PUSH EBP
00260211  8BEC            MOV EBP,ESP
00260213  83EC 30         SUB ESP,30
00260216  C645 D8 4C      MOV BYTE PTR SS:[EBP-28],4C
0026021A  C645 D9 6F      MOV BYTE PTR SS:[EBP-27],6F
0026021E  C645 DA 61      MOV BYTE PTR SS:[EBP-26],61
00260222  C645 DB 64      MOV BYTE PTR SS:[EBP-25],64
00260226  C645 DC 4C      MOV BYTE PTR SS:[EBP-24],4C
0026022A  C645 DD 69      MOV BYTE PTR SS:[EBP-23],69
0026022E  C645 DE 62      MOV BYTE PTR SS:[EBP-22],62
00260232  C645 DF 72      MOV BYTE PTR SS:[EBP-21],72
00260236  C645 E0 61      MOV BYTE PTR SS:[EBP-20],61
0026023A  C645 E1 72      MOV BYTE PTR SS:[EBP-1F],72
0026023E  C645 E2 79      MOV BYTE PTR SS:[EBP-1E],79
00260242  C645 E3 45      MOV BYTE PTR SS:[EBP-1D],45
00260246  C645 E4 78      MOV BYTE PTR SS:[EBP-1C],78
0026024A  C645 E5 41      MOV BYTE PTR SS:[EBP-1B],41
0026024E  C645 E6 00      MOV BYTE PTR SS:[EBP-1A],0
00260252  C645 E8 6B      MOV BYTE PTR SS:[EBP-18],6B
00260256  C645 E9 65      MOV BYTE PTR SS:[EBP-17],65
0026025A  C645 EA 72      MOV BYTE PTR SS:[EBP-16],72
0026025E  C645 EB 6E      MOV BYTE PTR SS:[EBP-15],6E
00260262  C645 EC 65      MOV BYTE PTR SS:[EBP-14],65
00260266  C645 ED 6C      MOV BYTE PTR SS:[EBP-13],6C
0026026A  C645 EE 33      MOV BYTE PTR SS:[EBP-12],33
0026026E  C645 EF 32      MOV BYTE PTR SS:[EBP-11],32
00260272  C645 F0 2E      MOV BYTE PTR SS:[EBP-10],2E
00260276  C645 F1 64      MOV BYTE PTR SS:[EBP-F],64
0026027A  C645 F2 6C      MOV BYTE PTR SS:[EBP-E],6C
0026027E  C645 F3 6C      MOV BYTE PTR SS:[EBP-D],6C
00260282  C645 F4 00      MOV BYTE PTR SS:[EBP-C],0
00260286  E8 75040000     CALL 00260700
0026028B  8945 D0         MOV DWORD PTR SS:[EBP-30],EAX
0026028E  E8 7DFEFFFF     CALL 00260110
00260293  8945 D4         MOV DWORD PTR SS:[EBP-2C],EAX
00260296  8B45 D4         MOV EAX,DWORD PTR SS:[EBP-2C]
00260299  05 00104000     ADD EAX,401000
0026029E  8945 F8         MOV DWORD PTR SS:[EBP-8],EAX
002602A1  8B4D D0         MOV ECX,DWORD PTR SS:[EBP-30]
002602A4  51              PUSH ECX
002602A5  E8 76FEFFFF     CALL 00260120
002602AA  83C4 04         ADD ESP,4
002602AD  8B55 08         MOV EDX,DWORD PTR SS:[EBP+8]
002602B0  8942 34         MOV DWORD PTR DS:[EDX+34],EAX
002602B3  8D45 D8         LEA EAX,DWORD PTR SS:[EBP-28]
002602B6  50              PUSH EAX
002602B7  8B4D D0         MOV ECX,DWORD PTR SS:[EBP-30]
002602BA  51              PUSH ECX
002602BB  8B55 08         MOV EDX,DWORD PTR SS:[EBP+8]
002602BE  8B42 34         MOV EAX,DWORD PTR DS:[EDX+34]
002602C1  FFD0            CALL EAX
002602C3  8B4D 08         MOV ECX,DWORD PTR SS:[EBP+8]
002602C6  8941 3C         MOV DWORD PTR DS:[ECX+3C],EAX
002602C9  6A 00           PUSH 0
002602CB  6A 00           PUSH 0
002602CD  8D55 E8         LEA EDX,DWORD PTR SS:[EBP-18]
002602D0  52              PUSH EDX
002602D1  8B45 08         MOV EAX,DWORD PTR SS:[EBP+8]
002602D4  8B48 3C         MOV ECX,DWORD PTR DS:[EAX+3C]
002602D7  FFD1            CALL ECX
002602D9  8945 D0         MOV DWORD PTR SS:[EBP-30],EAX
002602DC  C745 FC 0000000 MOV DWORD PTR SS:[EBP-4],0
002602E3  EB 09           JMP SHORT 002602EE
002602E5  8B55 FC         MOV EDX,DWORD PTR SS:[EBP-4]
002602E8  83C2 01         ADD EDX,1
002602EB  8955 FC         MOV DWORD PTR SS:[EBP-4],EDX
002602EE  837D FC 0F      CMP DWORD PTR SS:[EBP-4],0F
002602F2  73 22           JNB SHORT 00260316
002602F4  8B45 FC         MOV EAX,DWORD PTR SS:[EBP-4]
002602F7  6BC0 11         IMUL EAX,EAX,11
002602FA  0345 F8         ADD EAX,DWORD PTR SS:[EBP-8]
002602FD  50              PUSH EAX
002602FE  8B4D D0         MOV ECX,DWORD PTR SS:[EBP-30]
00260301  51              PUSH ECX
00260302  8B55 08         MOV EDX,DWORD PTR SS:[EBP+8]
00260305  8B42 34         MOV EAX,DWORD PTR DS:[EDX+34]
00260308  FFD0            CALL EAX
0026030A  8B4D FC         MOV ECX,DWORD PTR SS:[EBP-4]
0026030D  8B55 08         MOV EDX,DWORD PTR SS:[EBP+8]
00260310  89448A 1C       MOV DWORD PTR DS:[EDX+ECX*4+1C],EAX
00260314  EB CF           JMP SHORT 002602E5
00260316  8BE5            MOV ESP,EBP
00260318  5D              POP EBP
00260319  C3              RETN
0026031A  CC              INT3
```

Figure 81

A possible equivalent C code could be:

```
void function1(int arg) {
    char string1[] = "LoadLibraryExA";
    char string2[] = "kernel32.dll";
    int a, b;
    int *ptr = &arg;
    a = function2();  // external function call at 00260700
    b = function3();  // external function call at 00260110
    int c = b + 0x401000;
    int i = 0;
    while (i < 15) {
        int address = c + i * 17;
        int d = function4(address, a);
        ptr[i + 7] = d;
        i++;
    }
    int ans = function5(string2);
    ptr[15] = ans;
}
```

The reverse engineered function seems to be correct as we see these strings in memory:



Address	Hex dump	ASCII
0018FEA8	FF FF FF FF D4 FE 18 00	╘■↑.
0018FEB0	00 00 00 00 C0 FE 18 00	....└■↑.
0018FEB8	00 30 00 00 40 00 00 AA	.0..@..¬
0018FEC0	00 10 00 00 E0 FE 18 00	.►..α■↑.
0018FEC8	7D E3 53 76 4C 6F 61 64	}πSvLoad
0018FED0	4C 69 62 72 61 72 79 45	LibraryE
0018FED8	78 41 00 00 6B 65 72 6E	xA..kern
0018FEE0	65 6C 33 32 2E 64 6C 6C	el32.dll

Figure 82

The function at 0x260700 looks like this:

```
00260700   55               PUSH EBP
00260701   8BEC             MOV EBP,ESP
00260703   83EC 14          SUB ESP,14
00260706   64:A1 18000000   MOV EAX,DWORD PTR FS:[18]
0026070C   3E:8B40 30       MOV EAX,DWORD PTR DS:[EAX+30]
00260710   3E:8B48 0C       MOV ECX,DWORD PTR DS:[EAX+C]
00260714   894D F4          MOV DWORD PTR SS:[EBP-C],ECX
00260717   8B45 F4          MOV EAX,DWORD PTR SS:[EBP-C]
0026071A   8B48 0C          MOV ECX,DWORD PTR DS:[EAX+C]
0026071D   894D F8          MOV DWORD PTR SS:[EBP-8],ECX
00260720   8B55 F8          MOV EDX,DWORD PTR SS:[EBP-8]
00260723   8955 FC          MOV DWORD PTR SS:[EBP-4],EDX
00260726   B8 01000000      MOV EAX,1
0026072B   85C0             TEST EAX,EAX
0026072D  ˅0F84 80000000    JE 002607B3
00260733   837D F8 00       CMP DWORD PTR SS:[EBP-8],0
00260737  ˅75 04            JNZ SHORT 0026073D
00260739   33C0             XOR EAX,EAX
0026073B  ˅EB 76            JMP SHORT 002607B3
0026073D   8B4D F8          MOV ECX,DWORD PTR SS:[EBP-8]
00260740   8B51 2C          MOV EDX,DWORD PTR DS:[ECX+2C]
00260743   8B41 30          MOV EAX,DWORD PTR DS:[ECX+30]
00260746   8955 EC          MOV DWORD PTR SS:[EBP-14],EDX
00260749   8945 F0          MOV DWORD PTR SS:[EBP-10],EAX
0026074C   8B4D F0          MOV ECX,DWORD PTR SS:[EBP-10]
0026074F   0FB711           MOVZX EDX,WORD PTR DS:[ECX]
00260752   83FA 6B          CMP EDX,6B
00260755  ˅74 0B            JE SHORT 00260762
00260757   8B45 F0          MOV EAX,DWORD PTR SS:[EBP-10]
0026075A   0FB708           MOVZX ECX,WORD PTR DS:[EAX]
0026075D   83F9 4B          CMP ECX,4B
00260760  ˅75 38            JNZ SHORT 0026079A
00260762   8B55 F0          MOV EDX,DWORD PTR SS:[EBP-10]
00260765   0FB742 02        MOVZX EAX,WORD PTR DS:[EDX+2]
00260769   83F8 65          CMP EAX,65
0026076C  ˅74 0C            JE SHORT 0026077A
0026076E   8B4D F0          MOV ECX,DWORD PTR SS:[EBP-10]
00260771   0FB751 02        MOVZX EDX,WORD PTR DS:[ECX+2]
00260775   83FA 45          CMP EDX,45
00260778  ˅75 20            JNZ SHORT 0026079A
0026077A   8B45 F0          MOV EAX,DWORD PTR SS:[EBP-10]
0026077D   0FB748 04        MOVZX ECX,WORD PTR DS:[EAX+4]
00260781   83F9 72          CMP ECX,72
00260784  ˅74 0C            JE SHORT 00260792
00260786   8B55 F0          MOV EDX,DWORD PTR SS:[EBP-10]
00260789   0FB742 04        MOVZX EAX,WORD PTR DS:[EDX+4]
0026078D   83F8 52          CMP EAX,52
00260790  ˅75 08            JNZ SHORT 0026079A
00260792   8B4D F8          MOV ECX,DWORD PTR SS:[EBP-8]
00260795   8B41 18          MOV EAX,DWORD PTR DS:[ECX+18]
00260798  ˅EB 19            JMP SHORT 002607B3
0026079A   8B55 F8          MOV EDX,DWORD PTR SS:[EBP-8]
0026079D   8B02             MOV EAX,DWORD PTR DS:[EDX]
0026079F   8945 F8          MOV DWORD PTR SS:[EBP-8],EAX
002607A2   8B4D F8          MOV ECX,DWORD PTR SS:[EBP-8]
002607A5   3B4D FC          CMP ECX,DWORD PTR SS:[EBP-4]
002607A8  ˅75 04            JNZ SHORT 002607AE
002607AA   33C0             XOR EAX,EAX
002607AC  ˅EB 05            JMP SHORT 002607B3
002607AE  ^E9 73FFFFFF      JMP 00260726
002607B3   8BE5             MOV ESP,EBP
002607B5   5D               POP EBP
002607B6   C3               RETN
002607B7   CC               INT3
```

Figure 83

This function seems to be doing some conditional logic based on values retrieved from memory. Function at 0x260110 is:

```
00260110   E8 00000000   CALL 00260115
00260115   58            POP EAX
00260116   2D 15114300   SUB EAX,431115
0026011B   C3            RETN
0026011C   CC            INT3
```

Figure 84

Equivalent C code:

```
void function3(int arg) {
    int a = function5();
    return a – 431115;
}
```

Function at 0x260120 looks like it is calling GetProcAddress function to get addresses of multiple other functions.

```
00260120   55               PUSH EBP
00260121   8BEC             MOV EBP,ESP
00260123   83EC 30          SUB ESP,30
00260126   C645 D8 47       MOV BYTE PTR SS:[EBP-28],47
0026012A   C645 D9 65       MOV BYTE PTR SS:[EBP-27],65
0026012E   C645 DA 74       MOV BYTE PTR SS:[EBP-26],74
00260132   C645 DB 50       MOV BYTE PTR SS:[EBP-25],50
00260136   C645 DC 72       MOV BYTE PTR SS:[EBP-24],72
0026013A   C645 DD 6F       MOV BYTE PTR SS:[EBP-23],6F
0026013E   C645 DE 63       MOV BYTE PTR SS:[EBP-22],63
00260142   C645 DF 41       MOV BYTE PTR SS:[EBP-21],41
00260146   C645 E0 64       MOV BYTE PTR SS:[EBP-20],64
0026014A   C645 E1 64       MOV BYTE PTR SS:[EBP-1F],64
0026014E   C645 E2 72       MOV BYTE PTR SS:[EBP-1E],72
00260152   C645 E3 65       MOV BYTE PTR SS:[EBP-1D],65
00260156   C645 E4 73       MOV BYTE PTR SS:[EBP-1C],73
0026015A   C645 E5 73       MOV BYTE PTR SS:[EBP-1B],73
0026015E   C645 E6 00       MOV BYTE PTR SS:[EBP-1A],0
00260162   8B45 08          MOV EAX,DWORD PTR SS:[EBP+8]
00260165   8945 D0          MOV DWORD PTR SS:[EBP-30],EAX
00260168   8B4D D0          MOV ECX,DWORD PTR SS:[EBP-30]
0026016B   8B55 D0          MOV EDX,DWORD PTR SS:[EBP-30]
0026016E   0351 3C          ADD EDX,DWORD PTR DS:[ECX+3C]
00260171   8955 D4          MOV DWORD PTR SS:[EBP-2C],EDX
00260174   8B45 D4          MOV EAX,DWORD PTR SS:[EBP-2C]
00260177   8B48 78          MOV ECX,DWORD PTR DS:[EAX+78]
0026017A   034D 08          ADD ECX,DWORD PTR SS:[EBP+8]
0026017D   894D F8          MOV DWORD PTR SS:[EBP-8],ECX
00260180   8B55 F8          MOV EDX,DWORD PTR SS:[EBP-8]
00260183   8B42 24          MOV EAX,DWORD PTR DS:[EDX+24]
00260186   0345 08          ADD EAX,DWORD PTR SS:[EBP+8]
00260189   8945 E8          MOV DWORD PTR SS:[EBP-18],EAX
0026018C   8B4D F8          MOV ECX,DWORD PTR SS:[EBP-8]
0026018F   8B51 20          MOV EDX,DWORD PTR DS:[ECX+20]
00260192   0355 08          ADD EDX,DWORD PTR SS:[EBP+8]
00260195   8955 F0          MOV DWORD PTR SS:[EBP-10],EDX
00260198   8B45 F8          MOV EAX,DWORD PTR SS:[EBP-8]
0026019B   8B48 1C          MOV ECX,DWORD PTR DS:[EAX+1C]
0026019E   034D 08          ADD ECX,DWORD PTR SS:[EBP+8]
002601A1   894D FC          MOV DWORD PTR SS:[EBP-4],ECX
002601A4   C745 F4 0000000  MOV DWORD PTR SS:[EBP-C],0
002601AB  ˅EB 09            JMP SHORT 002601B6
002601AD   8B55 F4          MOV EDX,DWORD PTR SS:[EBP-C]
002601B0   83C2 01          ADD EDX,1
002601B3   8955 F4          MOV DWORD PTR SS:[EBP-C],EDX
002601B6   8B45 F8          MOV EAX,DWORD PTR SS:[EBP-8]
002601B9   8B4D F4          MOV ECX,DWORD PTR SS:[EBP-C]
002601BC   3B48 18          CMP ECX,DWORD PTR DS:[EAX+18]
002601BF  ˅73 41            JNB SHORT 00260202
002601C1   6A 0E            PUSH 0E
002601C3   8D55 D8          LEA EDX,DWORD PTR SS:[EBP-28]
002601C6   52               PUSH EDX
002601C7   8B45 F0          MOV EAX,DWORD PTR SS:[EBP-10]
002601CA   8B08             MOV ECX,DWORD PTR DS:[EAX]
002601CC   034D 08          ADD ECX,DWORD PTR SS:[EBP+8]
002601CF   51               PUSH ECX
002601D0   E8 2B030000      CALL 00260500
002601D5   83C4 0C          ADD ESP,0C
002601D8   85C0             TEST EAX,EAX
002601DA  ˅75 1B            JNZ SHORT 002601F7
002601DC   8B55 F4          MOV EDX,DWORD PTR SS:[EBP-C]
002601DF   8B45 E8          MOV EAX,DWORD PTR SS:[EBP-18]
002601E2   0FB70C50         MOVZX ECX,WORD PTR DS:[EAX+EDX*2]
002601E6   894D EC          MOV DWORD PTR SS:[EBP-14],ECX
002601E9   8B55 EC          MOV EDX,DWORD PTR SS:[EBP-14]
002601EC   8B45 FC          MOV EAX,DWORD PTR SS:[EBP-4]
002601EF   8B0490           MOV EAX,DWORD PTR DS:[EAX+EDX*4]
002601F2   0345 08          ADD EAX,DWORD PTR SS:[EBP+8]
002601F5  ˅EB 0D            JMP SHORT 00260204
002601F7   8B4D F0          MOV ECX,DWORD PTR SS:[EBP-10]
002601FA   83C1 04          ADD ECX,4
002601FD   894D F0          MOV DWORD PTR SS:[EBP-10],ECX
00260200  ^EB AB            JMP SHORT 002601AD
00260202   33C0             XOR EAX,EAX
00260204   8BE5             MOV ESP,EBP
00260206   5D               POP EBP
00260207   C3               RETN
00260208   CC               INT3
```

Figure 85

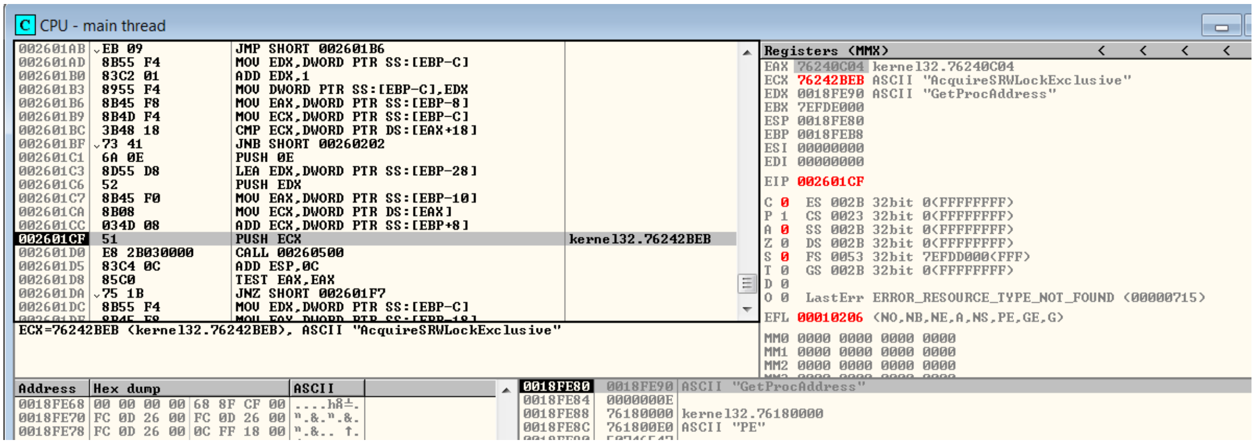


Figure 86

The function at 0x260500 is:

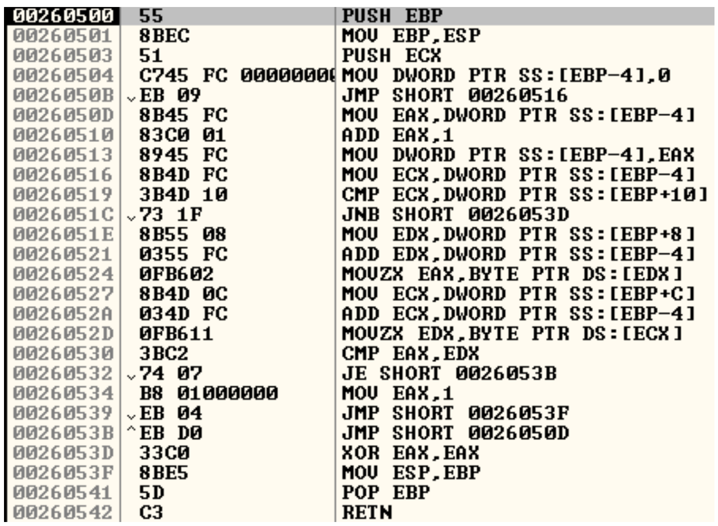


Figure 87

```
int function6(char *str1, char *str2) {
    int i = 0;
    while (1) {
        if (str1[i] == '\0' || str2[i] == '\0')
            break;
        if (str1[i] != str2[i])
            return 1;
        i++;
    }
    return 0;
}
```

This function looks like a simple string comparison.

As we move ahead, we see that multiple functions are loaded by the program like ActivateActCtx, Addatoma, AddConsoleAlias, AddIntegerLabelToBoundary, AddLocalAlternateComputerName and many more. It seems like all functions are getting loaded.

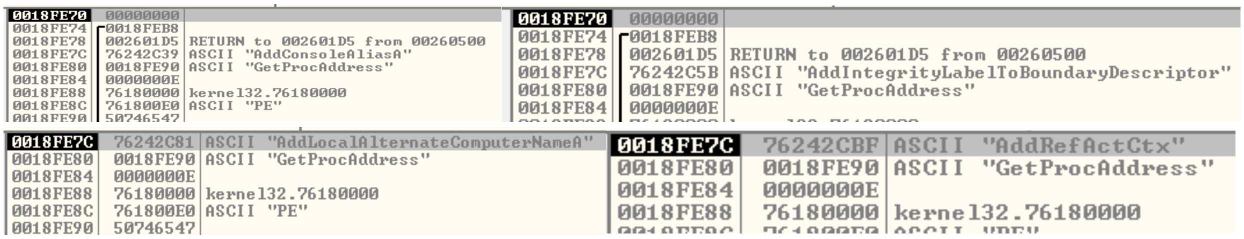


Figure 88

Our memory dump at 0x230000 now looks like:

Address	Hex dump	ASCII
00230000	33 33 33 00 00 00 00 00	333.....
00230008	00 00 00 00 00 00 00 00	....
00230010	00 47 65 74 4D 6F 64 75	.GetModu
00230018	6C 65 48 61 6E 64 6C 65	leHandle
00230020	41 00 57 72 69 74 65 46	A.WriteF
00230028	69 6C 65 00 00 00 00 00	ile.....
00230030	00 00 00 43 6C 6F 73 65	...Close
00230038	48 61 6E 64 6C 65 00 00	Handle..
00230040	00 00 00 00 56 69 72 74	....Virt
00230048	75 61 6C 46 72 65 65 00	ualFree.
00230050	00 00 00 00 00 55 6E 6D	.....Unm
00230058	61 70 56 69 65 77 4F 66	apViewOf
00230060	46 69 6C 65 00 00 47 65	File..Ge
00230068	74 50 72 6F 63 41 64 64	tProcAdd
00230070	72 65 73 73 00 00 00 56	ress...V
00230078	69 72 74 75 61 6C 41 6C	irtualAl
00230080	6C 6F 63 00 00 00 00 00	loc.....
00230088	4C 6F 61 64 4C 69 62 72	LoadLibr
00230090	61 72 79 45 78 41 00 00	aryExA..
00230098	00 53 65 74 46 69 6C 65	.SetFile
002300A0	50 6F 69 6E 74 65 72 00	Pointer.
002300A8	00 00 47 65 74 54 65 6D	..GetTem
002300B0	70 50 61 74 68 41 00 00	pPathA..
002300B8	00 00 00 56 69 72 74 75	...Virtu
002300C0	61 6C 50 72 6F 74 65 63	alProtec
002300C8	74 00 00 00 43 72 65 61	t...Crea
002300D0	74 65 46 69 6C 65 41 00	teFileA.
002300D8	00 00 00 00 00 6C 73 74	.....lst
002300E0	72 6C 65 6E 41 00 00 00	rlenA...
002300E8	00 00 00 00 00 00 6C 73	......ls
002300F0	74 72 63 61 74 41 00 00	trcatA..
002300F8	00 00 00 00 00 00 00 00	....
00230100	00 00 03 00 04 59 90 00	[illegible]

Figure 89

Finally, it encounters "GetProcAddress" again and leaves the stack.

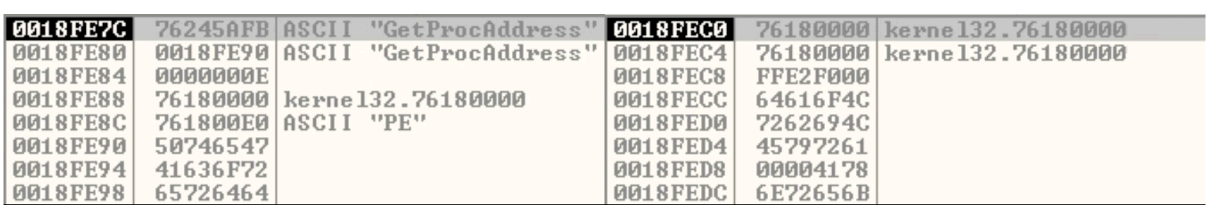


Figure 90

After performing some more imports from ntdll and kernel32 using LoadLibraryExA, the execution returns to the FUN_260210 at 0x2602C3. The program then gets information about the recently used directory (its own folder) and environment string. The execution then returns to 0x26030D after which kernel32's GetModuleHandleA, WriteFile, CloseHandle, VirtualFree, UnmapViewOfFile, VirtualAlloc, LoadLibraryExA, SetFilePointer, GetTempPathA, VirtualProtect, CreateFile are called.

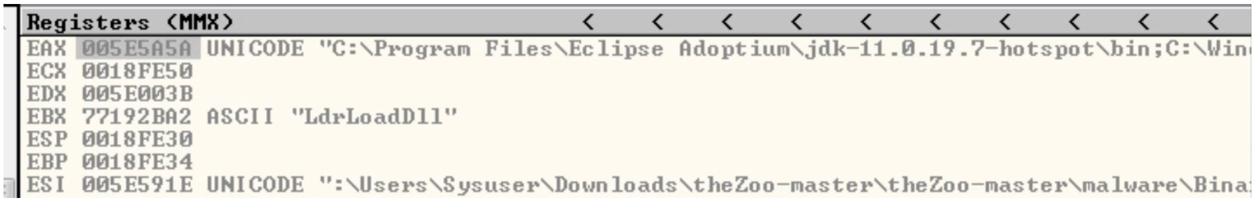


Figure 91

Again, the program performs more imports by calling function at address 0x260500 which we observe by setting breakpoint at 0x2601D0. When the function name matches GetProcAddress, it returns to 0x260BBC which is part of the function that starts at 0x260B20.

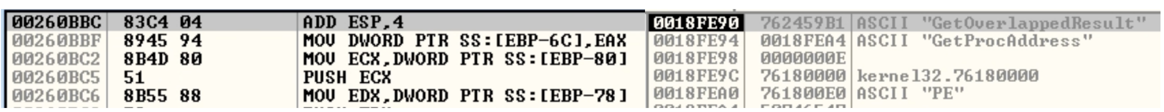
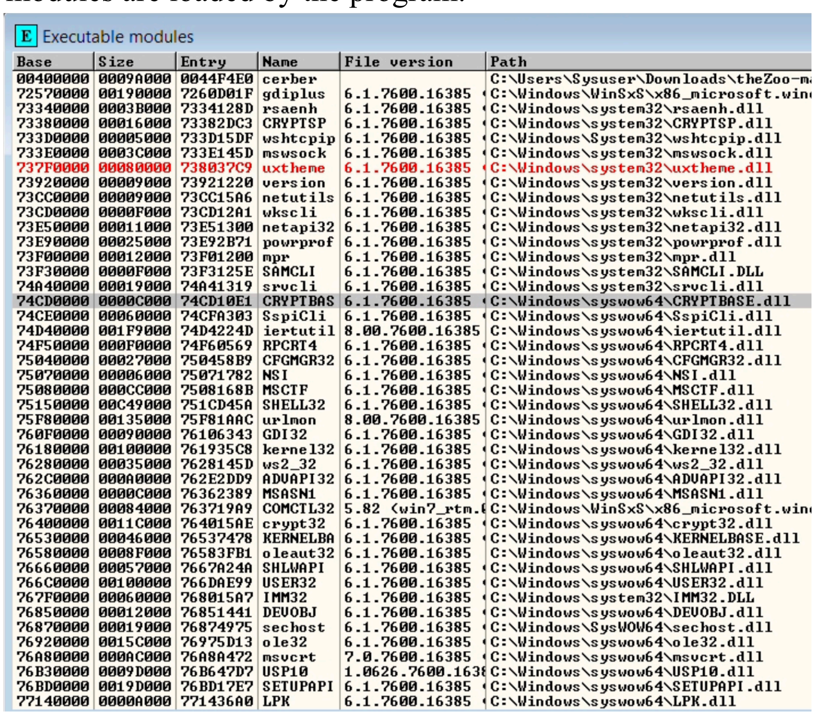


Figure 92

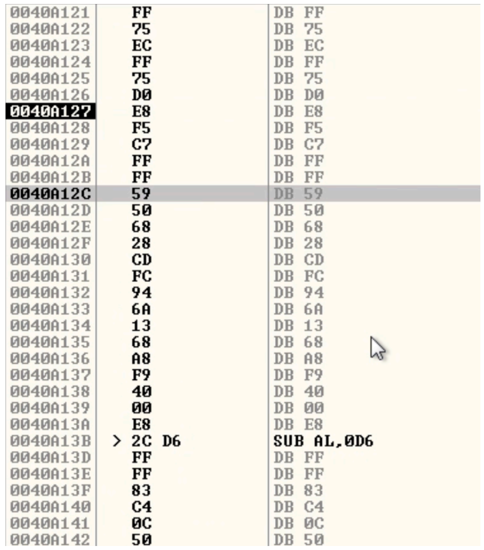
More executable modules are loaded by the program.


Executable modules

Base	Size	Entry	Name	File version	Path
00400000	0009A000	0044F4E0	cerber		C:\Users\Sysuser\Downloads\theZoo-ma
72570000	00190000	7260D01F	gdiplus	6.1.7600.16385	C:\Windows\WinSxS\x86_microsoft.win
73340000	0003B000	7334128D	rsaenh	6.1.7600.16385	C:\Windows\system32\rsaenh.dll
73380000	00016000	73382DC3	CRYPTSP	6.1.7600.16385	C:\Windows\system32\CRYPTSP.dll
733D0000	00005000	733D15DF	wshtcpip	6.1.7600.16385	C:\Windows\System32\wshtcpip.dll
733E0000	0003C000	733E145D	mswsock	6.1.7600.16385	C:\Windows\system32\mswsock.dll
737F0000	00080000	738037C9	uxtheme	6.1.7600.16385	C:\Windows\system32\uxtheme.dll
73920000	00009000	73921220	version	6.1.7600.16385	C:\Windows\system32\version.dll
73CC0000	00009000	73CC15A6	netutils	6.1.7600.16385	C:\Windows\system32\netutils.dll
73CD0000	0000F000	73CD12A1	wkscli	6.1.7600.16385	C:\Windows\system32\wkscli.dll
73E50000	00011000	73E51300	netapi32	6.1.7600.16385	C:\Windows\system32\netapi32.dll
73E90000	00025000	73E92B71	powrprof	6.1.7600.16385	C:\Windows\system32\powrprof.dll
73F00000	00012000	73F01200	mpr	6.1.7600.16385	C:\Windows\system32\mpr.dll
73F30000	0000F000	73F3125E	SAMCLI	6.1.7600.16385	C:\Windows\system32\SAMCLI.DLL
74A40000	00019000	74A41319	srvcli	6.1.7600.16385	C:\Windows\system32\srvcli.dll
74CD0000	0000C000	74CD10E1	CRYPTBAS	6.1.7600.16385	C:\Windows\syswow64\CRYPTBASE.dll
74CE0000	00060000	74CFA303	SspiCli	6.1.7600.16385	C:\Windows\syswow64\SspiCli.dll
74D40000	001F9000	74D4224D	iertutil	8.00.7600.16385	C:\Windows\syswow64\iertutil.dll
74F50000	000F0000	74F60569	RPCRT4	6.1.7600.16385	C:\Windows\syswow64\RPCRT4.dll
75040000	00027000	750458B9	CFGMGR32	6.1.7600.16385	C:\Windows\syswow64\CFGMGR32.dll
75070000	00006000	75071782	NSI	6.1.7600.16385	C:\Windows\syswow64\NSI.dll
75080000	000CC000	7508168B	MSCTF	6.1.7600.16385	C:\Windows\syswow64\MSCTF.dll
75150000	00C49000	751CD45A	SHELL32	6.1.7600.16385	C:\Windows\syswow64\SHELL32.dll
75F80000	00135000	75F81AAC	urlmon	8.00.7600.16385	C:\Windows\syswow64\urlmon.dll
760F0000	00090000	76106343	GDI32	6.1.7600.16385	C:\Windows\syswow64\GDI32.dll
76180000	00100000	761935C8	kernel32	6.1.7600.16385	C:\Windows\syswow64\kernel32.dll
76280000	00035000	7628145D	ws2_32	6.1.7600.16385	C:\Windows\syswow64\ws2_32.dll
762C0000	000A0000	762E2DD9	ADVAPI32	6.1.7600.16385	C:\Windows\syswow64\ADVAPI32.dll
76360000	0000C000	76362389	MSASN1	6.1.7600.16385	C:\Windows\syswow64\MSASN1.dll
76370000	00084000	763719A9	COMCTL32	5.82 (win7_rtm.	C:\Windows\WinSxS\x86_microsoft.win
76400000	0011C000	764015AE	crypt32	6.1.7600.16385	C:\Windows\syswow64\crypt32.dll
76530000	00046000	76537478	KERNELBA	6.1.7600.16385	C:\Windows\syswow64\KERNELBASE.dll
76580000	0008F000	76583FB1	oleaut32	6.1.7600.16385	C:\Windows\syswow64\oleaut32.dll
76660000	00057000	7667A24A	SHLWAPI	6.1.7600.16385	C:\Windows\syswow64\SHLWAPI.dll
766C0000	00100000	766DAE99	USER32	6.1.7600.16385	C:\Windows\syswow64\USER32.dll
767F0000	00060000	768015A7	IMM32	6.1.7600.16385	C:\Windows\system32\IMM32.DLL
76850000	00012000	76851441	DEVOBJ	6.1.7600.16385	C:\Windows\syswow64\DEVOBJ.dll
76870000	00019000	76874975	sechost	6.1.7600.16385	C:\Windows\SysWOW64\sechost.dll
76920000	0015C000	76975D13	ole32	6.1.7600.16385	C:\Windows\syswow64\ole32.dll
76A80000	000AC000	76A8A472	msvcrt	7.0.7600.16385	C:\Windows\syswow64\msvcrt.dll
76B30000	0009D000	76B647D7	USP10	1.0626.7600.1638	C:\Windows\syswow64\USP10.dll
76BD0000	0019D000	76BD17E7	SETUPAPI	6.1.7600.16385	C:\Windows\syswow64\SETUPAPI.dll
77140000	0000A000	771436A0	LPK	6.1.7600.16385	C:\Windows\syswow64\LPK.dll

Figure 93

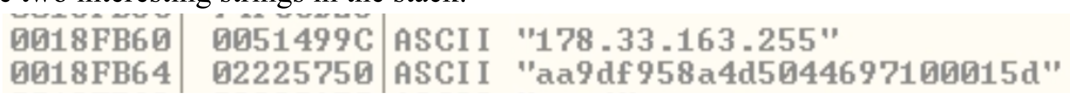
When we keep executing further, we see that instructions of original file which were visible in static analysis are no longer same as the original file.



```
0040A121   FF       DB FF
0040A122   75       DB 75
0040A123   EC       DB EC
0040A124   FF       DB FF
0040A125   75       DB 75
0040A126   D0       DB D0
0040A127   E8       DB E8
0040A128   F5       DB F5
0040A129   C7       DB C7
0040A12A   FF       DB FF
0040A12B   FF       DB FF
0040A12C   59       DB 59
0040A12D   50       DB 50
0040A12E   68       DB 68
0040A12F   28       DB 28
0040A130   CD       DB CD
0040A131   FC       DB FC
0040A132   94       DB 94
0040A133   6A       DB 6A
0040A134   13       DB 13
0040A135   68       DB 68
0040A136   A8       DB A8
0040A137   F9       DB F9
0040A138   40       DB 40
0040A139   00       DB 00
0040A13A   E8       DB E8
0040A13B > 2C D6    SUB AL,0D6
0040A13D   FF       DB FF
0040A13E   FF       DB FF
0040A13F   83       DB 83
0040A140   C4       DB C4
0040A141   0C       DB 0C
0040A142   50       DB 50
```

Figure 94

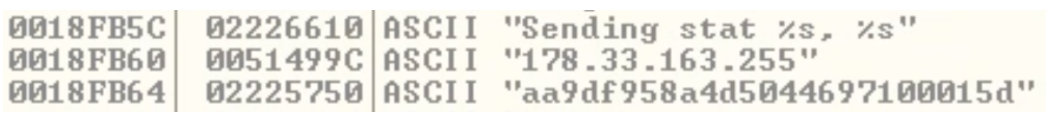
We see two interesting strings in the stack:



```
0018FB60  0051499C ASCII "178.33.163.255"
0018FB64  02225750 ASCII "aa9df958a4d5044697100015d"
```

Figure 95

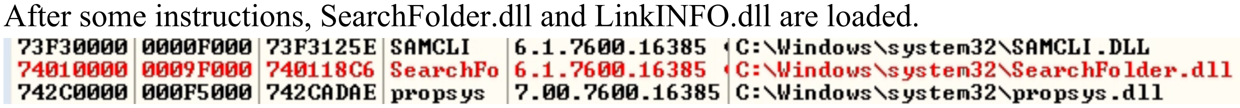
178.33.163.255 looks like the control server address. The other one is the message which is sent to the server using UDP. These are the same values which were observed in basic dynamic analysis.



```
0018FB5C  02226610 ASCII "Sending stat %s, %s"
0018FB60  0051499C ASCII "178.33.163.255"
0018FB64  02225750 ASCII "aa9df958a4d5044697100015d"
```

Figure 96

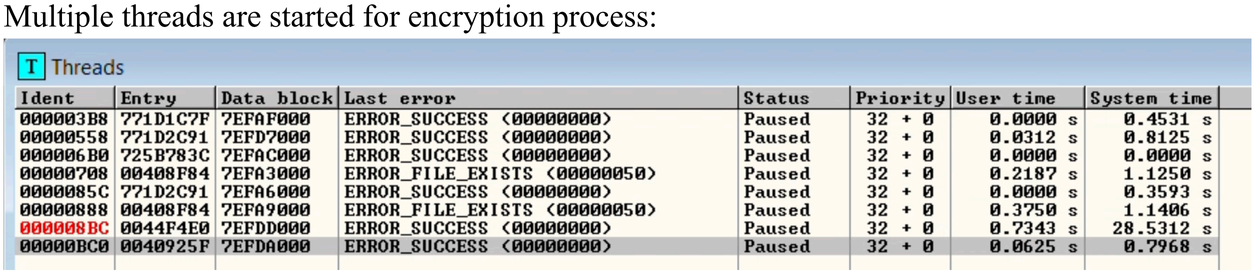
After some instructions, SearchFolder.dll and LinkINFO.dll are loaded.



73F30000	0000F000	73F3125E	SAMCLI	6.1.7600.16385	C:\Windows\system32\SAMCLI.DLL
74010000	0009F000	740118C6	SearchFo	6.1.7600.16385	C:\Windows\system32\SearchFolder.dll
742C0000	000F5000	742CADAE	propsys	7.00.7600.16385	C:\Windows\system32\propsys.dll

Figure 97

Multiple threads are started for encryption process:



Threads

Ident	Entry	Data block	Last error	Status	Priority	User time	System time
000003B8	771D1C7F	7EFAF000	ERROR_SUCCESS (00000000)	Paused	32 + 0	0.0000 s	0.4531 s
00000558	771D2C91	7EFD7000	ERROR_SUCCESS (00000000)	Paused	32 + 0	0.0312 s	0.8125 s
000006B0	725B783C	7EFAC000	ERROR_SUCCESS (00000000)	Paused	32 + 0	0.0000 s	0.0000 s
00000708	00408F84	7EFA3000	ERROR_FILE_EXISTS (00000050)	Paused	32 + 0	0.2187 s	1.1250 s
0000085C	771D2C91	7EFA6000	ERROR_SUCCESS (00000000)	Paused	32 + 0	0.0000 s	0.3593 s
00000888	00408F84	7EFA9000	ERROR_FILE_EXISTS (00000050)	Paused	32 + 0	0.3750 s	1.1406 s
000008BC	0044F4E0	7EFDD000	ERROR_SUCCESS (00000000)	Paused	32 + 0	0.7343 s	28.5312 s
00000BC0	0040925F	7EFDA000	ERROR_SUCCESS (00000000)	Paused	32 + 0	0.0625 s	0.7968 s

Figure 98

Encrypted files example:

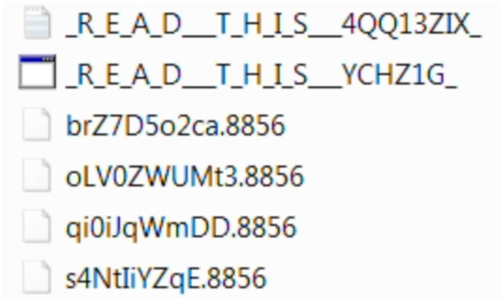


Figure 99

It is important to note that the extension 8856 is not random. Looking back on registry queries, we see that 8856 is part of the Machine GUID:

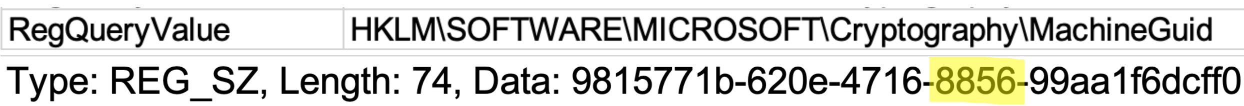
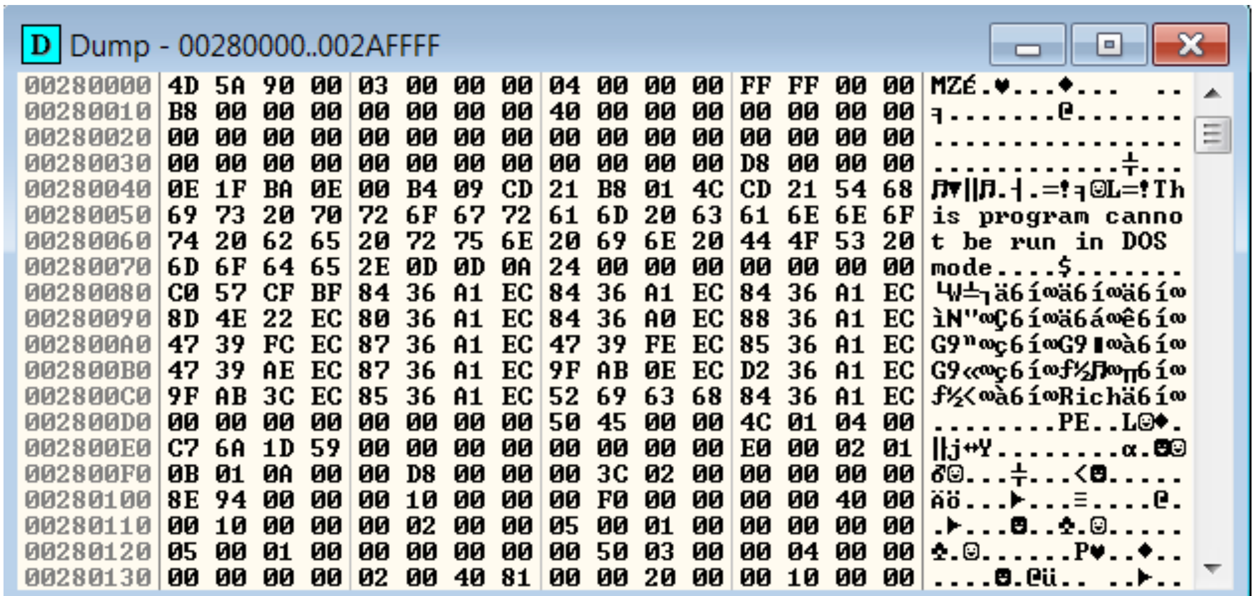


Figure 100

System files of an operating system (OS) are not encrypted, maybe to allow OS booting and display ransom note. After examining the newly created sections in memory dump, it looks like the dump starting at 0x280000 is the actual payload of the application.



Let's dump the payload and load it in Ghidra to further examine:

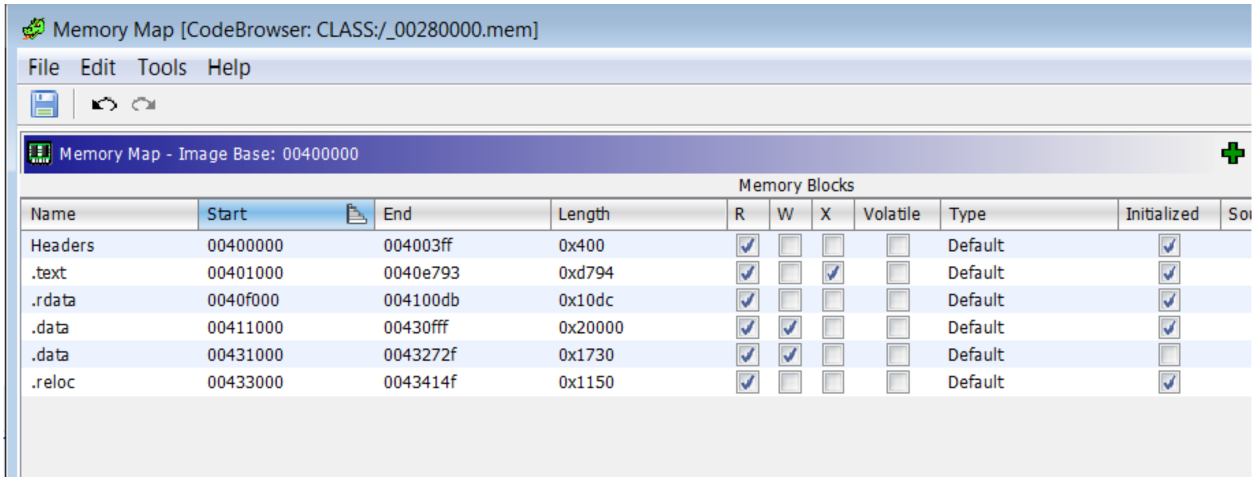
```
Project File Name:           _00280000.mem
Last Modified:               Tue Apr 30 17:06:21 PDT 2024
Readonly:                    false
Program Name:                _00280000.mem
Language ID:                 x86:LE:32:default (2.8)
Compiler ID:                 windows
Processor:                   x86
Endian:                      Little
Address Size:                32
Minimum Address:             00400000
Maximum Address:             0043414f
# of Bytes:                  201968
# of Memory Blocks:          6
# of Instructions:           0
# of Defined Data:           1715
# of Functions:              8
# of Symbols:                12
# of Data Types:             24
# of Data Type Categories:   3
Compiler:                    visualstudio:unknown
Created With Ghidra Version: 9.0.1
Date Created:                Tue Apr 30 17:06:16 PDT 2024
Executable Format:           Portable Executable (PE)
Executable Location:         C:/Users/Sysuser/Desktop/_00280000/_00280000.mem
Executable MD5:              ab0953388bf5b63bbc85cd10a7b73022
FSRL:                        file://C:/Users/Sysuser/Desktop/_00280000/_00280000.mem?MD5=ab0953388bf5b63
Relocatable:                 true
SectionAlignment:            4096
```

These are the strings found in the payload:

Defined Strings - 35 items

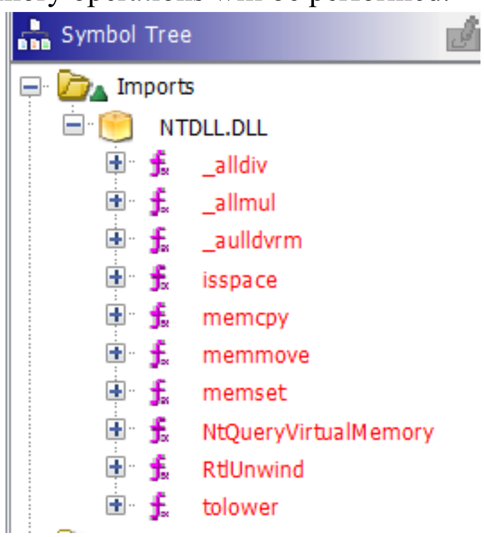
Location	String Value	String Representation	Data Type
00400220	.data	".data"	char[8]
004001f8	.rdata	".rdata"	char[8]
00400248	.reloc	".reloc"	char[8]
004001d0	.text	".text"	char[8]
004100b0	_alldiv	"_alldiv"	ds
004100a6	_allmul	"_allmul"	ds
00410086	_aulldvrm	"_aulldvrm"	ds
0040fd80	advapi32.dll	"advapi32.dll"	ds
0040f5c0	Broken file found!%s	u"Broken file found!\r\n...	unicode
0040fd90	crypt32.dll	"crypt32.dll"	ds
0040fd9c	gdi32.dll	"gdi32.dll"	ds
0040fda8	gdiplus.dll	"gdiplus.dll"	ds
00410068	isspace	"isspace"	ds
0040fdb4	kernel32.dll	"kernel32.dll"	ds
0041009c	memcpy	"memcpy"	ds
0041005e	memmove	"memmove"	ds
00410092	memset	"memset"	ds
0040fdc4	mpr.dll	"mpr.dll"	ds
00400000	MZ	"MZ"	char[2]
0040fdcc	netapi32.dll	"netapi32.dll"	ds
0040fbb8	ntdll.dll	"ntdll.dll"	ds
0041007a	ntdll.dll	"ntdll.dll"	ds
004100c6	NtQueryVirtualMemory	"NtQueryVirtualMemory"	ds
0040fddc	ole32.dll	"ole32.dll"	ds
0040fde8	oleaut32.dll	"oleaut32.dll"	ds
004000d8	PE	"PE"	char[4]
0040fdf8	powrprof.dll	"powrprof.dll"	ds
004100ba	RtlUnwind	"RtlUnwind"	ds
0040fe08	shell32.dll	"shell32.dll"	ds
0040fe14	shlwapi.dll	"shlwapi.dll"	ds
00410072	tolower	"tolower"	ds
0040fe20	urlmon.dll	"urlmon.dll"	ds
0040fe2c	user32.dll	"user32.dll"	ds
0040fe38	version.dll	"version.dll"	ds
0040fe44	ws2_32.dll	"ws2_32.dll"	ds

Memory map:

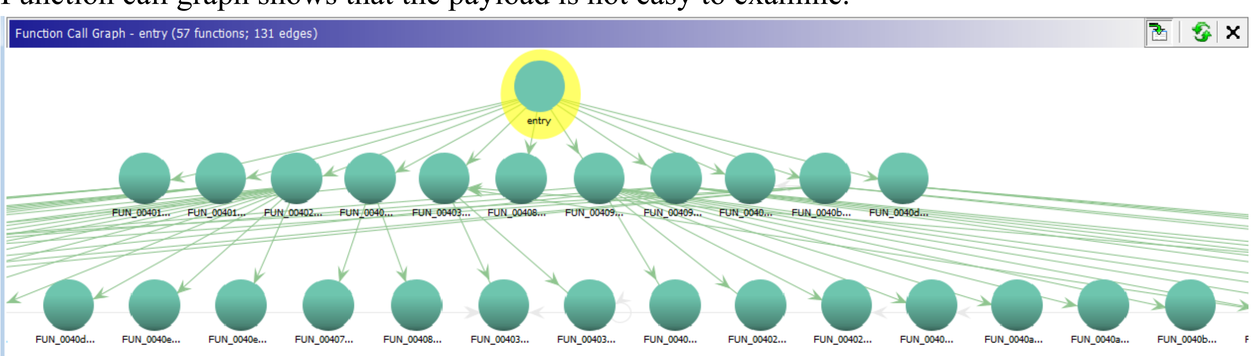


Name	Start	End	Length	R	W	X	Volatile	Type	Initialized	So
Headers	00400000	004003ff	0x400	✓				Default	✓	
.text	00401000	0040e793	0xd794	✓		✓		Default	✓	
.rdata	0040f000	004100db	0x10dc	✓				Default	✓	
.data	00411000	00430fff	0x20000	✓	✓			Default	✓	
.data	00431000	0043272f	0x1730	✓	✓			Default		
.reloc	00433000	0043414f	0x1150	✓				Default	✓	

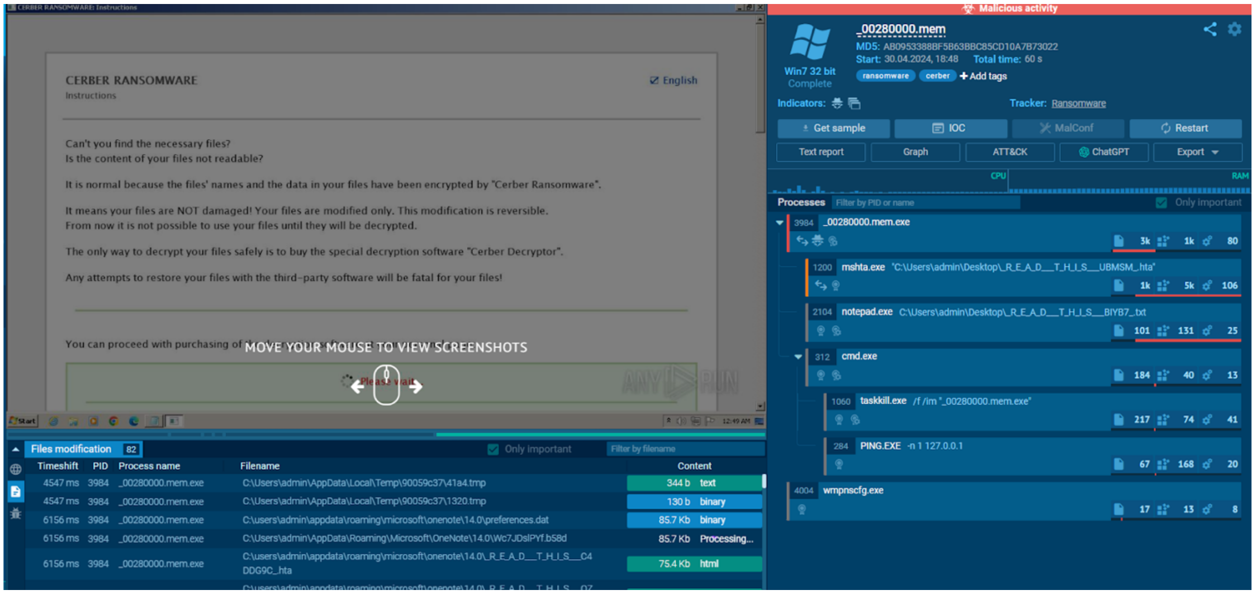
Imports show that a lot of memory operations will be performed.



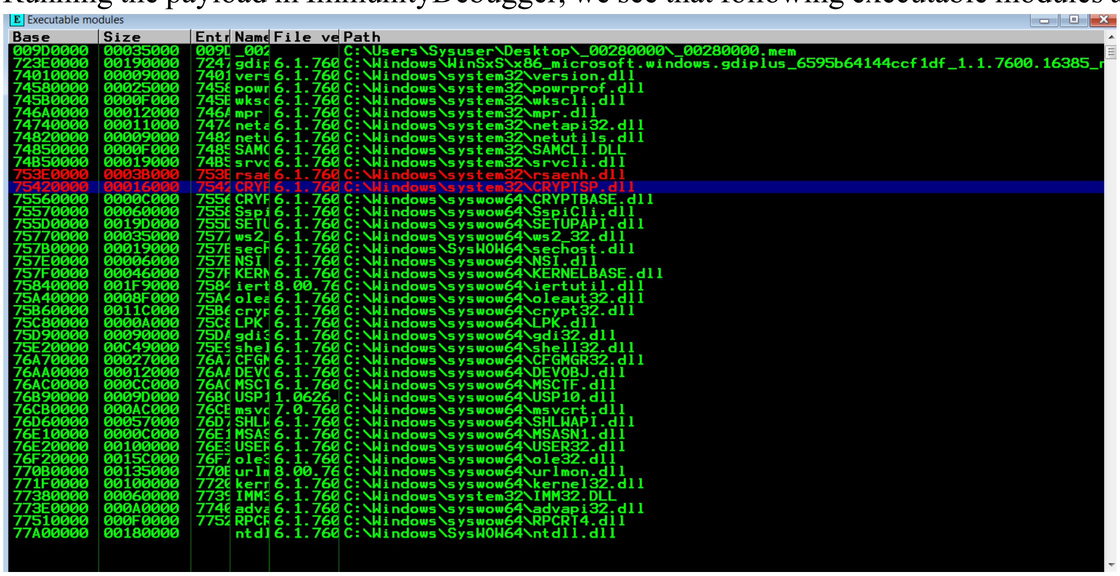
Function call graph shows that the payload is not easy to examine.



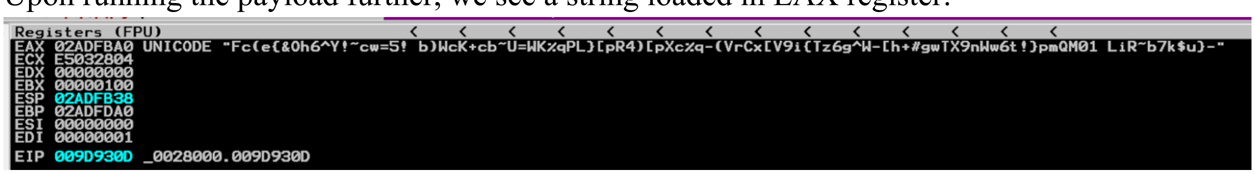
Since multiple memory sections were modified, we will confirm if this is the desired payload or not. Running the payload on any.run (https://app.any.run/tasks/89e938c5-3103-4dec-915b-39eb5e5d3fd4/) confirms that this is the malicious portion of the original cerber.exe. Note that the wallpaper is not changed while running this payload which means that the parent program cerber.exe is responsible for the side-work.



Running the payload in ImmunityDebugger, we see that following executable modules are loaded:



Upon running the payload further, we see a string loaded in EAX register:



"Fc(e{&Oh6^Y!~cw=5! b)WcK+cb~U=WK%qPL}[pR4)[pXc%q-(VrCx[V9i{Tz6g^W-[h+#gwTX9nWw6t!}pmQM01 LiR~b7k$u}-". It is hard to say if this is the real encryption key or not but this is something which is used by the payload multiple times during execution.

It is hard to identify functions from Ghidra directly, so using references from Immunity Debugger we see that in entry function, CreateMutex (*_DAT_00411428) is called.

```
009D948E ┌$ 55             PUSH EBP
009D948F │. 8BEC           MOV EBP,ESP
009D9491 │. 83E4 F8        AND ESP,FFFFFFF8
009D9494 │. 81EC A8020000  SUB ESP,2A8
009D949A │. 56             PUSH ESI
009D949B │. 57             PUSH EDI
009D949C │. E8 EA440000    CALL _0028000.009DD98B
009D94A1 │. 84C0           TEST AL,AL
009D94A3 │. 0F84 00010000  JE _0028000.009D95A9
009D94A9 │. 8D4424 08      LEA EAX,DWORD PTR SS:[ESP+8]
009D94AD │. 50             PUSH EAX
009D94AE │. E8 3C9BFFFF    CALL _0028000.009D2FEF
009D94B3 │. 59             POP ECX
009D94B4 │. 8D4424 08      LEA EAX,DWORD PTR SS:[ESP+8]
009D94B8 │. 50             PUSH EAX
009D94B9 │. 33F6           XOR ESI,ESI
009D94BB │. 56             PUSH ESI
009D94BC │. 56             PUSH ESI
009D94BD │. FF15 28149E00  CALL DWORD PTR DS:[9E1428]       kernel32.CreateMutexW
009D94C3 │. FF15 40149E00  CALL DWORD PTR DS:[9E1440]       kernel32.GetLastError
009D94C9 │. 3D B7000000    CMP EAX,0B7
009D94CE │. 0F84 D0000000  JE _0028000.009D95A4
009D94D4 │. 68 07800000    PUSH 8007
009D94D9 │. FF15 2C149E00  CALL DWORD PTR DS:[9E142C]       kernel32.SetErrorMode
009D94DF │. 56             PUSH ESI
009D94E0 │. FF15 30149E00  CALL DWORD PTR DS:[9E1430]       kernel32.GetModuleHandleA
009D94E6 │. 68 04010000    PUSH 104
009D94EB │. 68 2811A000    PUSH _0028000.00A01128           UNICODE "C:\Users\Sysuser\Desktop\_00280000
009D94F0 │. 56             PUSH ESI
```

```
uVar1 = FUN_0040d98b();
if ((char)uVar1 != 0) {
  FUN_00402fef(this,local_2b0);
  (*_DAT_00411428)(0,0,local_2b0);
  iVar2 = (*_DAT_00411440)();
  if (iVar2 != 0xb7) {
    (*_DAT_0041142c)(0x8007);
    DAT_00431120 = (*_DAT_00411430)(0);
```

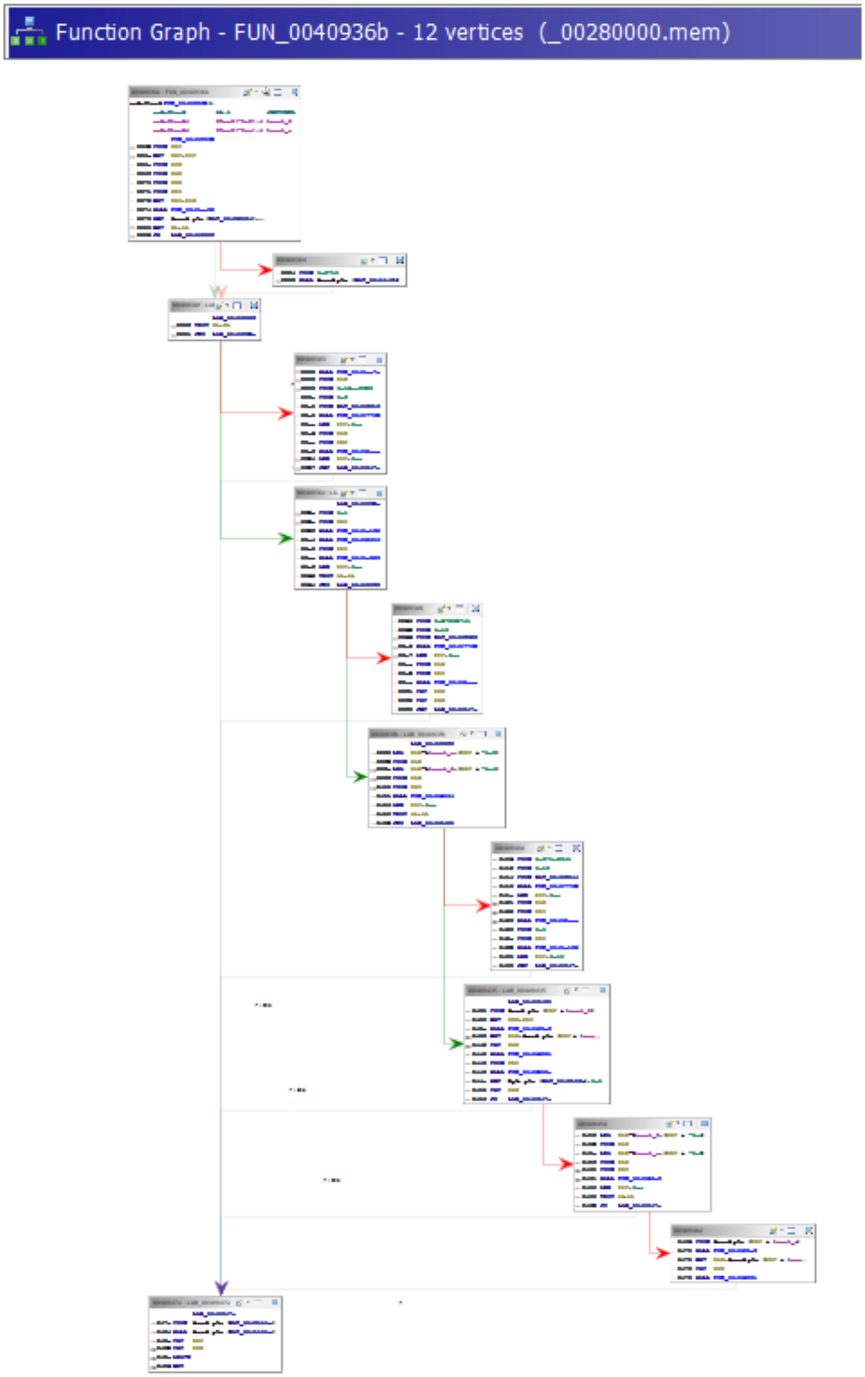
It also checks the error while creating mutex, if no error then it proceeds otherwise it means that the program has already infected the machine and thus it exits. Further analysis shows that this payload creates threads to run the encryption algorithm:

```
. 50             PUSH EAX
. 68 02020000    PUSH 202
. FF15 0C109E00  CALL DWORD PTR DS:[9E100C]          ws2_32.WSAStartup
. 56             PUSH ESI
. 56             PUSH ESI
. 6A 01          PUSH 1
. 56             PUSH ESI
. FF15 FC139E00  CALL DWORD PTR DS:[9E13FC]          kernel32.CreateEventW
. 56             PUSH ESI
. 56             PUSH ESI
. 56             PUSH ESI
. 68 5F929D00    PUSH _0028000.009D925F
. 56             PUSH ESI
. 56             PUSH ESI
. A3 1C11A000    MOV DWORD PTR DS:[A0111C],EAX
. FF15 EC149E00  CALL DWORD PTR DS:[9E14EC]          kernel32.CreateThread
. 8BF0           MOV ESI,EAX
. 8BC7           MOV EAX,EDI
. E8 F1FDFFFF    CALL _0028000.009D936B
. 6A FF          PUSH -1
. 56             PUSH ESI
. FF15 24159E00  CALL DWORD PTR DS:[9E1524]          kernel32.WaitForSingleObject
. 56             PUSH ESI
. FF15 60159E00  CALL DWORD PTR DS:[9E1560]          kernel32.CloseHandle
. FF35 1C11A000  PUSH DWORD PTR DS:[A0111C]
```

In Ghidra, this is the corresponding code for kernel32.CreateThread.

```
iVar4 = (*_DAT_004114ec)(0,0,&LAB_0040925f,0,0,0);
```

Right after creating the thread, encryption function is called, and program waits for its completion (kernel32.WaitForSingleObject) before executing further. The encryption function is FUN_0040936b; its function call graph is complicated and contains 12 vertices:



However, it seems that a file is loaded at different offsets into the memory, then on each chunk encryption is performed. These encrypted chunks overwrite the original files on the same offsets. Finally, the file is renamed based on the Machine GUID (as discussed above).

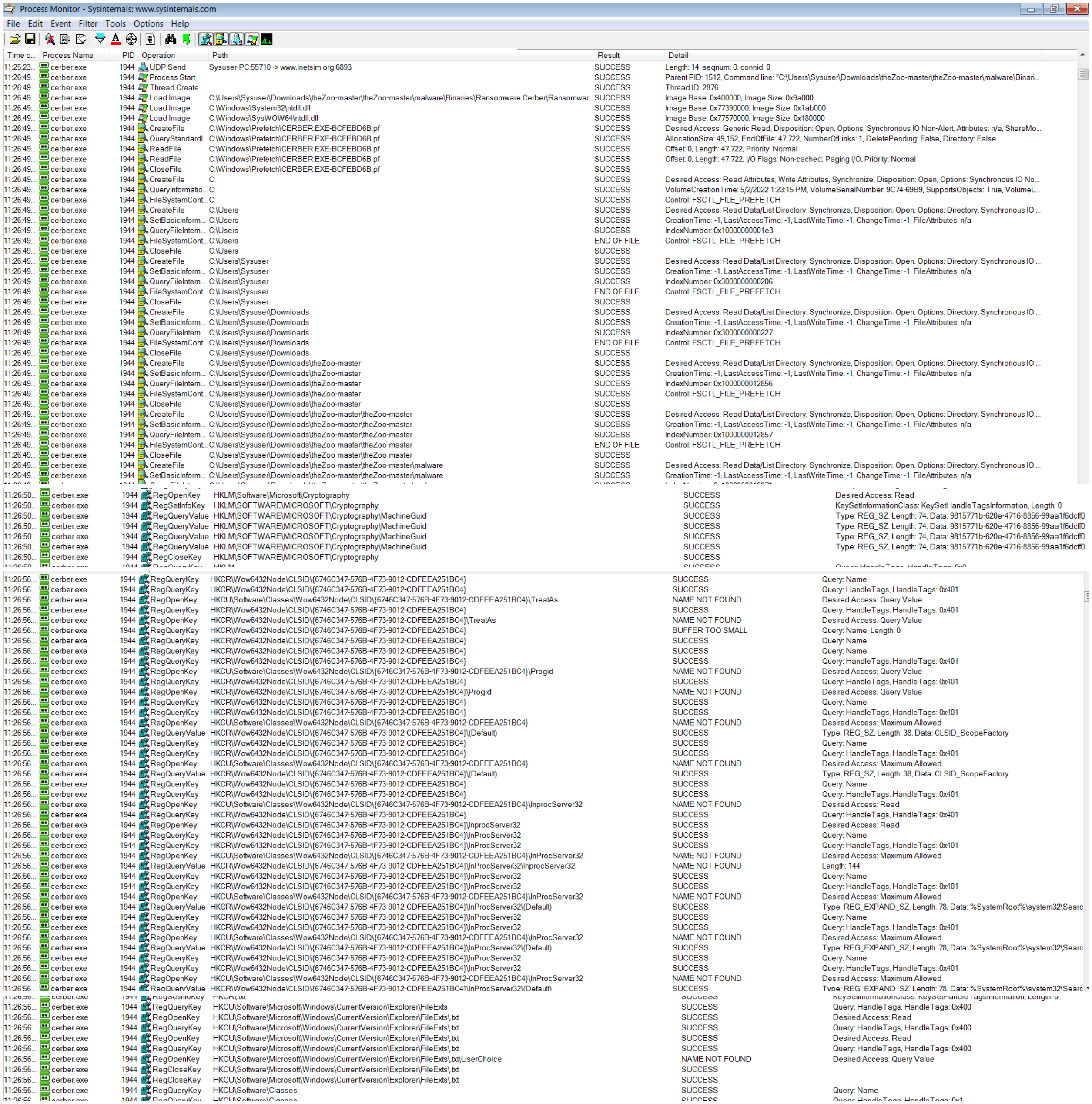
Steps after infection

It is clear that cerber.exe is a ransomware. There were no significant registry changes. There is no background process which is running after execution except notepad and mshta which just display the ransom note. The program deletes itself after execution. We can try to delete the .hta and .txt ransom note files created in the all the subdirectories. As per my understanding, the encryption algorithm is not simple and so it is not possible to decrypt files. It seems that the only way to decrypt the files is by using the key. I tried searching for online resources for decryptor tools for Cerber but there are no legitimate tools available. A YouTube video showed that the URL present in the ransom note allows converting one file to original form for free. However, visiting the URL or paying ransom is not a good option in any case. We can try to restore our system using backup files (stored in a secure place). Currently, Windows security system identifies Cerber as soon as it is downloaded so it is unlikely to infect the machine if system protection settings are in place. However, there are new versions of Cerber are available in market (ransomware-as-a-service). So, it is recommended to use antivirus and keep the system updated to protect against these attacks.

Appendix

Procmon Screenshots:

Time o...	Process Name	PID	Operation	Path	Result	Detail
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0
11:24:12...	cerber.exe	1944	UDP Send	Sysuser-PC:51909 -> www.inetsim.org:6893	SUCCESS	Length: 25, seqnum: 0, connid: 0



Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time o...	Process Name	PID	Operation	Path	Result	Detail
11:25:23...	cerber.exe	1944	UDP Send	Sysuser-PC:55710 -> www.inetsim.org:6893	SUCCESS	Length: 14, seqnum: 0, connid: 0
11:26:49...	cerber.exe	1944	Process Start		SUCCESS	Parent PID: 1512, Command line: "C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master\malware\Binari...
11:26:49...	cerber.exe	1944	Thread Create		SUCCESS	Thread ID: 2876
11:26:49...	cerber.exe	1944	Load Image	C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master\malware\Binaries\Ransomware.Cerber\Ransomwar...	SUCCESS	Image Base: 0x400000, Image Size: 0x9a000
11:26:49...	cerber.exe	1944	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x77390000, Image Size: 0x1ab000
11:26:49...	cerber.exe	1944	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77570000, Image Size: 0x180000
11:26:49...	cerber.exe	1944	CreateFile	C:\Windows\Prefetch\CERBER.EXE-BCFEBD6B.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMo...
11:26:49...	cerber.exe	1944	QueryStandardI...	C:\Windows\Prefetch\CERBER.EXE-BCFEBD6B.pf	SUCCESS	AllocationSize: 49,152, EndOfFile: 47,722, NumberOfLinks: 1, DeletePending: False, Directory: False
11:26:49...	cerber.exe	1944	ReadFile	C:\Windows\Prefetch\CERBER.EXE-BCFEBD6B.pf	SUCCESS	Offset: 0, Length: 47,722, Priority: Normal
11:26:49...	cerber.exe	1944	ReadFile	C:\Windows\Prefetch\CERBER.EXE-BCFEBD6B.pf	SUCCESS	Offset: 0, Length: 47,722, I/O Flags: Non-cached, Paging I/O, Priority: Normal
11:26:49...	cerber.exe	1944	CloseFile	C:\Windows\Prefetch\CERBER.EXE-BCFEBD6B.pf	SUCCESS	
11:26:49...	cerber.exe	1944	CreateFile	C:	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO No...
11:26:49...	cerber.exe	1944	QueryInformatio...	C:	SUCCESS	VolumeCreationTime: 5/2/2022 1:23:15 PM, VolumeSerialNumber: 9C74-69B9, SupportsObjects: True, VolumeL...
11:26:49...	cerber.exe	1944	FileSystemCont...	C:	SUCCESS	Control: FSCTL_FILE_PREFETCH
11:26:49...	cerber.exe	1944	CreateFile	C:\Users	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO ...
11:26:49...	cerber.exe	1944	SetBasicInform...	C:\Users	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime: -1, ChangeTime: -1, FileAttributes: n/a
11:26:49...	cerber.exe	1944	QueryFileIntern...	C:\Users	SUCCESS	IndexNumber: 0x10000000001e3
11:26:49...	cerber.exe	1944	FileSystemCont...	C:\Users	END OF FILE	Control: FSCTL_FILE_PREFETCH
11:26:49...	cerber.exe	1944	CloseFile	C:\Users	SUCCESS	
11:26:49...	cerber.exe	1944	CreateFile	C:\Users\Sysuser	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO ...
11:26:49...	cerber.exe	1944	SetBasicInform...	C:\Users\Sysuser	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime: -1, ChangeTime: -1, FileAttributes: n/a
11:26:49...	cerber.exe	1944	QueryFileIntern...	C:\Users\Sysuser	SUCCESS	IndexNumber: 0x3000000000206
11:26:49...	cerber.exe	1944	FileSystemCont...	C:\Users\Sysuser	END OF FILE	Control: FSCTL_FILE_PREFETCH
11:26:49...	cerber.exe	1944	CloseFile	C:\Users\Sysuser	SUCCESS	
11:26:49...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\Downloads	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO ...
11:26:49...	cerber.exe	1944	SetBasicInform...	C:\Users\Sysuser\Downloads	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime: -1, ChangeTime: -1, FileAttributes: n/a
11:26:49...	cerber.exe	1944	QueryFileIntern...	C:\Users\Sysuser\Downloads	SUCCESS	IndexNumber: 0x3000000000227
11:26:49...	cerber.exe	1944	FileSystemCont...	C:\Users\Sysuser\Downloads	END OF FILE	Control: FSCTL_FILE_PREFETCH
11:26:49...	cerber.exe	1944	CloseFile	C:\Users\Sysuser\Downloads	SUCCESS	
11:26:49...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\Downloads\theZoo-master	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO ...
11:26:49...	cerber.exe	1944	SetBasicInform...	C:\Users\Sysuser\Downloads\theZoo-master	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime: -1, ChangeTime: -1, FileAttributes: n/a
11:26:49...	cerber.exe	1944	QueryFileIntern...	C:\Users\Sysuser\Downloads\theZoo-master	SUCCESS	IndexNumber: 0x1000000012856
11:26:49...	cerber.exe	1944	FileSystemCont...	C:\Users\Sysuser\Downloads\theZoo-master	SUCCESS	Control: FSCTL_FILE_PREFETCH
11:26:49...	cerber.exe	1944	CloseFile	C:\Users\Sysuser\Downloads\theZoo-master	SUCCESS	
11:26:49...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO ...
11:26:49...	cerber.exe	1944	SetBasicInform...	C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime: -1, ChangeTime: -1, FileAttributes: n/a
11:26:49...	cerber.exe	1944	QueryFileIntern...	C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master	SUCCESS	IndexNumber: 0x1000000012857
11:26:49...	cerber.exe	1944	FileSystemCont...	C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master	END OF FILE	Control: FSCTL_FILE_PREFETCH
11:26:49...	cerber.exe	1944	CloseFile	C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master	SUCCESS	
11:26:49...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master\malware	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO ...
11:26:49...	cerber.exe	1944	SetBasicInform...	C:\Users\Sysuser\Downloads\theZoo-master\theZoo-master\malware	SUCCESS	CreationTime: -1, LastAccessTime: -1, LastWriteTime: -1, ChangeTime: -1, FileAttributes: n/a

11:26:50...	cerber.exe	1944	RegOpenKey	HKLM\Software\Microsoft\Cryptography	SUCCESS	Desired Access: Read
11:26:50...	cerber.exe	1944	RegSetInfoKey	HKLM\SOFTWARE\MICROSOFT\Cryptography	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
11:26:50...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Cryptography\MachineGuid	SUCCESS	Type: REG_SZ, Length: 74, Data: 9815771b-620e-4716-8856-99aa1f6dcff0
11:26:50...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Cryptography\MachineGuid	SUCCESS	Type: REG_SZ, Length: 74, Data: 9815771b-620e-4716-8856-99aa1f6dcff0
11:26:50...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Cryptography\MachineGuid	SUCCESS	Type: REG_SZ, Length: 74, Data: 9815771b-620e-4716-8856-99aa1f6dcff0
11:26:50...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\Cryptography\MachineGuid	SUCCESS	Type: REG_SZ, Length: 74, Data: 9815771b-620e-4716-8856-99aa1f6dcff0
11:26:50...	cerber.exe	1944	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\Cryptography	SUCCESS	

11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\TreatAs	NAME NOT FOUND	Desired Access: Query Value
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\TreatAs	NAME NOT FOUND	Desired Access: Query Value
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	BUFFER TOO SMALL	Query: Name, Length: 0
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\Progid	NAME NOT FOUND	Desired Access: Query Value
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\Progid	NAME NOT FOUND	Desired Access: Query Value
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	NAME NOT FOUND	Desired Access: Maximum Allowed
11:26:56...	cerber.exe	1944	RegQueryValue	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\(Default)	SUCCESS	Type: REG_SZ, Length: 38, Data: CLSID_ScopeFactory
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	NAME NOT FOUND	Desired Access: Maximum Allowed
11:26:56...	cerber.exe	1944	RegQueryValue	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\(Default)	SUCCESS	Type: REG_SZ, Length: 38, Data: CLSID_ScopeFactory
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InprocServer32	NAME NOT FOUND	Desired Access: Read
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InprocServer32	SUCCESS	Desired Access: Read
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	NAME NOT FOUND	Desired Access: Maximum Allowed
11:26:56...	cerber.exe	1944	RegQueryValue	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32\InprocServer32	NAME NOT FOUND	Length: 144
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	NAME NOT FOUND	Desired Access: Maximum Allowed
11:26:56...	cerber.exe	1944	RegQueryValue	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32\(Default)	SUCCESS	Type: REG_EXPAND_SZ, Length: 78, Data: %SystemRoot%\system32\Searc
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	NAME NOT FOUND	Desired Access: Maximum Allowed
11:26:56...	cerber.exe	1944	RegQueryValue	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32\(Default)	SUCCESS	Type: REG_EXPAND_SZ, Length: 78, Data: %SystemRoot%\system32\Searc
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	SUCCESS	Query: Name
11:26:56...	cerber.exe	1944	RegQueryKey	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32	NAME NOT FOUND	Desired Access: Maximum Allowed
11:26:56...	cerber.exe	1944	RegQueryValue	HKCR\Wow6432Node\CLSID\{6746C347-576B-4F73-9012-CDFEEA251BC4}\InProcServer32\(Default)	SUCCESS	Type: REG_EXPAND_SZ, Length: 78, Data: %SystemRoot%\system32\Searc

11:26:56...	cerber.exe	1944	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts	SUCCESS	Query: HandleTags, HandleTags: 0x400
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt	SUCCESS	Desired Access: Read
11:26:56...	cerber.exe	1944	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt	SUCCESS	Query: HandleTags, HandleTags: 0x400
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt	SUCCESS	Desired Access: Read
11:26:56...	cerber.exe	1944	RegQueryKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt	SUCCESS	Query: HandleTags, HandleTags: 0x400
11:26:56...	cerber.exe	1944	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt\UserChoice	NAME NOT FOUND	Desired Access: Query Value
11:26:56...	cerber.exe	1944	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt	SUCCESS	
11:26:56...	cerber.exe	1944	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.txt	SUCCESS	
11:26:56...	cerber.exe	1944	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name

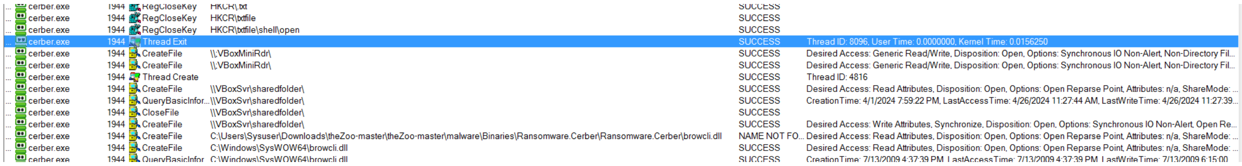
11:26:57...	cerber.exe	1944	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Op
11:26:57...	cerber.exe	1944	QueryDirectory	C:*	SUCCESS	Filter: *, 1: $Recycle.Bin
11:26:57...	cerber.exe	1944	CreateFile	C:\$Recycle.Bin	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\$Recycle.Bin	SUCCESS	CreationTime: 7/13/2009 8:18:56 PM, LastAccessTime: 5/2/2022 1:51:32 PM, La
11:26:57...	cerber.exe	1944	CloseFile	C:\$Recycle.Bin	SUCCESS	
11:26:57...	cerber.exe	1944	QueryDirectory	C:\	SUCCESS	0: Documents and Settings, 1: pagefile.sys, 2: PerfLogs, 3: Program Files, 4: Pr
11:26:57...	cerber.exe	1944	CreateFile	C:\PerfLogs	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\PerfLogs	SUCCESS	CreationTime: 7/13/2009 8:20:08 PM, LastAccessTime: 7/13/2009 8:20:08 PM, L
11:26:57...	cerber.exe	1944	CloseFile	C:\PerfLogs	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\PerfLogs	ACCESS DENIED	Desired Access: Read Control, Disposition: Open, Options: Open Reparse Po
11:26:57...	cerber.exe	1944	CreateFile	C:\PerfLogs	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\PerfLogs	SUCCESS	CreationTime: 7/13/2009 8:20:08 PM, LastAccessTime: 7/13/2009 8:20:08 PM, L
11:26:57...	cerber.exe	1944	CloseFile	C:\PerfLogs	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\PerfLogs	ACCESS DENIED	Desired Access: Write Attributes, Synchronize, Disposition: Open, Options: Syı
11:26:57...	cerber.exe	1944	CreateFile	C:\Program Files	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\Program Files	SUCCESS	CreationTime: 7/13/2009 8:20:08 PM, LastAccessTime: 7/27/2023 7:49:33 AM, L
11:26:57...	cerber.exe	1944	CloseFile	C:\Program Files	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Program Files	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Open Reparse Po
11:26:57...	cerber.exe	1944	QuerySecurityFi...	C:\Program Files	SUCCESS	Information: Owner
11:26:57...	cerber.exe	1944	CloseFile	C:\Program Files	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Program Files	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Op
11:26:57...	cerber.exe	1944	QueryDirectory	C:\Users\Public*	SUCCESS	Filter: *, 1: .
11:26:57...	cerber.exe	1944	QueryDirectory	C:\Users\Public	SUCCESS	0: .., 1: Desktop, 2: desktop.ini, 3: Documents, 4: Downloads, 5: Favorites, 6: Lib
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Desktop	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\Users\Public\Desktop	SUCCESS	CreationTime: 7/13/2009 8:20:08 PM, LastAccessTime: 9/21/2023 11:12:30 AM,
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Desktop	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Documents	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\Users\Public\Documents	SUCCESS	CreationTime: 7/13/2009 8:20:08 PM, LastAccessTime: 7/27/2023 1:52:17 PM, L
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Documents	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Documents	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Open Reparse Po
11:26:57...	cerber.exe	1944	QuerySecurityFi...	C:\Users\Public\Documents	SUCCESS	Information: Owner
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Documents	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Documents	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\Users\Public\Documents	SUCCESS	CreationTime: 7/13/2009 8:20:08 PM, LastAccessTime: 7/27/2023 1:52:17 PM, L
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Documents	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Documents	SUCCESS	Desired Access: Write Attributes, Synchronize, Disposition: Open, Options: Syı
11:26:57...	cerber.exe	1944	SetBasicInform...	C:\Users\Public\Documents	SUCCESS	CreationTime: 0, LastAccessTime: 0, LastWriteTime: 0, ChangeTime: 0, FileAtt
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Documents	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Documents	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Op
11:26:57...	cerber.exe	1944	QueryDirectory	C:\Users\Public\Documents*	SUCCESS	Filter: *, 1: .
11:26:57...	cerber.exe	1944	QueryDirectory	C:\Users\Public\Documents	SUCCESS	0: .., 1: desktop.ini, 2: Explorer Suite Signatures, 3: Lab03-01.exe, 4: My Music, 5
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Documents\Explorer Suite Signatures	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\Users\Public\Documents\Explorer Suite Signatures	SUCCESS	CreationTime: 7/27/2023 7:49:33 AM, LastAccessTime: 7/27/2023 7:49:33 AM, L
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Pictures	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Pictures	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Op
11:26:57...	cerber.exe	1944	QueryDirectory	C:\Users\Public\Pictures*	SUCCESS	Filter: *, 1: .
11:26:57...	cerber.exe	1944	QueryDirectory	C:\Users\Public\Pictures	SUCCESS	0: .., 1: desktop.ini, 2: Sample Pictures
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Pictures\Sample Pictures	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\Users\Public\Pictures\Sample Pictures	SUCCESS	CreationTime: 7/13/2009 10:32:38 PM, LastAccessTime: 7/13/2009 10:32:38 PM
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Pictures\Sample Pictures	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Pictures\Sample Pictures	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Open Reparse Po
11:26:57...	cerber.exe	1944	QuerySecurityFi...	C:\Users\Public\Pictures\Sample Pictures	SUCCESS	Information: Owner
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Pictures\Sample Pictures	SUCCESS	
11:26:57...	cerber.exe	1944	QueryDirectory	C:\Users\Public\Pictures	NO MORE FILES	
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Pictures	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Recorded TV	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\Users\Public\Recorded TV	SUCCESS	CreationTime: 7/14/2009 12:45:14 AM, LastAccessTime: 7/14/2009 12:48:11 AM
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Recorded TV	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Recorded TV	SUCCESS	Desired Access: Read Control, Disposition: Open, Options: Open Reparse Po
11:26:57...	cerber.exe	1944	QuerySecurityFi...	C:\Users\Public\Recorded TV	SUCCESS	Information: Owner
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Recorded TV	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Recorded TV	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:26:57...	cerber.exe	1944	QueryBasicInfor...	C:\Users\Public\Recorded TV	SUCCESS	CreationTime: 7/14/2009 12:45:14 AM, LastAccessTime: 7/14/2009 12:48:11 AM
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Recorded TV	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Recorded TV	SUCCESS	Desired Access: Write Attributes, Synchronize, Disposition: Open, Options: Syı
11:26:57...	cerber.exe	1944	SetBasicInform...	C:\Users\Public\Recorded TV	SUCCESS	CreationTime: 0, LastAccessTime: 0, LastWriteTime: 0, ChangeTime: 0, FileAtt
11:26:57...	cerber.exe	1944	CloseFile	C:\Users\Public\Recorded TV	SUCCESS	
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Recorded TV	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Op
11:26:57...	cerber.exe	1944	QueryDirectory	C:\Users\Public\Recorded TV*	SUCCESS	Filter: *, 1: .
11:26:57...	cerber.exe	1944	QueryDirectory	C:\Users\Public\Recorded TV	SUCCESS	0: .., 1: desktop.ini, 2: Sample Media
11:26:57...	cerber.exe	1944	CreateFile	C:\Users\Public\Recorded TV\Sample Media	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse P
11:27:15...	cerber.exe	1944	CreateFile	C:\Users\Public\Documents	SUCCESS	Desired Access: Write Data/Add File, Synchronize, Disposition: Open, Option
11:27:15...	cerber.exe	1944	SetRenameInfo...	C:\Users\Public\Documents\ProcessMonitor(1).zip	SUCCESS	ReplaceIfExists: False, FileName: C:\Users\Public\Documents\uvXILIKvXa.88
11:27:15...	cerber.exe	1944	CloseFile	C:\Users\Public\Documents	SUCCESS	
11:27:15...	cerber.exe	1944	CloseFile	C:\Users\Public\Documents\uvXILIKvXa.8856	SUCCESS	
11:27:15...	cerber.exe	1944	CreateFile	C:\Users\Public\Documents_R_E_A_D___T_H_I_S___5FLKEUR6_.hta	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Create, Options:
11:27:15...	cerber.exe	1944	WriteFile	C:\Users\Public\Documents_R_E_A_D___T_H_I_S___5FLKEUR6_.hta	SUCCESS	Offset: 0, Length: 77,342, Priority: Normal
11:27:15...	cerber.exe	1944	CloseFile	C:\Users\Public\Documents_R_E_A_D___T_H_I_S___5FLKEUR6_.hta	SUCCESS	
11:27:15...	cerber.exe	1944	CreateFile	C:\Users\Public\Documents_R_E_A_D___T_H_I_S___SG5J_.txt	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Create, Options:
11:27:15...	cerber.exe	1944	WriteFile	C:\Users\Public\Documents_R_E_A_D___T_H_I_S___SG5J_.txt	SUCCESS	Offset: 0, Length: 1,360, Priority: Normal
11:27:15...	cerber.exe	1944	WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 526,140, Length: 227,955
11:27:15...	cerber.exe	1944	CloseFile	C:\Users\Public\Documents_R_E_A_D___T_H_I_S___SG5J_.txt	SUCCESS	
11:27:15...	cerber.exe	1944	WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 1,792, Length: 60
11:27:15...	cerber.exe	1944	QueryStandardI...	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	AllocationSize: 757,760, EndOfFile: 754,095, NumberOfLinks: 1, DeletePending
11:27:15...	cerber.exe	1944	WriteFile	C:\Users\Public\Documents\Explorer Suite Signatures\IMAGE_FILE_MACHINE_I386.xml	SUCCESS	Offset: 754,095, Length: 86, Priority: Normal
11:27:15...	cerber.exe	1944	CloseFile	C:\Users\Sysuser\Documents\depends22_x86\4re8LCts8s.8856	SUCCESS	
11:27:15...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\Documents\depends22_x86_R_E_A_D___T_H_I_S___AIGHOB_.hta	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Create, Options:
11:27:15...	cerber.exe	1944	WriteFile	C:\Users\Sysuser\Documents\depends22_x86_R_E_A_D___T_H_I_S___AIGHOB_.hta	SUCCESS	Offset: 0, Length: 77,342, Priority: Normal
11:27:15...	cerber.exe	1944	WriteFile	C:\Users\Sysuser\Documents\depends22_x86.zip	SUCCESS	Offset: 1,852, Length: 262,144, Priority: Normal
11:27:15...	cerber.exe	1944	CloseFile	C:\Users\Sysuser\Documents\depends22_x86_R_E_A_D___T_H_I_S___AIGHOB_.hta	SUCCESS	
11:27:15...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\Documents\depends22_x86_R_E_A_D___T_H_I_S___CVLREUDA_.txt	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Create, Options:
11:27:15...	cerber.exe	1944	WriteFile	C:\Users\Sysuser\Documents\depends22_x86_R_E_A_D___T_H_I_S___CVLREUDA_.txt	SUCCESS	Offset: 0, Length: 1,360, Priority: Normal
11:27:15...	cerber.exe	1944	ReadFile	C:	SUCCESS	Offset: 42,405,888, Length: 128, I/O Flags: Non-cached, Paging I/O, Synchronou
11:27:15...	cerber.exe	1944	CloseFile	C:\Users\Sysuser\Documents\depends22_x86_R_E_A_D___T_H_I_S___CVLREUDA_.txt	SUCCESS	
11:27:15...	cerber.exe	1944	ReadFile	C:\Users\Sysuser\Documents\depends22_x86.zip	SUCCESS	Offset: 263,996, Length: 262,144, Priority: Normal
11:27:15...	cerber.exe	1944	WriteFile	C:\Users\Sysuser\Documents\depends22_x86.zip	SUCCESS	Offset: 263,996, Length: 262,144, Priority: Normal
11:27:15...	cerber.exe	1944	ReadFile	C:\Users\Sysuser\Documents\depends22_x86.zip	SUCCESS	Offset: 526,140, Length: 84,629, Priority: Normal
11:27:15...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\Documents\Lab17-02.dll	SUCCESS	Desired Access: Write Attributes, Synchronize, Disposition: Open, Options: Syı
11:27:53...	cerber.exe	1944	ReadFile	C:\Users\Sysuser\Desktop\snapshot_2024-03-27_00-26.zip	SUCCESS	Offset: 10,225,468, Length: 262,144
11:27:53...	cerber.exe	1944	WriteFile	C:\Users\Sysuser\Desktop\snapshot_2024-03-27_00-26.zip	SUCCESS	Offset: 10,225,468, Length: 262,144
11:27:53...	cerber.exe	1944	Thread Exit		SUCCESS	Thread ID: 7888, User Time: 0.2187500, Kernel Time: 2.0937500
11:27:53...	cerber.exe	1944	ReadFile	C:\Users\Sysuser\Desktop\snapshot_2024-03-27_00-26.zip	SUCCESS	Offset: 10,487,612, Length: 262,144
11:27:53...	cerber.exe	1944	WriteFile	C:\Users\Sysuser\Desktop\snapshot_2024-03-27_00-26.zip	SUCCESS	Offset: 10,487,612, Length: 262,144
11:27:53	cerber.exe	1944	ReadFile	C:\Users\Sysuser\Desktop\snapshot_2024-03-27_00-26.zip	SUCCESS	Offset: 10,749,756, Length: 262,144

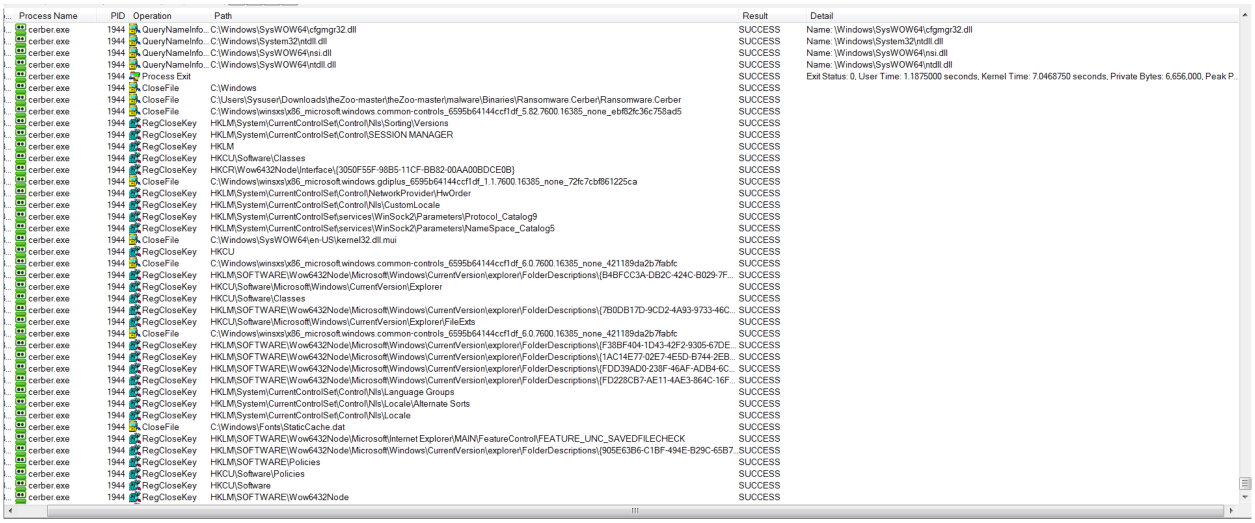
11:27:54...	cerber.exe	1944	ReadFile	C:\Windows\Fonts\StaticCache.dat	SUCCESS	Offset: 1,359,872, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchron
11:27:54...	cerber.exe	1944	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:27:54...	cerber.exe	1944	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback	SUCCESS	Desired Access: Query Value
11:27:54...	cerber.exe	1944	RegSetInfoKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane1	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane2	SUCCESS	Type: REG_SZ, Length: 24, Data: SimSun-ExtB
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane2	SUCCESS	Type: REG_SZ, Length: 24, Data: SimSun-ExtB
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane3	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane4	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane5	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane6	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane7	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane8	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane9	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane10	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane11	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane12	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane13	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane14	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane15	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Plane16	NAME NOT FOUND	Length: 144
11:27:54...	cerber.exe	1944	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	
11:27:54...	cerber.exe	1944	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
11:27:54...	cerber.exe	1944	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
11:27:54...	cerber.exe	1944	RegSetInfoKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
11:27:54...	cerber.exe	1944	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	Query: Cached, SubKeys: 4, Values: 1
11:27:54...	cerber.exe	1944	RegEnumKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	Index: 0, Name: MingLiU
11:27:54...	cerber.exe	1944	RegEnumKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	Index: 1, Name: MingLiU_HKSCS
11:27:54...	cerber.exe	1944	RegEnumKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	Index: 2, Name: PMingLiU
11:27:54...	cerber.exe	1944	RegEnumKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	Index: 3, Name: SimSun
11:27:54...	cerber.exe	1944	RegQueryKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	Query: HandleTags, HandleTags: 0x100
11:27:54...	cerber.exe	1944	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback\Consolas	NAME NOT FOUND	Desired Access: Query Value
11:27:54...	cerber.exe	1944	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\LanguagePack\SurrogateFallback	SUCCESS	
11:27:54...	cerber.exe	1944	ReadFile	C:\Windows\Fonts\consola.ttf	SUCCESS	Offset: 90,112, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronous
11:27:55...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\AppData\Local\Temp	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse
11:27:55...	cerber.exe	1944	QueryBasicInfor...	C:\Users\Sysuser\AppData\Local\Temp	SUCCESS	CreationTime: 5/2/2022 1:51:27 PM, LastAccessTime: 4/26/2024 11:23:41 AM, L
11:27:55...	cerber.exe	1944	CloseFile	C:\Users\Sysuser\AppData\Local\Temp	SUCCESS	
11:27:55...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\AppData\Local\Temp\tmpE33C.tmp	SUCCESS	Desired Access: Generic Read, Disposition: Create, Options: Synchronous IO
11:27:55...	cerber.exe	1944	CloseFile	C:\Users\Sysuser\AppData\Local\Temp\tmpE33C.tmp	SUCCESS	
11:27:55...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\AppData\Local\Temp\tmpE33C.tmp	SUCCESS	Desired Access: Write Attributes, Synchronize, Disposition: Open, Options: Sy
11:27:55...	cerber.exe	1944	SetBasicInform...	C:\Users\Sysuser\AppData\Local\Temp\tmpE33C.tmp	SUCCESS	CreationTime: 0, LastAccessTime: 0, LastWriteTime: 0, ChangeTime: 0, FileAtt

11:27:55...	cerber.exe	1944	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
11:27:55...	cerber.exe	1944	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\	SUCCESS	Desired Access: Read, Maximum Allowed
11:27:55...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\CurrentBuildNumber	SUCCESS	Type: REG_SZ, Length: 10, Data: 7600
11:27:55...	cerber.exe	1944	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\CSDVersion	NAME NOT FOUND	Length: 134
11:27:55...	cerber.exe	1944	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION	SUCCESS	
11:27:55...	cerber.exe	1944	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:27:55...	cerber.exe	1944	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:27:55...	cerber.exe	1944	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
11:27:55...	cerber.exe	1944	RegQueryValue	HKCU\Control Panel\Desktop\TileWallpaper	SUCCESS	Type: REG_SZ, Length: 4, Data: 0
11:27:55...	cerber.exe	1944	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
11:27:55...	cerber.exe	1944	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:27:55...	cerber.exe	1944	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:27:55...	cerber.exe	1944	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
11:27:55...	cerber.exe	1944	RegQueryValue	HKCU\Control Panel\Desktop\WallpaperStyle	SUCCESS	Type: REG_SZ, Length: 6, Data: 10
11:27:55...	cerber.exe	1944	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
11:27:55...	cerber.exe	1944	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:27:55...	cerber.exe	1944	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:27:55...	cerber.exe	1944	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
11:27:55...	cerber.exe	1944	RegQueryValue	HKCU\Control Panel\Desktop\WallpaperOriginX	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:27:55...	cerber.exe	1944	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
11:27:55...	cerber.exe	1944	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:27:55...	cerber.exe	1944	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
11:27:55...	cerber.exe	1944	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
11:27:55...	cerber.exe	1944	RegQueryValue	HKCU\Control Panel\Desktop\WallpaperOriginY	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11:27:55...	cerber.exe	1944	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
11:27:55...	cerber.exe	1944	CreateFile	C:\Users\Sysuser\AppData\Local\Temp\tmpE33C.bmp	SUCCESS	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse
11:27:55...	cerber.exe	1944	QueryBasicInfor...	C:\Users\Sysuser\AppData\Local\Temp\tmpE33C.bmp	SUCCESS	CreationTime: 4/26/2024 11:28:30 AM, LastAccessTime: 4/26/2024 11:28:30 AM
11:27:55...	cerber.exe	1944	CloseFile	C:\Users\Sysuser\AppData\Local\Temp\tmpE33C.bmp	SUCCESS	

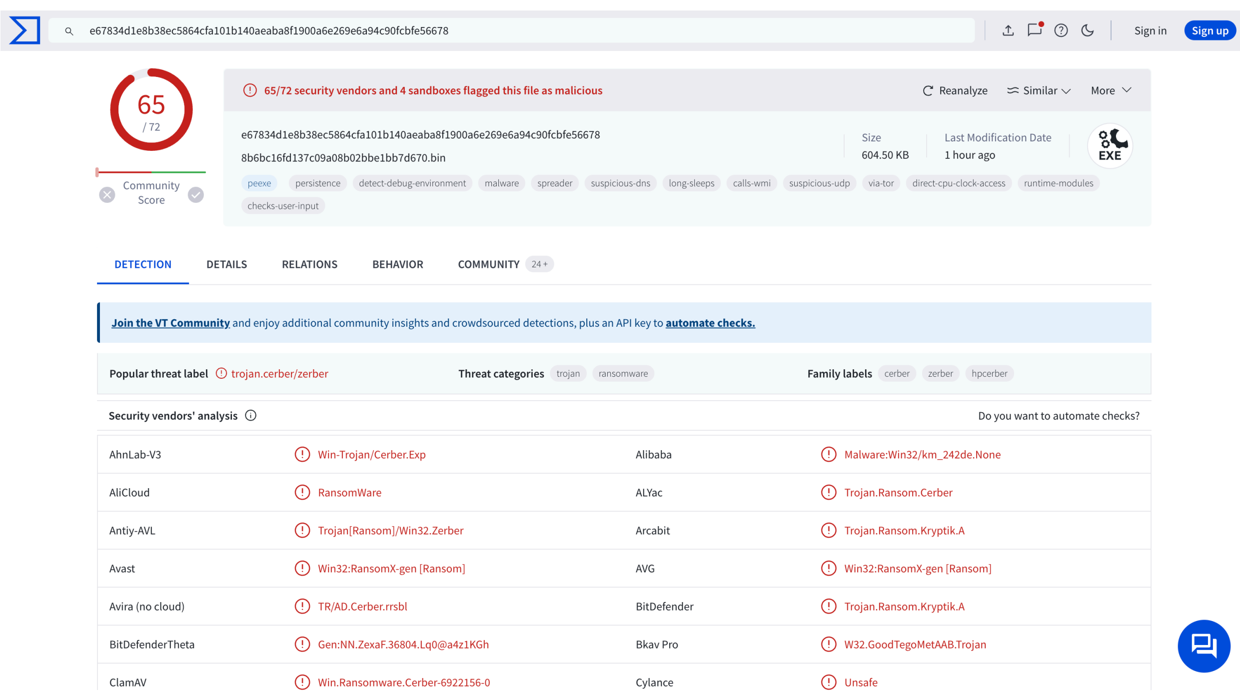
11:28:01...	cerber.exe	1944	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\App Paths\mshta.exe	NAME NOT FOUND	Desired Access: Read
11:28:01...	cerber.exe	1944	RegQueryKey	HKCR\htafile\Shell\Open	SUCCESS	Query: Name
11:28:01...	cerber.exe	1944	RegQueryKey	HKCR\htafile\Shell\Open	SUCCESS	Query: HandleTags, HandleTags: 0x401
11:28:01...	cerber.exe	1944	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\mshta.exe	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
11:28:01...	cerber.exe	1944	QuerySecurityFi...	C:\Windows\SysWOW64\mshta.exe	SUCCESS	Information: Label
11:28:01...	cerber.exe	1944	ReadFile	C:\Windows\SysWOW64\mshta.exe	SUCCESS	Offset: 5,120, Length: 30,208, I/O Flags: Non-cached, Paging I/O, Synchronous I
11:28:01...	cerber.exe	1944	QueryNameInfo...	C:\Windows\SysWOW64\mshta.exe	SUCCESS	Name: \Windows\SysWOW64\mshta.exe
11:28:01...	cerber.exe	1944	Process Create	C:\Windows\SysWOW64\mshta.exe	SUCCESS	PID: 8008, Command line: "C:\Windows\SysWOW64\mshta.exe" "C:\Users\Sy
11:28:01...	cerber.exe	1944	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\AppCertDlls	REPARSE	Desired Access: Query Value

...	cerber.exe	1944	Load Image	C:\Windows\SysWOW64\notepad.exe	SUCCESS	Image Base: 0x3c60000, Image Size: 0x10000
...	cerber.exe	1944	CloseFile	C:\Windows\SysWOW64\notepad.exe	SUCCESS	
...	cerber.exe	1944	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
...	cerber.exe	1944	RegOpenKey	HKCU\Software\Microsoft\Windows\CurrentVersion\App Paths\NOTEPAD.EXE	NAME NOT FO...	Desired Access: Read
...	cerber.exe	1944	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
...	cerber.exe	1944	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\App Paths\NOTEPAD.EXE	REPARSE	Desired Access: Read
...	cerber.exe	1944	RegOpenKey	HKLM\SOFTWARE\MICROSOFT\Windows\CurrentVersion\App Paths\NOTEPAD.EXE	NAME NOT FO...	Desired Access: Read
...	cerber.exe	1944	RegQueryKey	HKCR\txtfile\shell\open	SUCCESS	Query: Name
...	cerber.exe	1944	RegQueryKey	HKCR\txtfile\shell\open	SUCCESS	Query: HandleTags, HandleTags: 0x401
...	cerber.exe	1944	RegOpenKey	HKCU\Software\Classes\txtfile\shell\open\command	NAME NOT FO...	Desired Access: Query Value
...	cerber.exe	1944	RegQueryKey	HKCR\txtfile\shell\open	SUCCESS	Query: HandleTags, HandleTags: 0x401
...	cerber.exe	1944	RegOpenKey	HKCR\txtfile\shell\open\command	SUCCESS	Desired Access: Query Value





This is the analysis of cerber.exe on VirusTotal:



References

- https://nyameeeain.medium.com/queueuserapc-process-injection-6f31fcb89410
- https://learn.microsoft.com/en-us/windows/win32/api/processthreadsapi/nf-processthreadsapi-queueuserapc
- https://learn.microsoft.com/en-us/windows/win32/api/securitybaseapi/nf-securitybaseapi-impersonateloggedonuser
- https://www.allthingsdfir.com/tracing-malicious-downloads/
- https://learn.microsoft.com/en-us/windows/win32/api/winbase/nf-winbase-createfilemappinga
- https://myspybot.com/cerber-ransomware-evolution/
- https://www.virustotal.com/gui/file/e67834d1e8b38ec5864cfa101b140aeaba8f1900a6e269e6a94c90fcbfe56678
- https://www.youtube.com/watch?v=p_ZfeHuHTW8
- https://www.unixtimestamp.com/
- https://www.asciitable.com/
- https://www.microsoft.com/en-us/wdsi/threats/threat-search?query=Win32/Cerber&page=4
- https://learn.microsoft.com/en-us/windows-hardware/drivers/ifs/irp-mj-file-system-control
- https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/security-privacy/ie-security-zones-registry-entries
- https://serverfault.com/questions/93785/looking-for-a-unique-guid-to-identify-a-windows-installation
- https://learn.microsoft.com/en-us/windows/win32/api/memoryapi/nf-memoryapi-virtualalloc
- https://github.com/ytisf/theZoo/tree/master
- https://www.f-secure.com/v-descs/trojan-downloader-w32-cerber.shtml
- https://myspybot.com/cerber-ransomware-evolution/