

Malware Analysis Final Report

Contents

I. Check in VirusTotal	2
II. Check in tools	4
Check in PEid	4
Check in PView	5
Dependency Walker	5
BinText	5
Resource Hacker	6
Malware on IDA	7

I. Check in VirusTotal

47
/ 70

Community Score

47 security vendors flagged this file as malicious

7481fb2327af90bef5a37eb8b1f7d11052f41e612a4e48f1885079fc3e370e8d
JPEG1X32.DLL
pedll

31.00 KB
Size

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

DLL

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

- The virus can be detected in 47 anti-virus platforms.

- Basic properties:

Basic Properties

MD5	53908fb164e2e2053ceba4bdb6d09db9
SHA-1	3219ba119ac4a0b74b174debfbb645203e87f602
SHA-256	7481fb2327af90bef5a37eb8b1f7d11052f41e612a4e48f1885079fc3e370e8d
Vhash	1340466d15155078z3409lz45z46z1
Authentihash	cefe1dee528b78a316e0f0796afc4325e3d115771842f7cddc90461314357909
Imphash	52660550aa2ac90863c1cfb4fd3ab2f8
Rich PE header hash	0a2e9ab8745a908b3afef87526fd1c2c
SSDEEP	768:euqAO/5CDYnY/1rhbAxZXUYJlxqyd3azWQcPjcl:ebAOs/hhkfDxj+crcI
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 types: MD5, SHA-1, SHA-256, Vhash, Authentihash, SSDEEP.

+ File type: Win32 DLL

+ Packer used: PEiD and F-PROT

+ File size: 31 KB

+ Creation time: 2013-04-09 14:15:17

Its aim and behaviors:

+ Target machine: Intel 386 or later processors and compatible processors +

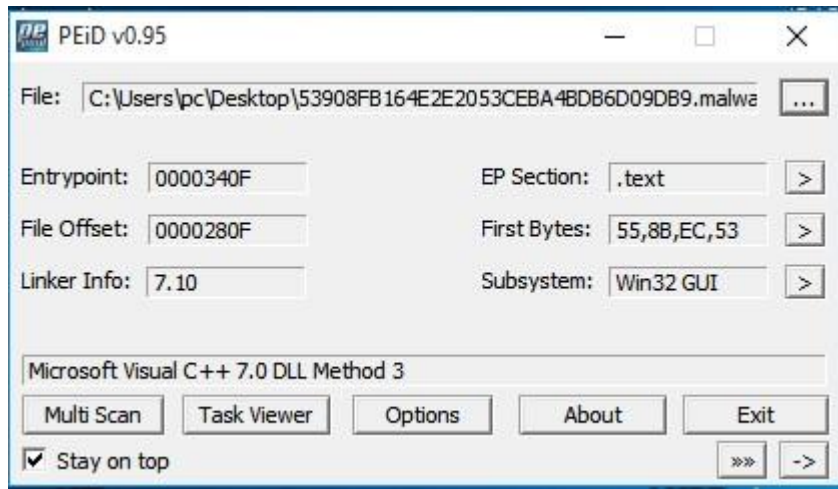
Imports:

Imports

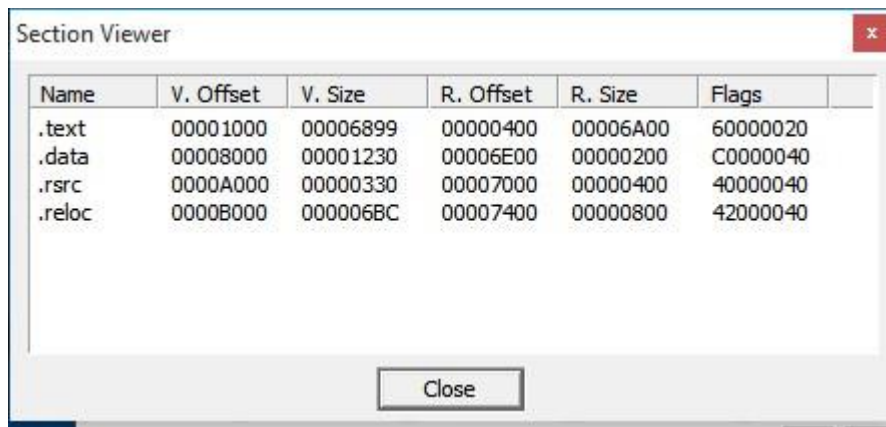
- + ADVAPI32.dll
- + KERNEL32.dll
- + msvcrt.dll
- + WS2_32.dll
- + USER32.dll

II. Check in tools

Check in PEid



Section Viewer:



Check in PReview

PEview - C:\Users\pc\Desktop\53908FB164E2E2053CEBA48DB6D09DB9.malware

FileViewGoHelp

53908FB164E2E2053CEBA48DB6D09DB9

IMAGE_DOS_HEADER

MS-DOS Stub Program

IMAGE_NT_HEADERS

IMAGE_SECTION_HEADER .text

IMAGE_SECTION_HEADER .data

IMAGE_SECTION_HEADER .rsrc

IMAGE_SECTION_HEADER .reloc

SECTION .text

SECTION .data

SECTION .rsrc

SECTION .reloc

pFile

Raw Data

Value

00000000

4D 5A 90 00 03 00 00 00

04 00 00 00 FF FF 00 00

MZ.....@.....

00000010

B8 00 00 00 00 00 00 00

40 00 00 00 00 00 00 00

.....@.....

00000020

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

.....@.....

00000030

00 00 00 00 00 00 00 00

00 00 00 00 F0 00 00 00

.....@.....

00000040

0E 1F BA 0E 00 B4 09 CD

21 B8 01 4C CD 21 54 68

.....!...L!Th

00000050

69 73 20 70 72 6F 67 72

61 6D 20 63 61 6E 6E 6F

is program canno

00000060

74 20 62 65 20 72 75 6E

20 69 6E 20 44 4F 53 20

t be run in DOS

00000070

6D 6F 64 65 2E 0D 0D 0A

24 00 00 00 00 00 00 00

mode...\$.e6`_e6`_

00000080

21 57 0E 0C 65 36 60 5F

65 36 60 5F 65 36 60 5F

!W...e6`_e6`_>o_f6`_

00000090

9F 15 79 5F 6D 36 60 5F

E6 3E 6F 5F 66 36 60 5F

..y_m6`_>o_f6`_>?_b6`_e6a_46`_

000000A0

EB 3E 3F 5F 62 36 60 5F

65 36 61 5F 34 36 60 5F

..>_f6`_><_d6`_>_q6`_>>_d6`_

000000B0

E6 3E 3D 5F 66 36 60 5F

E6 3E 3C 5F 64 36 60 5F

..>_d6`_Riche6`_>_d6`_Riche6`_

000000C0

EB 3E 00 5F 71 36 60 5F

E6 3E 3E 5F 64 36 60 5F

..>_d6`_Riche6`_>_d6`_Riche6`_

000000D0

E6 3E 3A 5F 64 36 60 5F

52 69 63 68 65 36 60 5F

..>_d6`_Riche6`_>_d6`_Riche6`_

000000E0

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

.....

000000F0

50 45 00 00 4C 01 04 00

75 22 64 51 00 00 00 00

PE...L...u"dQ...!

00000100

00 00 00 00 E0 00 0E 21

0B 01 07 0A 00 6A 00 00

.....!...j...4.....

00000110

00 20 00 00 00 00 00 00

0F 34 00 00 00 10 00 00

.....y.....

00000120

00 80 00 00 00 00 00 79

00 10 00 00 00 02 00 00

.....y.....

00000130

05 00 01 00 05 00 01 00

04 00 00 00 00 00 00 00

.....y.....

00000140

00 C0 00 00 00 04 00 00

1D BC 00 00 02 00 00 04

.....y.....

00000150

00 00 04 00 00 10 00 00

00 00 10 00 00 10 00 00

.....y.....

00000160

00 00 00 00 10 00 00 00

50 78 00 00 49 00 00 00

.....Px...I.....

00000170

9C 71 00 00 78 00 00 00

00 A0 00 00 30 03 00 00

...q...x.....0.....

00000180

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

.....q...x.....0.....

00000190

00 F0 00 00 C8 05 00 00

60 11 00 00 1C 00 00 00

.....q...x.....0.....

Viewing 53908FB164E2E2053CEBA48DB6D09DB9.malware

Dependency Walker

Dependency Walker - [53908FB164E2E2053CEBA48DB6D09DB9.malware]

FileEditViewOptionsProfileWindowHelp

53908FB164E2E2053CEBA48DB6D09DB9.MALWARE

MSVCRT.DLL

KERNEL32.DLL

USER32.DLL

ADVAPI32.DLL

WS2_32.DLL

PI

Ordinal ^

Hint

Function

Entry Point

1

N/A

187 (0x00BB)

_adjust_fdiv

Not Bound

2

N/A

320 (0x0140)

_initterm

Not Bound

3

N/A

491 (0x01EB)

_snprintf

Not Bound

4

N/A

636 (0x027C)

_wtoi

Not Bound

5

N/A

687 (0x02AF)

free

Not Bound

6

N/A

728 (0x02E8)

malloc

Not Bound

E

Ordinal ^

Hint

Function

Entry Point

1

(0x0001)

1 (0x0001)

??0_non_rtti_object@@QAE@ABV0@@Z

0x00038A80

2

(0x0002)

2 (0x0002)

??0_non_rtti_object@@QAE@PBD@Z

0x00038AB0

3

(0x0003)

3 (0x0003)

??0bad_cast@@AAE@PBQBD@Z

0x00038AE0

4

(0x0004)

4 (0x0004)

??0bad_cast@@QAE@ABQBD@Z

0x00038AE0

5

(0x0005)

5 (0x0005)

??0bad_cast@@QAE@ABV0@@Z

0x00038B10

Module

File Time Stamp

Link Time Stamp

File Size

Attr.

Link Checksum

Real Checksum

CPU

Subsystem

API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL

Error opening file. The system cannot find the file specified (2).

API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL

Error opening file. The system cannot find the file specified (2).

API-MS-WIN-CORE-APPINIT-L1-1-0.DLL

Error opening file. The system cannot find the file specified (2).

API-MS-WIN-CORE-ATOMS-L1-1-0.DLL

Error opening file. The system cannot find the file specified (2).

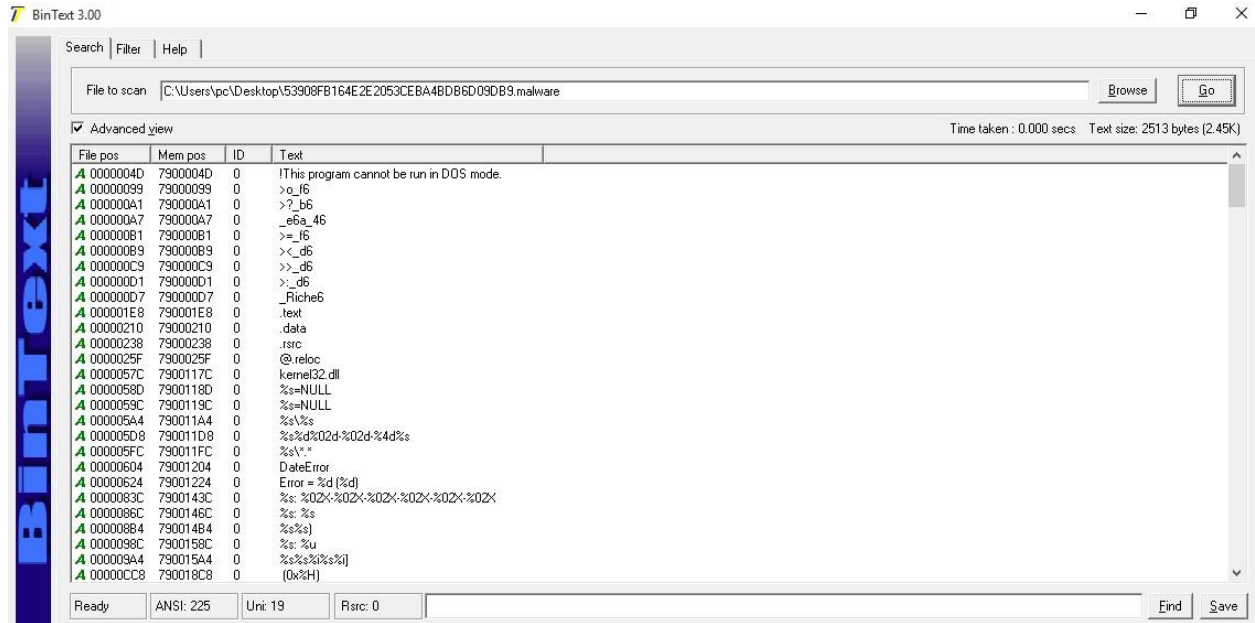
API-MS-WIN-CORE-COMM-L1-1-0.DLL

Error opening file. The system cannot find the file specified (2).

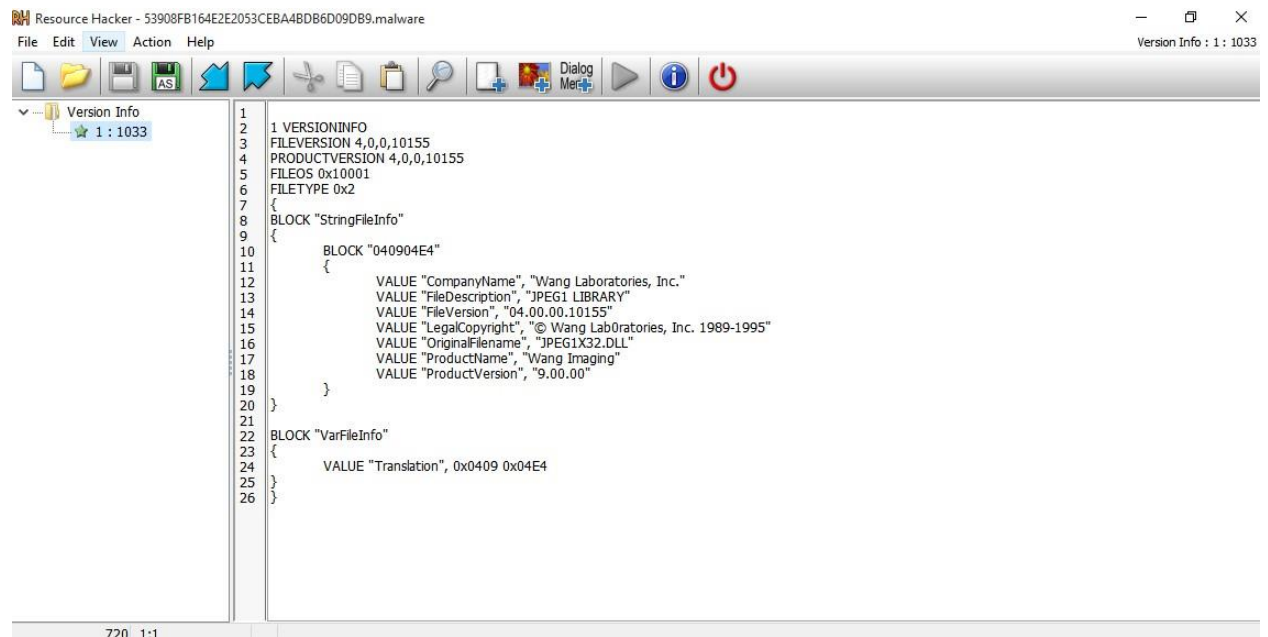
Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.

For Help, press F1

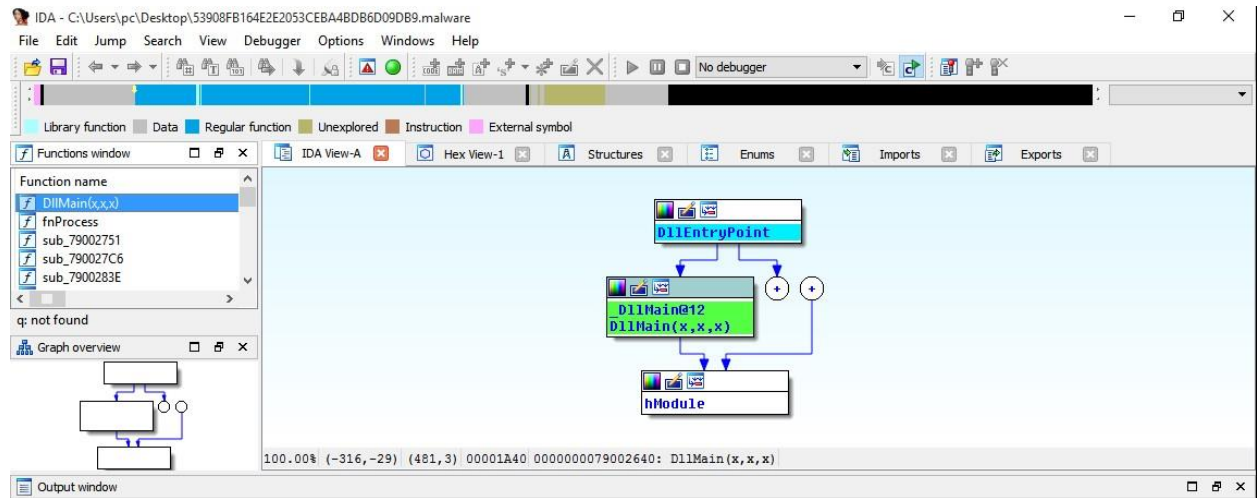
BinText



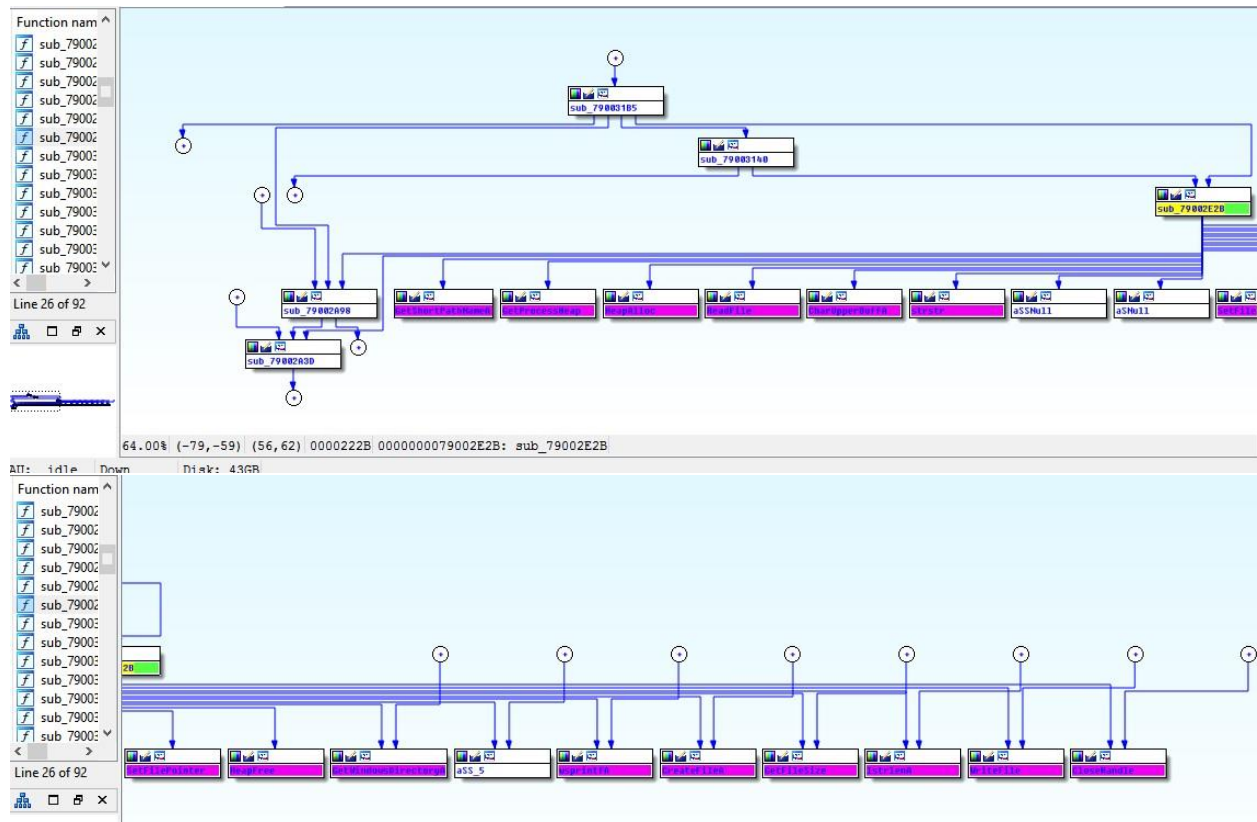
Resource Hacker



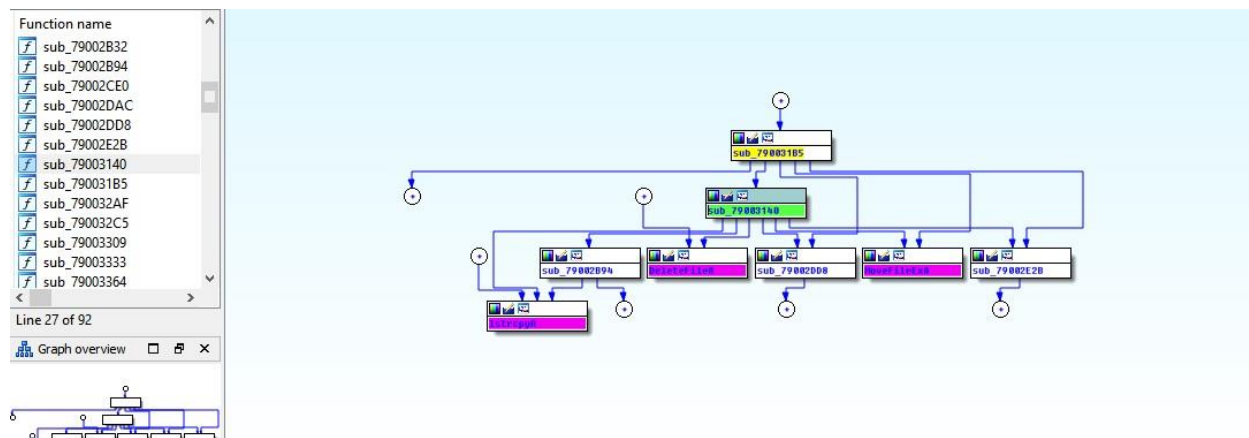
Malware on IDA



DllMain(x,x,x)



Check sub_79002E2B



Check sub_79003140

IDA - C:\Users\pc\Desktop\53908FB164E2053CEBA48DB6D09DB9.malware

File Edit Jump Search View Debugger Options Windows Help

No debugger

Library function Data Regular function Unexplored Instruction External symbol

Functions window

Function name	Address	Ordinal	Name	Library
sub_79003364	00000007...		RegDeleteKeyA	ADVAPI32
DllEntryPoint	00000007...		RegOpenKeyExA	ADVAPI32
_alloca_probe	00000007...		RegEnumKeyExA	ADVAPI32
_initterm	00000007...		RegCloseKey	ADVAPI32
sub_790034F4	00000007...		RegEnumValueA	ADVAPI32
malloc	00000007...		RegQueryInfoKeyA	ADVAPI32
sub_79003532	00000007...		RegQueryValueExA	ADVAPI32
Concurrency::details::UMSFreeVirt	00000007...		GetDiskFreeSpaceA	KERNEL32
sub_79003551	00000007...		IstrcmpA	KERNEL32
sub_79003555	00000007...		QueryDosDeviceA	KERNEL32
sub_79003558	00000007...		GlobalAlloc	KERNEL32
sub_79003610	00000007...		GlobalFree	KERNEL32
sub_79003666	00000007...		IstrlenA	KERNEL32
sub_79003679	00000007...		LoadLibraryA	KERNEL32
sub_7900369C	00000007...		FreeLibrary	KERNEL32
sub_79003725	00000007...		GetProcAddress	KERNEL32
sub_79003768	00000007...		IstrcpyA	KERNEL32
sub_7900390C	00000007...		ExpandEnvironmentStringsA	KERNEL32
sub_79003990	00000007...		IstrcatA	KERNEL32
sub_79003AE3	00000007...		GetVersionExA	KERNEL32
sub_79003B07	00000007...		CloseHandle	KERNEL32
sub_79003B07	00000007...		GetVolumeInformationA	KERNEL32

Q: not found QQ: not found

AU: idle Down Disk: 43GB

Imports

Functions window

Name	Address	Ordinal
fnProcess	0000000079002656	1
DllEntryPoint	000000007900340F	

Exports