

Malware Analysis Final Report

Contents

Check on virus total	2
Check in tool	3
PeiD	3
Bintext	4
PEview	4
Dependency Walker	5
Check on ida	5

Check on virus total

47 security vendors flagged this file as malicious

7481fb2327af90bef5a37eb8b1f7d11052f41e612a4e48f1885079fc3e370e8d
.JPG5K32.DLL

31.00 KB Size 2020-09-29 14:56:50 UTC 1 year ago

Community Score

DETECTION	DETAILS	COMMUNITY
Ad-Aware	Backdoor.Mask.E	AegisLab
AhnLab-V3	Trojan.Win32.Careto.R97401	Alibaba
ALYac	Backdoor.Mask.E	Antiy-AVL
Arcabit	Backdoor.Mask.E	Avast
AVG	Win32.Careto-D [Trj]	BitDefender
Bkav Pro	W32.Madheard.TL.Trojan	Comodo
Cylance	Unsafe	Cyren
DrWeb	BackDoor.Mask.29	Emisoft
eScan	Backdoor.Mask.E	ESET-NOD32
FireEye	Backdoor.Mask.E	Fortinet
GData	Backdoor.Mask.E	Ikarus
Jiangmin	Trojan.Careto.c	K7AntiVirus
K7GW	Trojan (004dcb541)	Kaspersky

- The virus can be detected in 47
- Its basic information

MD5	53908fb164e2e2053ceba4bdb6d09db9
SHA-1	3219ba119ac4a0b74b174debfb645203e87f602
SHA-256	7481fb2327af90bef5a37eb8b1f7d11052f41e612a4e48f1885079fc3e370e8d
Vhash	1340466d15155078z3409lz45z46z1
Authentihash	cefe1dee528b78a316e0f0796afc4325e3d115771842f7cddc90461314357909
Imphash	52660550aa2ac90863c1c1cfb4fd3ab2f8
Rich PE header hash	0a2e9ab8745a908b3afef87526fd1c2c
SSDEEP	768:euqA0/5CDYnY/1rhbAxZXUYJlxqyd3azWQcPjcl:ebA0s/hhkfDxj+crcl
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
TrID	Win16 NE executable (generic) (45%)
TrID	Win32 Dynamic Link Library (generic) (21.1%)
TrID	Win32 Executable (generic) (14.4%)
TrID	OS/2 Executable (generic) (6.5%)
TrID	Generic Win/DOS Executable (6.4%)
File size	31.00 KB (31744 bytes)
PEID packer	Microsoft Visual C++ v7.0 DLL

- + Hashes type : MD5, SHA-1, SHA-256, Vhash, Authentihash, SSDEEP
- + File type : Win32 DLL
- + File size : 31.00 KB (31744 bytes)
- + Creation time: 2013-04-09 14:15:17
- + Target machine : PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
- + Imports :

ADVAPI32.dll

KERNEL32.dll

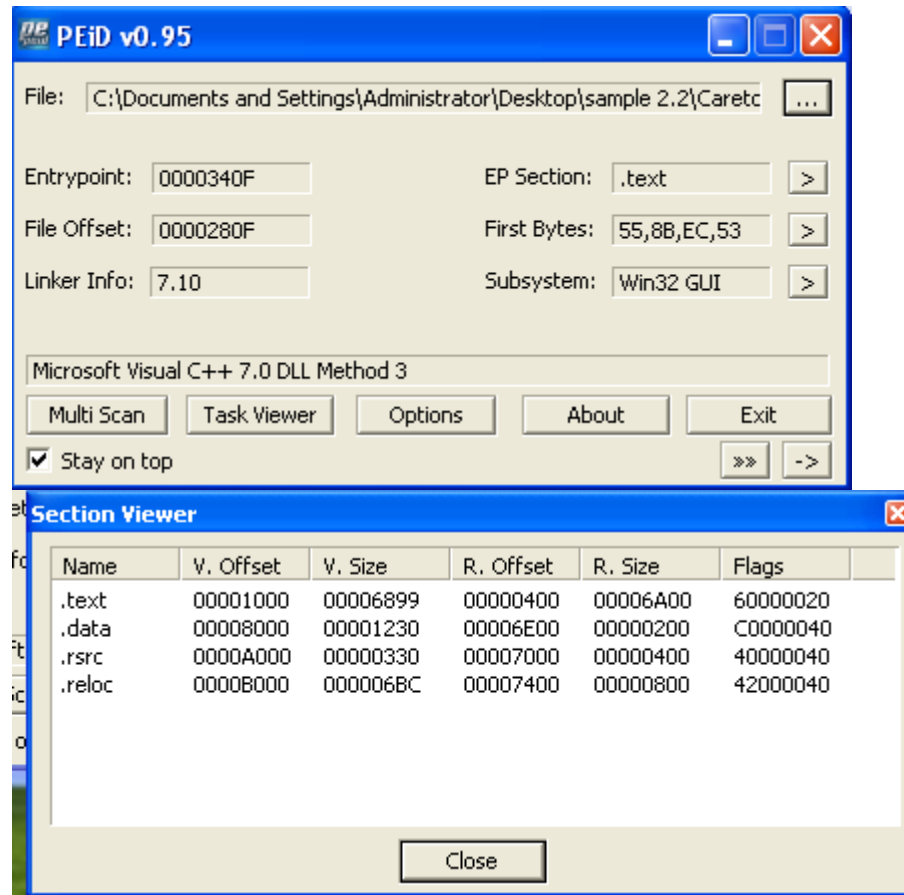
msvcrt.dll

WS2_32.dll

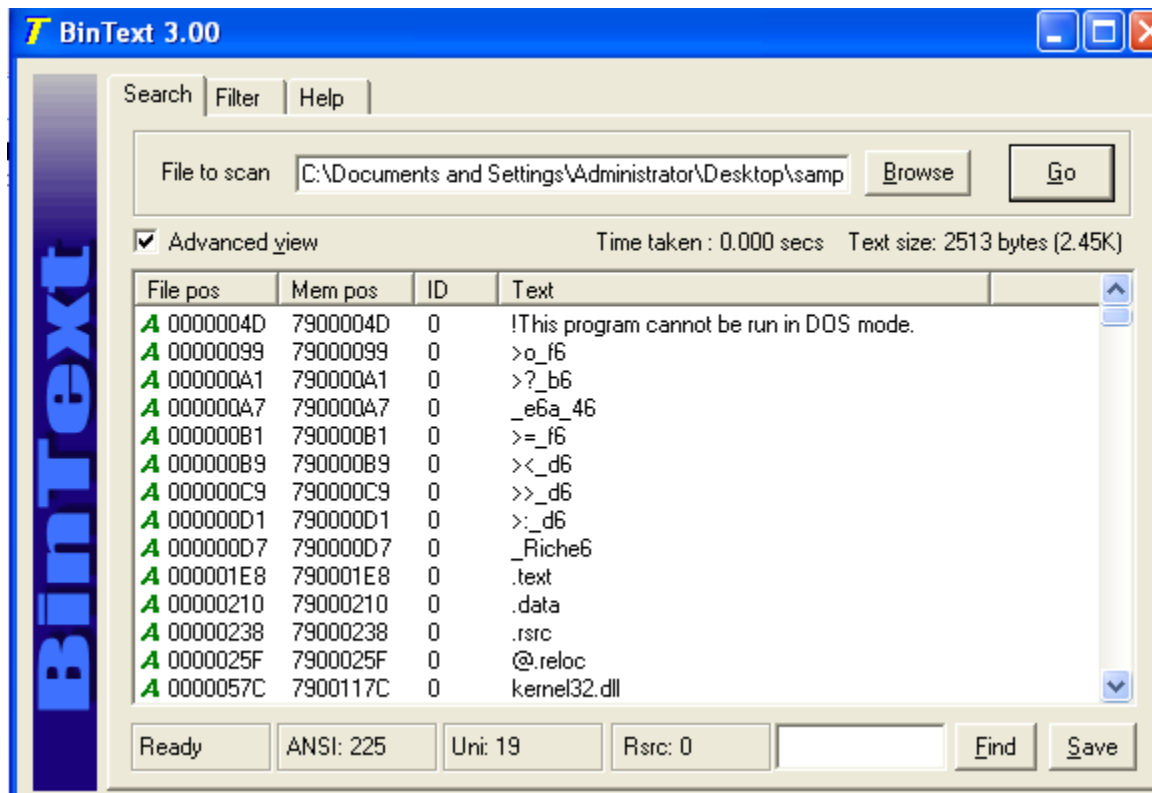
USER32.dll

Check in tool

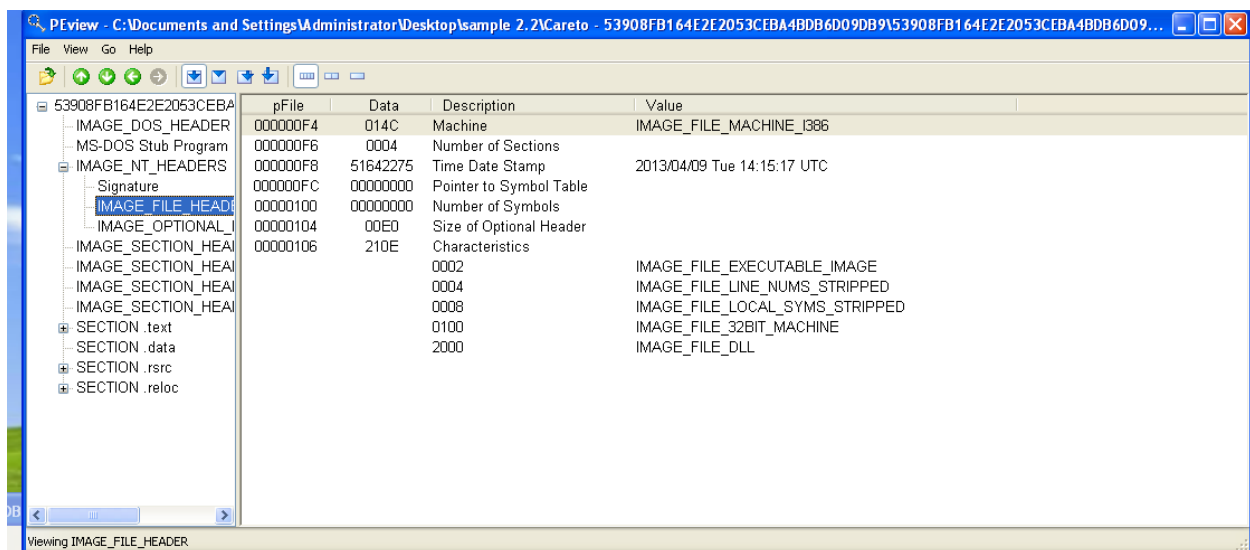
PeiD



Bintext



PEview

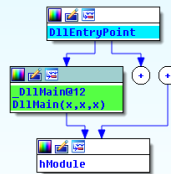


The screenshot shows the Dependency Walker application window. The title bar reads "Dependency Walker - [53908FB164E2E2053CEBA4B0B6D090B9.malware]". The menu bar includes File, Edit, View, Options, Profile, Window, and Help. The toolbar contains various icons for file operations and viewing options. The main window is divided into two panes. The left pane, titled "Loaded Modules", lists the following modules: 53908FB164E2E2053CEBA4B0B6D090B9.MALWARE, MSVCRT.DLL, KERNEL32.DLL, USER32.DLL, ADVAPI32.DLL, and WS2_32.DLL. The right pane, titled "Export/Import", shows the export table for the main module. It has columns for Ordinal, Hint, Function, and Entry Point. The first entry is: 1 (0x0001) 0 (0x0000) InitProcess 0x00002656. Below this, there is a section for the import table, which is currently empty. At the bottom of the window, there is a status bar that reads "For Help, press F1".

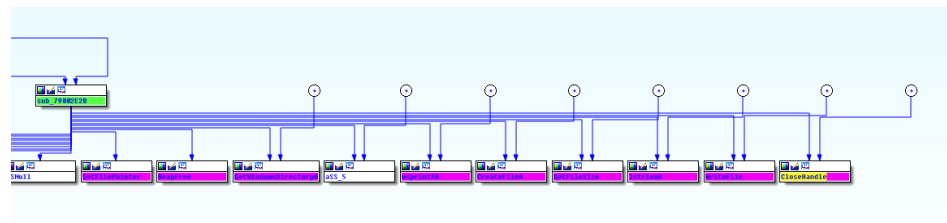
Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver
IESHIMS.DLL														
WER.DLL														
MPR.DLL														
53908FB164E2E2053CEBA4B0B6D090B9.MALWARE	04/14/2008 4:00a	04/13/2008 5:10p	59,904	A	0x00013C87	0x00013C87	x86	Console	CV	0x71B20000	Unknown	0x00012000	Not Loaded	5.1.2600.5512
ADVAPI32.DLL	12/01/2015 11:45a	04/09/2013 7:15a	31,744	A	0x00008C1D	0x00008BEE3	x86	GUI	PDB	0x79000000	Unknown	0x0000C000	Not Loaded	4.0.0.10195
ADVAPI32.DLL	04/22/2013 1:37a	04/22/2013 2:37a	618,496	A	0x000048F8	0x000048F8	x86	Console	CV	0x77D00000	Unknown	0x00009B00	Not Loaded	5.1.2600.4382
GD32.DLL	10/09/2013 5:12a	10/09/2013 6:12a	287,744	A	0x00052131	0x00052131	x86	Console	CV	0x77F10000	Unknown	0x00049000	Not Loaded	5.1.2600.6460

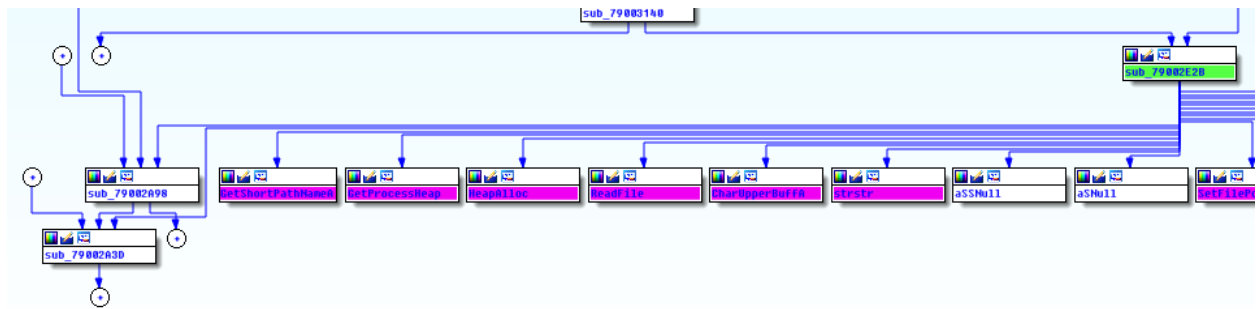
Warning: At least one delay-load dependency module was not found.
Warning: At least one module has an unresolved import due to a missing export function in a delay-load dependent module.

Check on ida



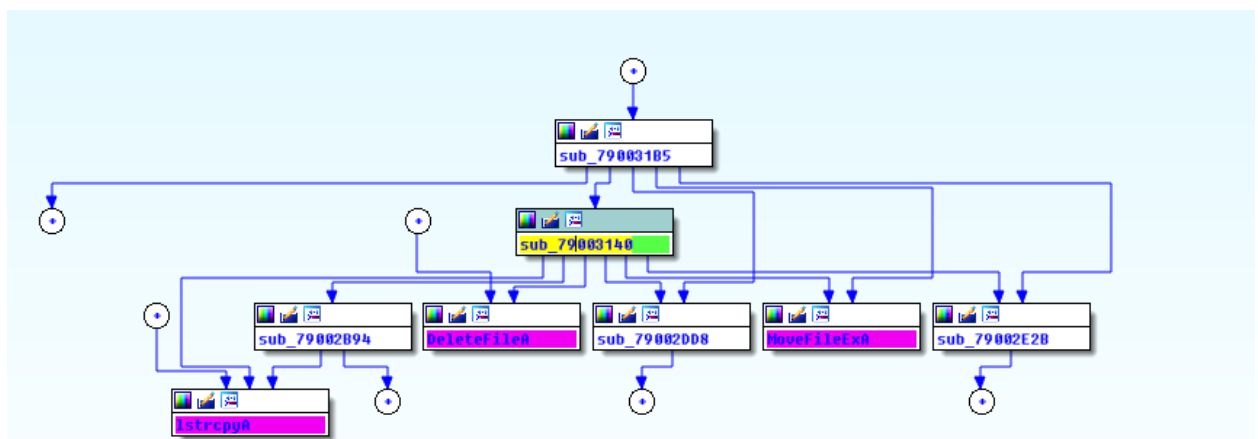
Check sub_79002E2B





Important function

Check sub_79003104



Imports

Address	Ordinal	Name	Library
00000000...		RegDeleteKeyA	ADVAPI32
00000000...		RegOpenKeyExA	ADVAPI32
00000000...		RegEnumKeyExA	ADVAPI32
00000000...		RegCloseKey	ADVAPI32
00000000...		RegEnumValueA	ADVAPI32
00000000...		RegQueryInfoKeyA	ADVAPI32
00000000...		RegQueryValueExA	ADVAPI32
00000000...		GetDiskFreeSpaceA	KERNEL32
00000000...		IstrcmpiA	KERNEL32
00000000...		QueryDosDeviceA	KERNEL32
00000000...		GlobalAlloc	KERNEL32
00000000...		GlobalFree	KERNEL32
00000000...		IstrlenA	KERNEL32
00000000...		LoadLibraryA	KERNEL32
00000000...		FreeLibrary	KERNEL32
00000000...		GetProcAddress	KERNEL32
00000000...		IstrcpyA	KERNEL32
00000000...		ExpandEnvironmentStringsA	KERNEL32
00000000...		IstrcatA	KERNEL32
00000000...		GetVersionExA	KERNEL32
00000000...		CloseHandle	KERNEL32
00000000...		GetVolumeInformationA	KERNEL32
00000000...		WriteFile	KERNEL32
00000000...		SetFilePointer	KERNEL32
00000000...		ReadFile	KERNEL32
00000000...		HeapAlloc	KERNEL32
00000000...		GetProcessHeap	KERNEL32
00000000...		GetFileSize	KERNEL32
00000000...		CreateFileA	KERNEL32

Line 1 of 76

Export

Name	Address	Ordinal
fnProcess	0000000079002656	1
DllEntryPoint	000000007900340F	