Trịnh Quốc Hiếu – BI10-060 – USTH CS

Malware Analysis Final Report

Contents

Check in VirusTotal..2

Information gathered :..2

Check in tools...4

Check in PEid..4

Check on BinText..5

Check PEview 5

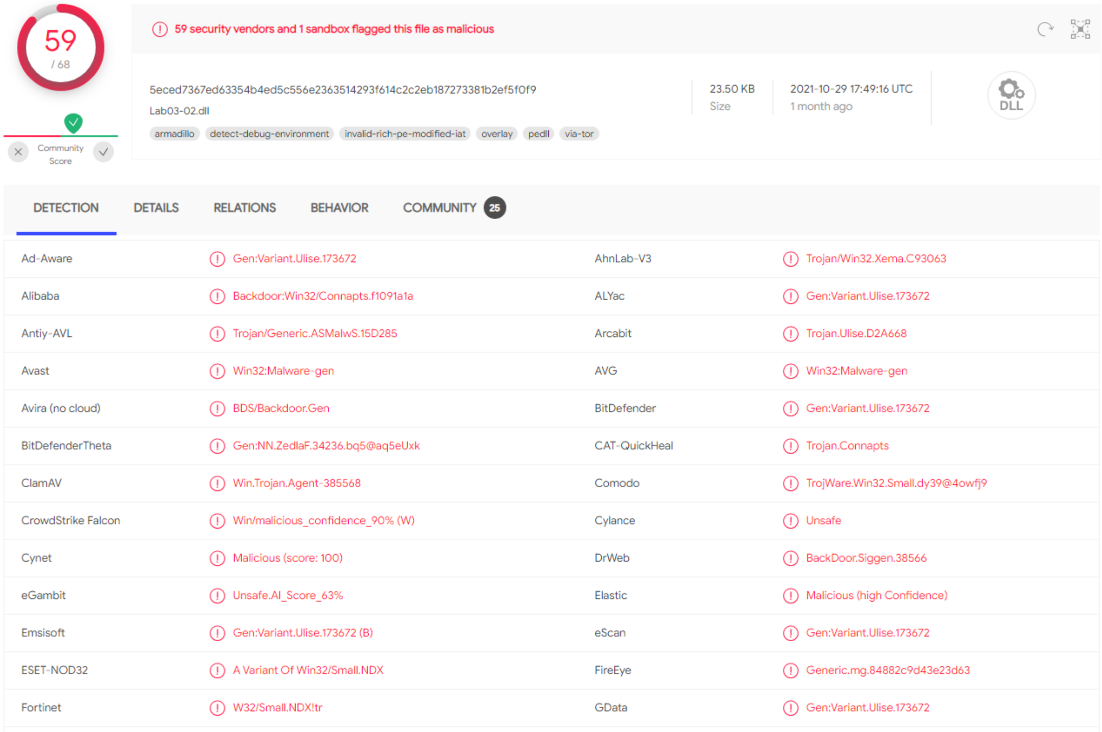
Check Reesource..6

Check malware on IDAq...7

Summary 9

Check in VirusTotal

Information gathered :



59 security vendors and 1 sandbox flagged this file as malicious

5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9

Lab03-02.dll

armadillo detect-debug-environment invalid-rich-pe-modified-iat overlay pedll via-tor

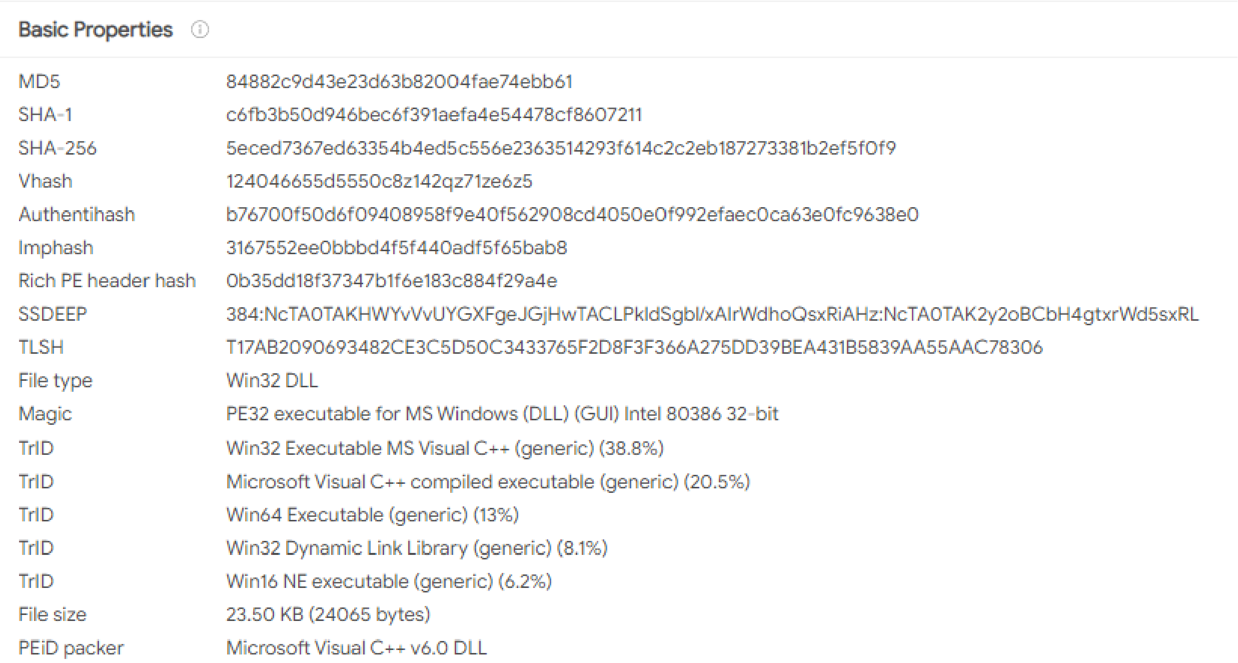
23.50 KB
Size

2021-10-29 17:49:16 UTC
1 month ago

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 25

Ad-Aware	Gen:Variant.Ulise.173672	AhnLab-V3	Trojan/Win32.Xema.C93063
Alibaba	Backdoor:Win32/Connapts.f1091a1a	ALYac	Gen:Variant.Ulise.173672
Antiy-AVL	Trojan/Generic.ASMalwS.15D285	Arcabit	Trojan.Ulise.D2A668
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	BDS/Backdoor.Gen	BitDefender	Gen:Variant.Ulise.173672
BitDefenderTheta	Gen:NN.ZedlaF.34236.bq5@aq5eUxk	CAT-QuickHeal	Trojan.Connapts
ClamAV	Win.Trojan.Agent-385568	Comodo	TrojWare.Win32.Small.dy39@4owfj9
CrowdStrike Falcon	Win/malicious_confidence_90% (W)	Cylance	Unsafe
Cynet	Malicious (score: 100)	DrWeb	BackDoor.Siggen.38566
eGambit	Unsafe.AI_Score_63%	Elastic	Malicious (high Confidence)
Emsisoft	Gen:Variant.Ulise.173672 (B)	eScan	Gen:Variant.Ulise.173672
ESET-NOD32	A Variant Of Win32/Small.NDX	FireEye	Generic.mg.84882c9d43e23d63
Fortinet	W32/Small.NDX!tr	GData	Gen:Variant.Ulise.173672

- The virus can be detected in 59
- Its basic information



Basic Properties

MD5	84882c9d43e23d63b82004fae74ebb61
SHA-1	c6fb3b50d946bec6f391aefa4e54478cf8607211
SHA-256	5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9
Vhash	124046655d5550c8z142qz71ze6z5
Authentihash	b76700f50d6f09408958f9e40f562908cd4050e0f992efaec0ca63e0fc9638e0
Imphash	3167552ee0bbbd4f5f440adf5f65bab8
Rich PE header hash	0b35dd18f37347b1f6e183c884f29a4e
SSDEEP	384:NcTA0TAKHWYvVvUYGXFgeJGjHwTACLPkldSgbl/xAlrWdhoQsxRiAHz:NcTA0TAK2y2oBCbH4gtxrWd5sxRL
TLSH	T17AB2090693482CE3C5D50C3433765F2D8F3F366A275DD39BEA431B5839AA55AAC78306
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (38.8%)
TrID	Microsoft Visual C++ compiled executable (generic) (20.5%)
TrID	Win64 Executable (generic) (13%)
TrID	Win32 Dynamic Link Library (generic) (8.1%)
TrID	Win16 NE executable (generic) (6.2%)
File size	23.50 KB (24065 bytes)
PEiD packer	Microsoft Visual C++ v6.0 DLL

+ Hashes types : MD5, SHA-1, SHA-256, Vhash, Authentihas, SSDEEP.

+ File type : Win32 DLL

+ Packer used: PEiD paker

+ File size : 23.50 KB (24065 bytes)

+ Creation time: 2010-09-28 01:00:25

- It aim and behaviors

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

+ Imports : ADVAPI32.dll

KERNEL32.dll

MSVCRT.dll

WS2_32.dll

WININET.dll

+ Contact IP:

54.70.80.82	US
34.215.46.102	US
13.227.222.97	US
34.216.113.46	US
13.227.222.34	US
13.227.222.36	US
54.148.159.250	US
44.235.28.153	US
35.167.137.152	US
44.225.87.131	US
13.227.222.18	US
35.155.229.139	US
20.190.160.8	NL
20.190.159.132	IE
40.126.31.6	IE
40.126.31.4	IE
40.126.31.1	IE

13.89.179.12	US
40.126.31.141	IE
40.126.31.143	IE

+ Domain:

firefox.settings.services.mozilla.com

telemetry-incoming.r53-2.services.mozilla.com

pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com

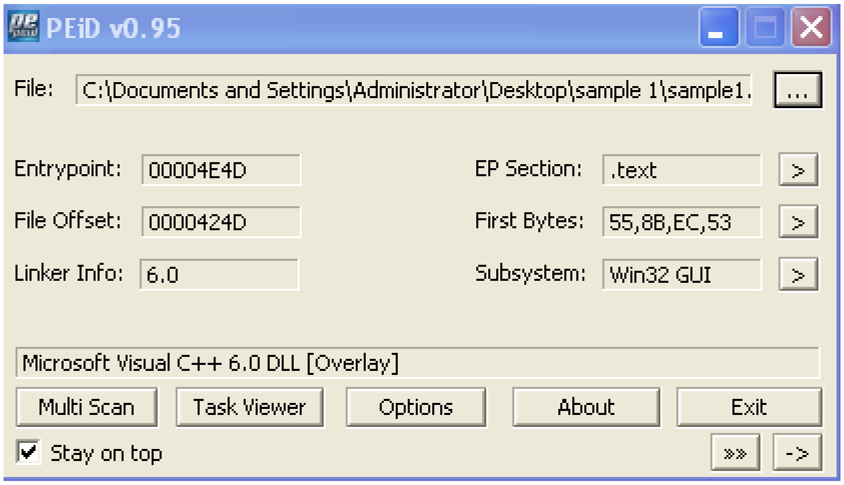
login.live.com

arc.msn.com

incoming.telemetry.mozilla.org

Check in tools

Check in PEid



PEiD v0.95

File: C:\Documents and Settings\Administrator\Desktop\sample 1\sample1.

Entrypoint: 00004E4D

EP Section: .text

File Offset: 0000424D

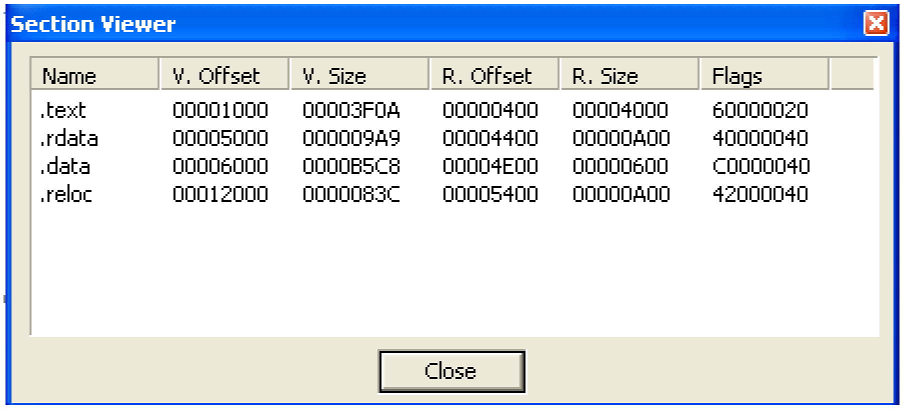
First Bytes: 55,8B,EC,53

Linker Info: 6.0

Subsystem: Win32 GUI

Microsoft Visual C++ 6.0 DLL [Overlay]

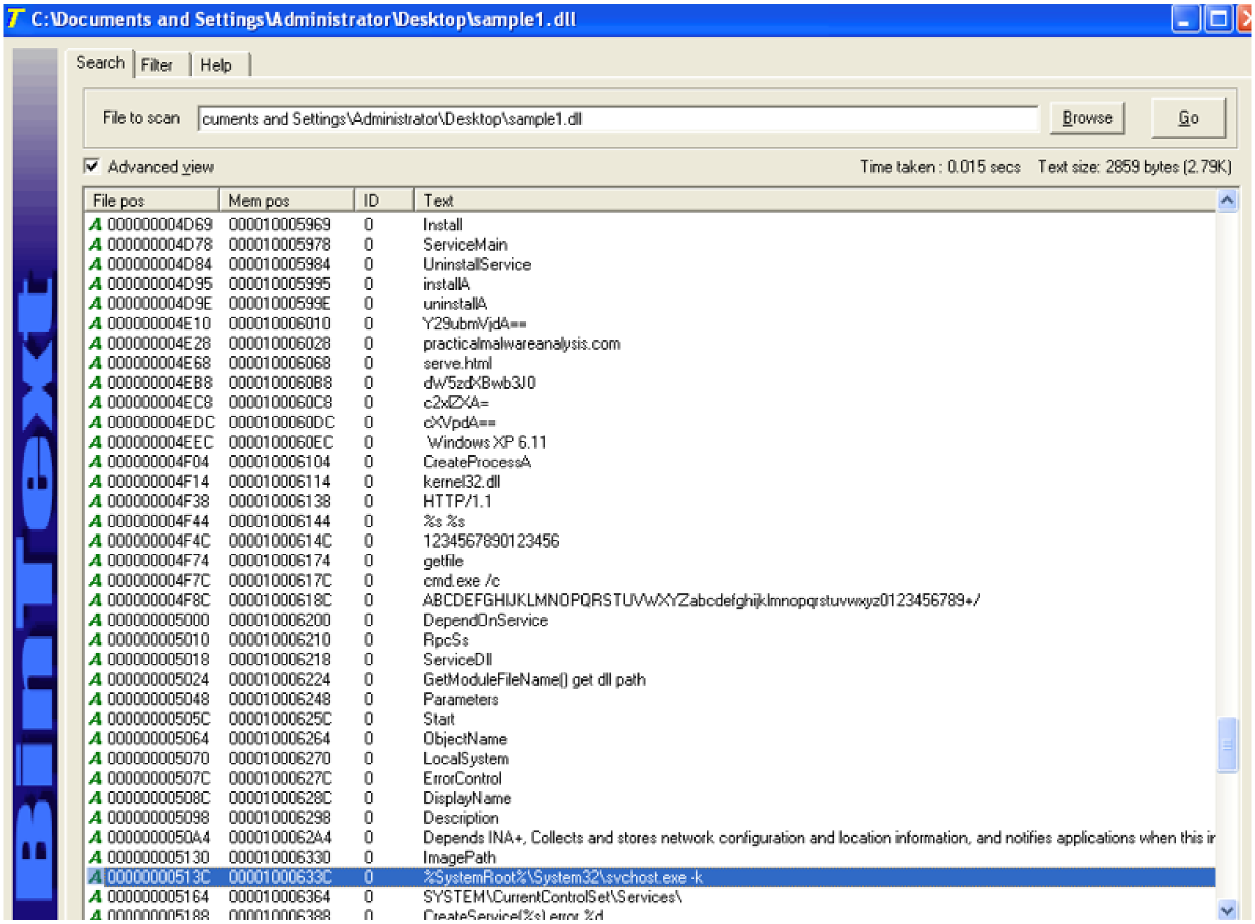
☑ Stay on top



Section Viewer

Name	V. Offset	V. Size	R. Offset	R. Size	Flags
.text	00001000	00003F0A	00000400	00004000	60000020
.rdata	00005000	000009A9	00004400	00000A00	40000040
.data	00006000	0000B5C8	00004E00	00000600	C0000040
.reloc	00012000	0000083C	00005400	00000A00	42000040

Check on BinText



File to scan: cuments and Settings\Administrator\Desktop\sample1.dll

☑ Advanced view

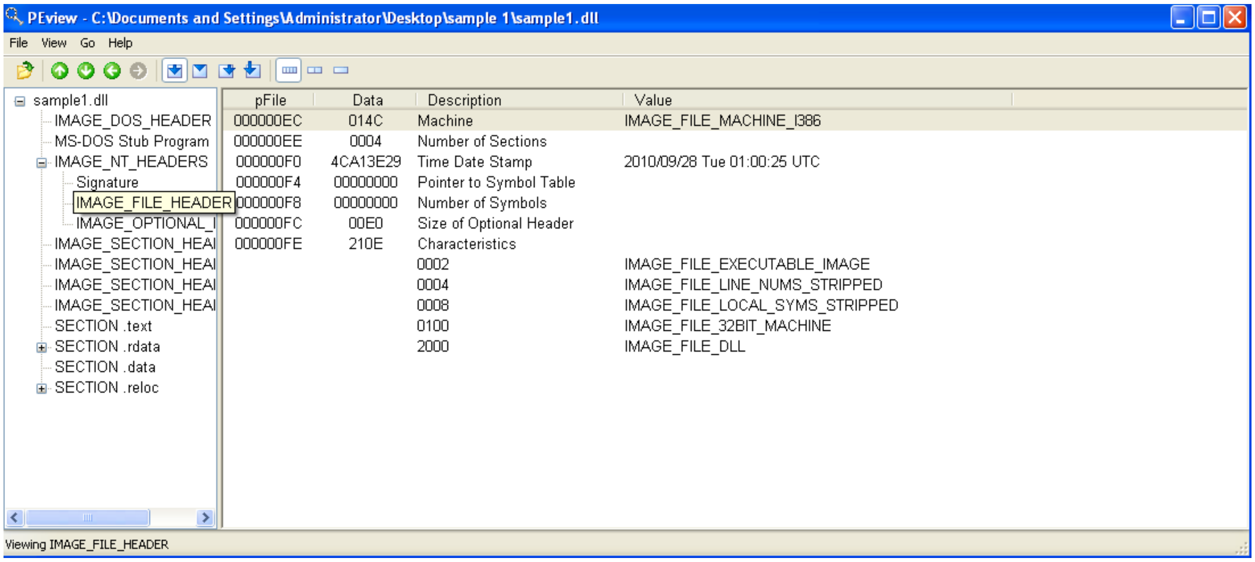
Time taken : 0.015 secs   Text size: 2859 bytes (2.79K)

File pos	Mem pos	ID	Text
A 000000004D69	000010005969	0	Install
A 000000004D78	000010005978	0	ServiceMain
A 000000004D84	000010005984	0	UninstallService
A 000000004D95	000010005995	0	installA
A 000000004D9E	00001000599E	0	uninstallA
A 000000004E10	000010006010	0	Y29ubmVjdA==
A 000000004E28	000010006028	0	practicalmalwareanalysis.com
A 000000004E68	000010006068	0	serve.html
A 000000004EB8	0000100060B8	0	dW5zdXBwb3J0
A 000000004EC8	0000100060C8	0	c2xlZXA=
A 000000004EDC	0000100060DC	0	cXVpdA==
A 000000004EEC	0000100060EC	0	Windows XP 6.11
A 000000004F04	000010006104	0	CreateProcessA
A 000000004F14	000010006114	0	kernel32.dll
A 000000004F38	000010006138	0	HTTP/1.1
A 000000004F44	000010006144	0	%s %s
A 000000004F4C	00001000614C	0	1234567890123456
A 000000004F74	000010006174	0	getfile
A 000000004F7C	00001000617C	0	cmd.exe /c
A 000000004F8C	00001000618C	0	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
A 000000005000	000010006200	0	DependOnService
A 000000005010	000010006210	0	RpcSs
A 000000005018	000010006218	0	ServiceDll
A 000000005024	000010006224	0	GetModuleFileName() get dll path
A 000000005048	000010006248	0	Parameters
A 00000000505C	00001000625C	0	Start
A 000000005064	000010006264	0	ObjectName
A 000000005070	000010006270	0	LocalSystem
A 00000000507C	00001000627C	0	ErrorControl
A 00000000508C	00001000628C	0	DisplayName
A 000000005098	000010006298	0	Description
A 0000000050A4	0000100062A4	0	Depends INA+, Collects and stores network configuration and location information, and notifies applications when this ir
A 000000005130	000010006330	0	ImagePath
A 00000000513C	00001000633C	0	%SystemRoot%\System32\svchost.exe -k
A 000000005164	000010006364	0	SYSTEM\CurrentControlSet\Services\
A 000000005188	000010006388	0	CreateService(%s) error %d

Some interested string : HTTP/1.1

I think is a Trojan

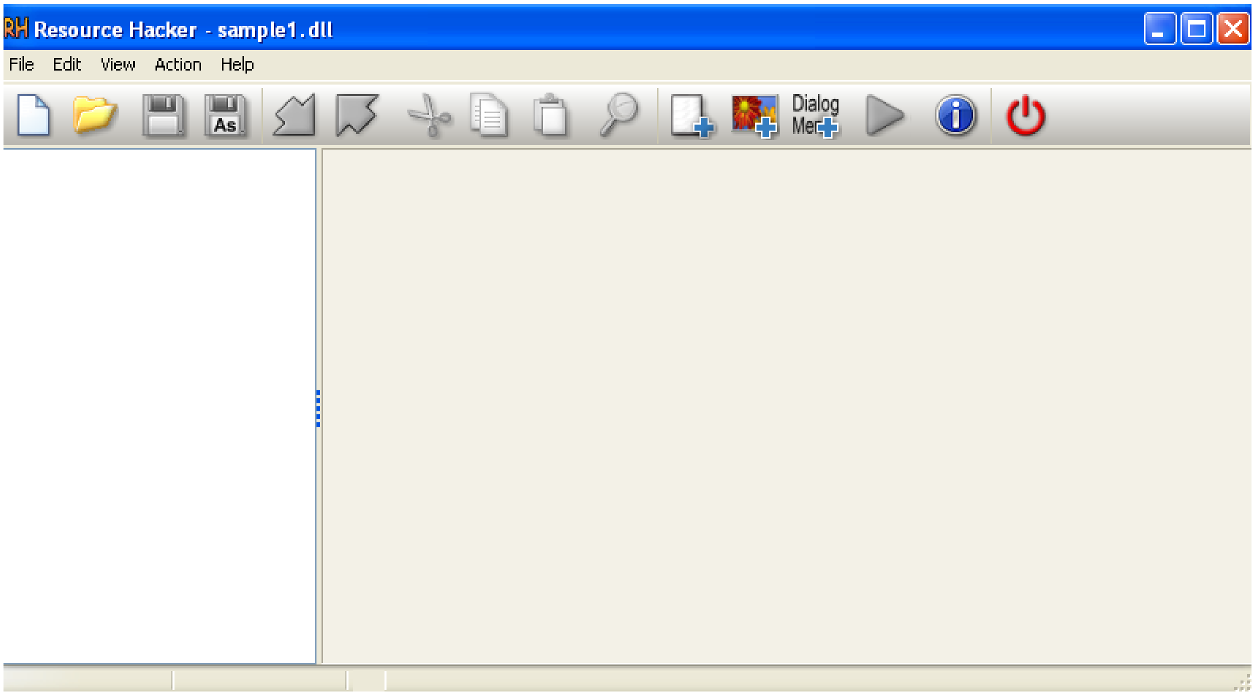
Check PEview



pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0004	Number of Sections	
000000F0	4CA13E29	Time Date Stamp	2010/09/28 Tue 01:00:25 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	210E	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE
		2000	IMAGE_FILE_DLL

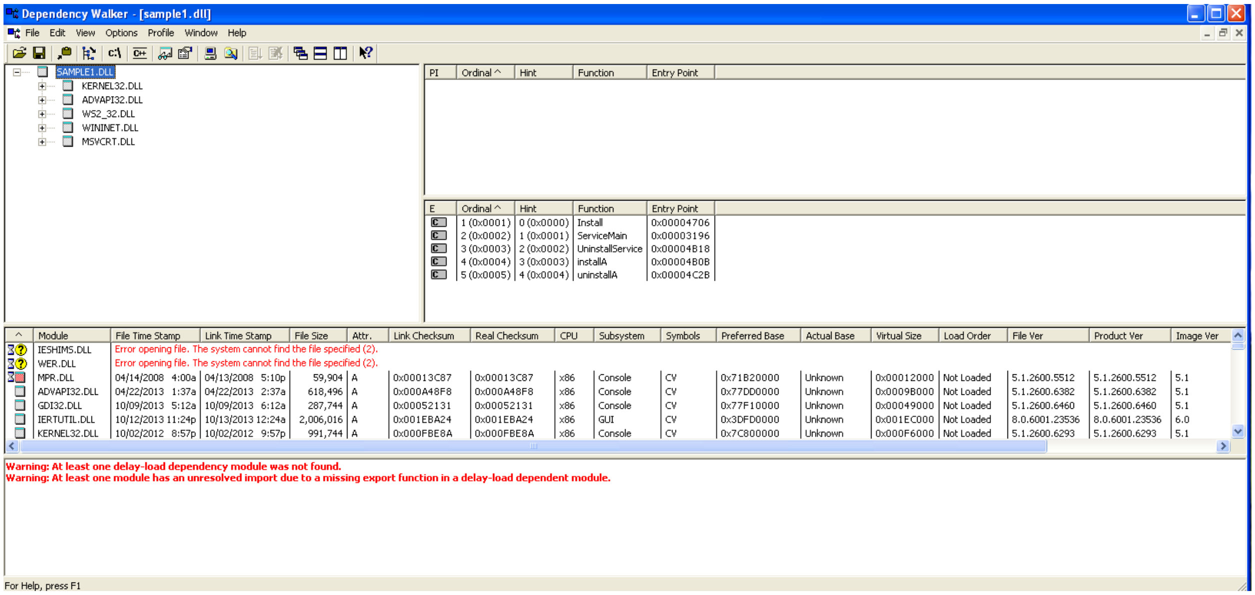
Viewing IMAGE_FILE_HEADER

Check Reesource



Have nothing

Check Dependency Walker



```
SAMPLE1.DLL
    KERNEL32.DLL
    ADVAPI32.DLL
    WS2_32.DLL
    WININET.DLL
    MSVCRT.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	Install	0x00004706
C	2 (0x0002)	1 (0x0001)	ServiceMain	0x00003196
C	3 (0x0003)	2 (0x0002)	UninstallService	0x00004B18
C	4 (0x0004)	3 (0x0003)	installA	0x00004B0B
C	5 (0x0005)	4 (0x0004)	uninstallA	0x00004C2B

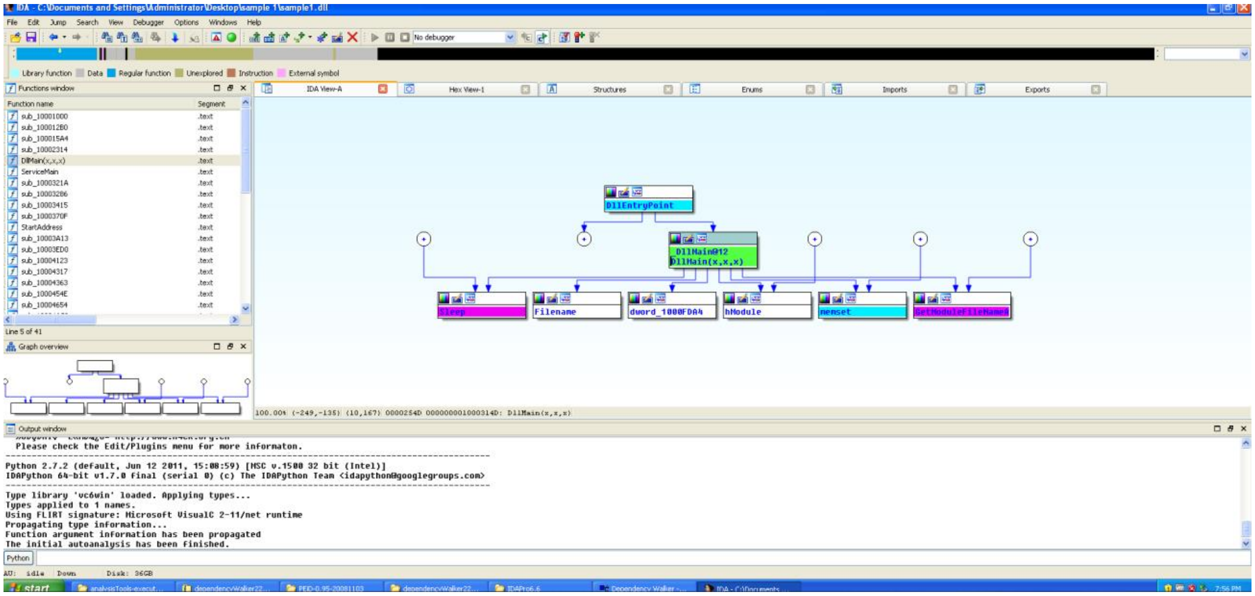
^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver	Product Ver	Image Ver
?	IESHIMS.DLL	Error opening file. The system cannot find the file specified (2).															
?	WER.DLL	Error opening file. The system cannot find the file specified (2).															
	MPR.DLL	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	5.1.2600.5512	5.1
	ADVAPI32.DLL	04/22/2013 1:37a	04/22/2013 2:37a	618,496	A	0x000A48F8	0x000A48F8	x86	Console	CV	0x77DD0000	Unknown	0x0009B000	Not Loaded	5.1.2600.6382	5.1.2600.6382	5.1
	GDI32.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	5.1.2600.6460	5.1
	IERTUTIL.DLL	10/12/2013 11:24p	10/13/2013 12:24a	2,006,016	A	0x001EBA24	0x001EBA24	x86	GUI	CV	0x3DFD0000	Unknown	0x001EC000	Not Loaded	8.0.6001.23536	8.0.6001.23536	6.0
	KERNEL32.DLL	10/02/2012 8:57p	10/02/2012 9:57p	991,744	A	0x000FBE8A	0x000FBE8A	x86	Console	CV	0x7C800000	Unknown	0x000F6000	Not Loaded	5.1.2600.6293	5.1.2600.6293	5.1

```
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.
```

For Help, press F1

- Check internet connect

Check malware on IDAq



Function name	Segment
sub_10001000	.text
sub_100012B0	.text
sub_100015A4	.text
sub_10002314	.text
DllMain(x,x,x)	.text
ServiceMain	.text
sub_1000321A	.text
sub_10003286	.text
sub_10003415	.text
sub_1000370F	.text
StartAddress	.text
sub_10003A13	.text
sub_10003ED0	.text
sub_10004123	.text
sub_10004317	.text
sub_10004363	.text
sub_1000454E	.text
sub_10004654	.text

Line 5 of 41

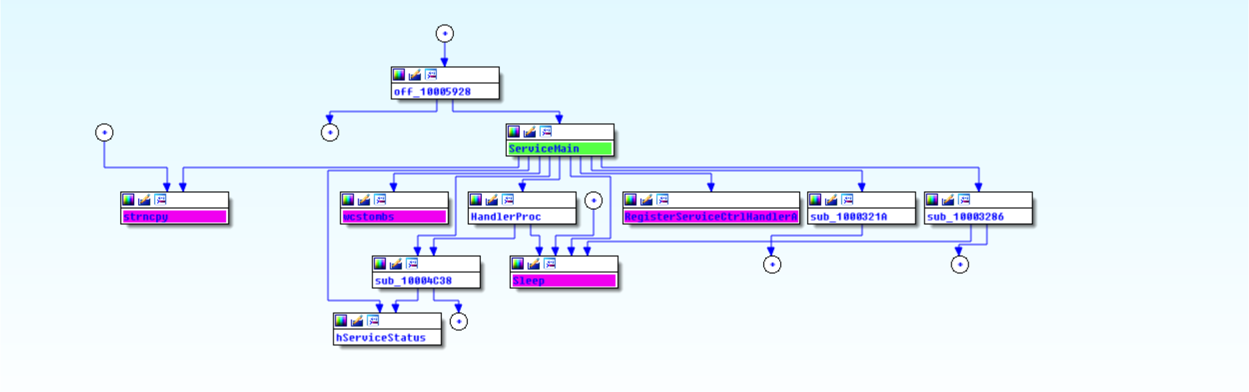
```
100.00% (-249,-135) (10,167) 0000254D 000000001000314D: DllMain(x,x,x)
```

```
  Please check the Edit/Plugins menu for more informaton.
---------------------------------------------------------------------------------------
Python 2.7.2 (default, Jun 12 2011, 15:08:59) [MSC v.1500 32 bit (Intel)]
IDAPython 64-bit v1.7.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
---------------------------------------------------------------------------------------
Type library 'vc6win' loaded. Applying types...
Types applied to 1 names.
Using FLIRT signature: Microsoft VisualC 2-11/net runtime
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
```

```
AU:  idle   Down      Disk: 36GB
```

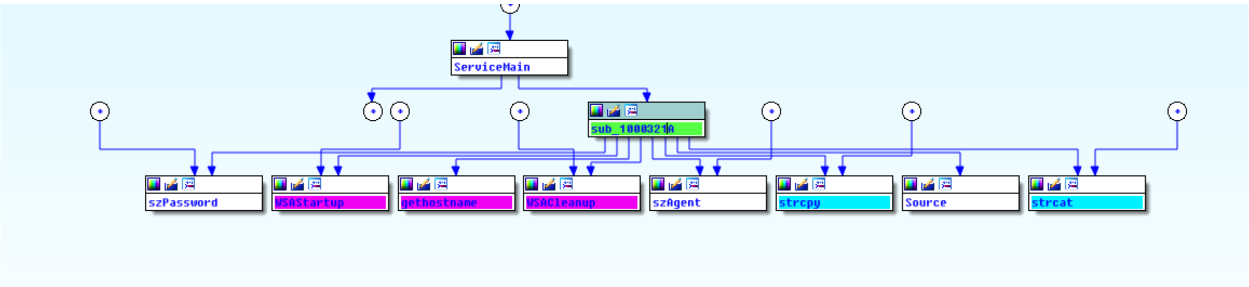
It is main DllMain(x,x,x)

We check ServiceMain

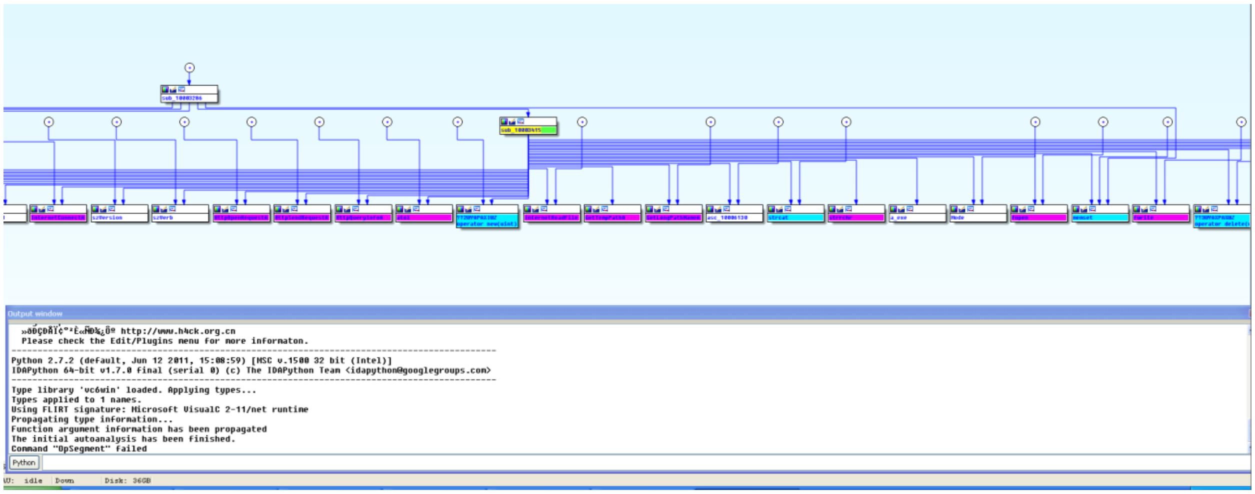


It look like the main of the malware

We check sub_1000321A



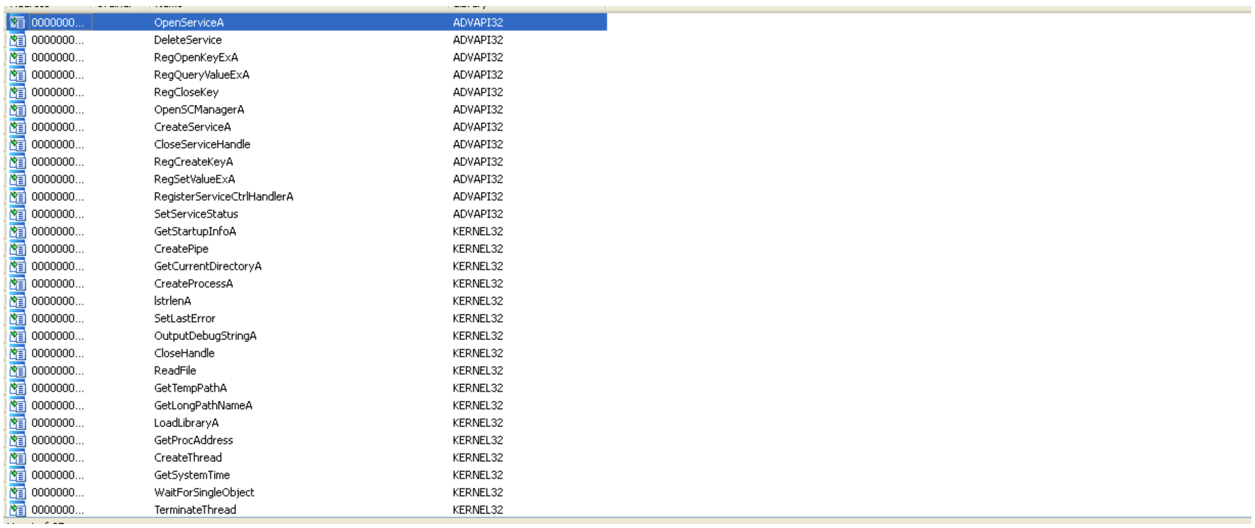
We check sub_10003415



```
  »ðÕÇÐÅÏ¢º²È«ÑÐ¾¿Ôº http://www.h4ck.org.cn
  Please check the Edit/Plugins menu for more informaton.
---------------------------------------------------------------------------------------
Python 2.7.2 (default, Jun 12 2011, 15:08:59) [MSC v.1500 32 bit (Intel)]
IDAPython 64-bit v1.7.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
---------------------------------------------------------------------------------------
Type library 'vc6win' loaded. Applying types...
Types applied to 1 names.
Using FLIRT signature: Microsoft VisualC 2-11/net runtime
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
Command "OpSegment" failed
```

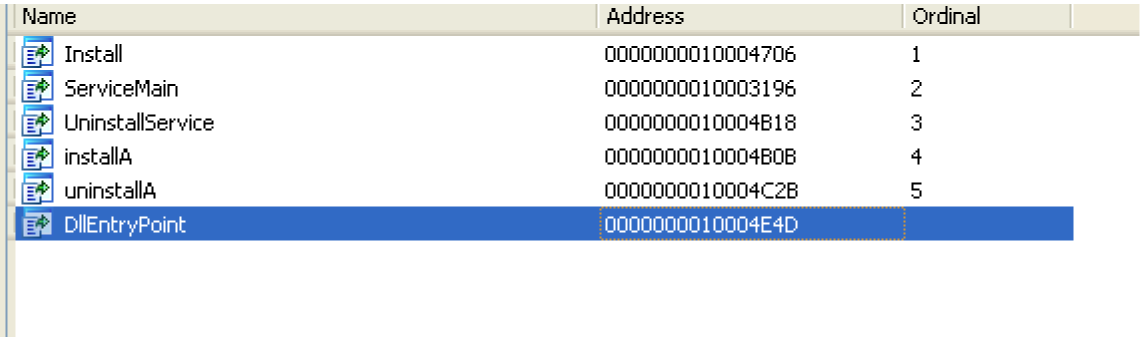
AU: idle   Down   Disk: 36GB

Import



0000000...		OpenServiceA	ADVAPI32
0000000...		DeleteService	ADVAPI32
0000000...		RegOpenKeyExA	ADVAPI32
0000000...		RegQueryValueExA	ADVAPI32
0000000...		RegCloseKey	ADVAPI32
0000000...		OpenSCManagerA	ADVAPI32
0000000...		CreateServiceA	ADVAPI32
0000000...		CloseServiceHandle	ADVAPI32
0000000...		RegCreateKeyA	ADVAPI32
0000000...		RegSetValueExA	ADVAPI32
0000000...		RegisterServiceCtrlHandlerA	ADVAPI32
0000000...		SetServiceStatus	ADVAPI32
0000000...		GetStartupInfoA	KERNEL32
0000000...		CreatePipe	KERNEL32
0000000...		GetCurrentDirectoryA	KERNEL32
0000000...		CreateProcessA	KERNEL32
0000000...		lstrlenA	KERNEL32
0000000...		SetLastError	KERNEL32
0000000...		OutputDebugStringA	KERNEL32
0000000...		CloseHandle	KERNEL32
0000000...		ReadFile	KERNEL32
0000000...		GetTempPathA	KERNEL32
0000000...		GetLongPathNameA	KERNEL32
0000000...		LoadLibraryA	KERNEL32
0000000...		GetProcAddress	KERNEL32
0000000...		CreateThread	KERNEL32
0000000...		GetSystemTime	KERNEL32
0000000...		WaitForSingleObject	KERNEL32
0000000...		TerminateThread	KERNEL32

Exports



Name	Address	Ordinal
Install	0000000010004706	1
ServiceMain	0000000010003196	2
UninstallService	0000000010004B18	3
installA	0000000010004B0B	4
uninstallA	0000000010004C2B	5
DllEntryPoint	0000000010004E4D	

Summary

Create a service name INA+