

# Malware Analysis Final Report

## Contents

I. Check on VirusTotal.....	2
Information gathered:.....	2
II. Check on tools .....	5
Check on PEid .....	5
Check on PView.....	6
Dependency Walker .....	7
Check on BinText .....	7
Resource Hacker.....	8
Malware on IDA.....	8
III. Conclusion .....	11

# I. Check on VirusTotal

## Information gathered:

5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9

59 / 68

59 security vendors and 1 sandbox flagged this file as malicious

5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9  
Lab03-02.dll

23.50 KB  
Size

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

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

Community Score

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Ad-Aware	Gen:Variant.Ulise.173672	AhnLab-V3	Trojan.Win32.Xeme.C93063	
Alibaba	Backdoor:Win32/Connpts.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@eq5eLwkk	CAT-QuickHeal	Trojan.Connpts	
ClamAV	Win.Trojan.Agent-385568	Comodo	TrojWare.Win32.Small.dy39@4owfj9	
CrowdStrike Falcon	Win/malicious_confidence_90% (W)	Cylance	Unsafe	

- The virus can be detected in 59 anti-virus platforms.

- Basic properties:

#### Basic Properties ⓘ

MD5	84882c9d43e23d63b82004fae74ebb61
SHA-1	c6fb3b50d946bec6f391aefa4e54478cf8607211
SHA-256	5eced7367ed63354b4ed5c556e2363514293f614c2c2eb187273381b2ef5f0f9
Vhash	124046655d5550c8z142qz71ze6z5
Authentihash	b76700f50d6f09408958f9e40f562908cd4050e0f992efaec0ca63e0fc9638e0
Imphash	3167552ee0bbbd4f5f440adff5f65bab8
Rich PE header hash	0b35dd18f37347b1f6e183c884f29e4e
SSDEEP	384:NcTA0TAKHWYVVvUYGXFgeJGjHwTACLPkIdSgbl/xAirWdhoQsxRIAHZ:NcTA0TAK2y2oBCbH4gtxrWd5sxRL
TLSH	T17AB2090693482CE3C5D50C3433765F2D8F3F366A275DD39BEA431B5839AA55AAC78306
File type	Win32 DLL
Magic	PE32 executable for MSWindows (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, Authentihash, SSDEEP.

+ File type: Win32 DLL

+ Packer used: PEiD and F-PROT

+ File size: 23.5 KB

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

- 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
- + WININET.dll

+ Contact IP:

IP	Detections	Autonomous System	Country
54.70.80.82	 / 90	16509	US
34.215.46.102	 / 90	16509	US
13.227.222.97	 / 91	16509	US
34.216.113.46	 / 90	16509	US
13.227.222.34	 / 89	16509	US
13.227.222.36	 / 90	16509	US
54.148.159.250	 / 89	16509	US
44.235.28.153	 / 90	16509	US
35.167.137.152	 / 90	16509	US
44.225.87.131	 / 89	16509	US
13.227.222.18	 / 89	16509	US
35.155.229.139	 / 90	16509	US
20.190.160.8	 / 90	8075	NL
20.190.159.132	 / 90	8075	IE
40.126.31.6	 / 90	8075	IE
40.126.31.4	 / 90	8075	IE
40.126.31.1	 / 90	8075	IE
13.89.179.12	 / 90	8075	US
40.126.31.141	 / 90	8075	IE
40.126.31.143	 / 90	8075	IE
20.190.160.129	 / 90	8075	NL
20.190.160.75	 / 90	8075	NL
20.190.160.73	 / 90	8075	NL
20.190.160.71	 / 90	8075	NL
40.126.31.139	 / 90	8075	IE

20.190.159.136	0 / 90	8075	IE
20.42.73.29	0 / 90	8075	US
20.190.159.138	0 / 90	8075	IE
40.126.31.135	0 / 90	8075	IE
40.126.31.137	0 / 90	8075	IE
20.190.160.136	0 / 90	8075	NL
20.190.160.134	0 / 90	8075	NL
20.190.160.67	0 / 90	8075	NL
20.49.157.6	0 / 91	8075	GB

+ Contacted domains:

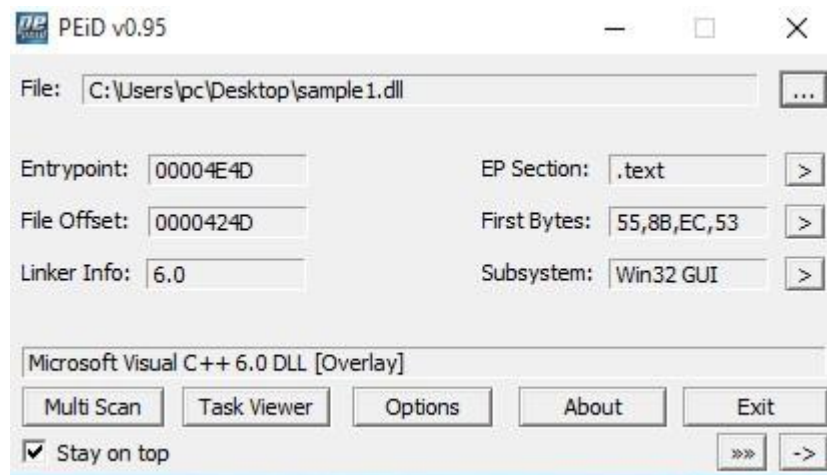
#### Contacted Domains ⓘ

Domain	Detections	Created	Registrar
firefox.settings.services.mozilla.com	0 / 90	1994-10-18	MarkMonitor Inc.
telemetry-incoming.r53-2.services.mozilla.com	0 / 90	1994-10-18	MarkMonitor Inc.
pipeline-incoming-prod-elb-149169523.us-west-2.elb.amazonaws.com	0 / 90	2005-08-18	MarkMonitor Inc.
login.live.com	0 / 90	1994-12-28	CSC CORPORATE DOMAINS, INC.
arc.msn.com	0 / 90	1994-11-10	MarkMonitor Inc.
incoming.telemetry.mozilla.org	0 / 90	1998-01-24	MarkMonitor Inc.

+ Behavior: Open/write files, create processes, make shell commands, create/open mutexes, load module.

## II. Check on tools

### Check on PEid



Section Viewer:

## 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

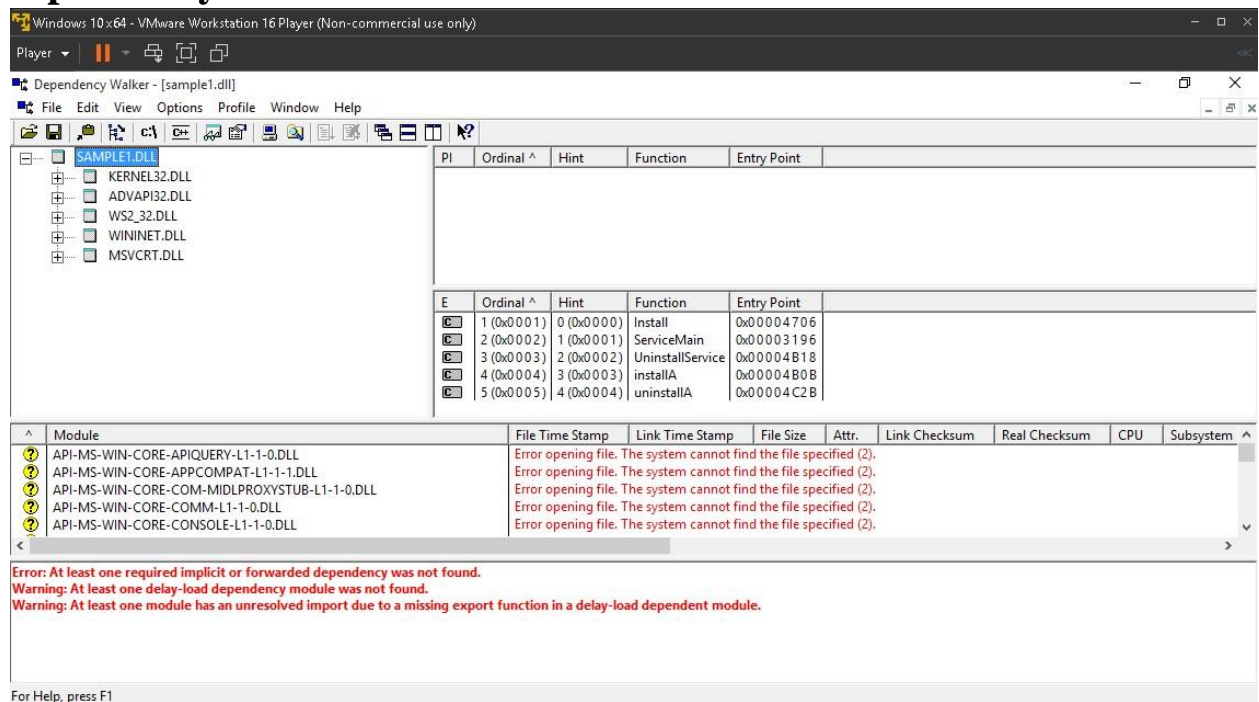
Close

## Check on PView

PEview - C:\Users\pc\Desktop\sample1.dll

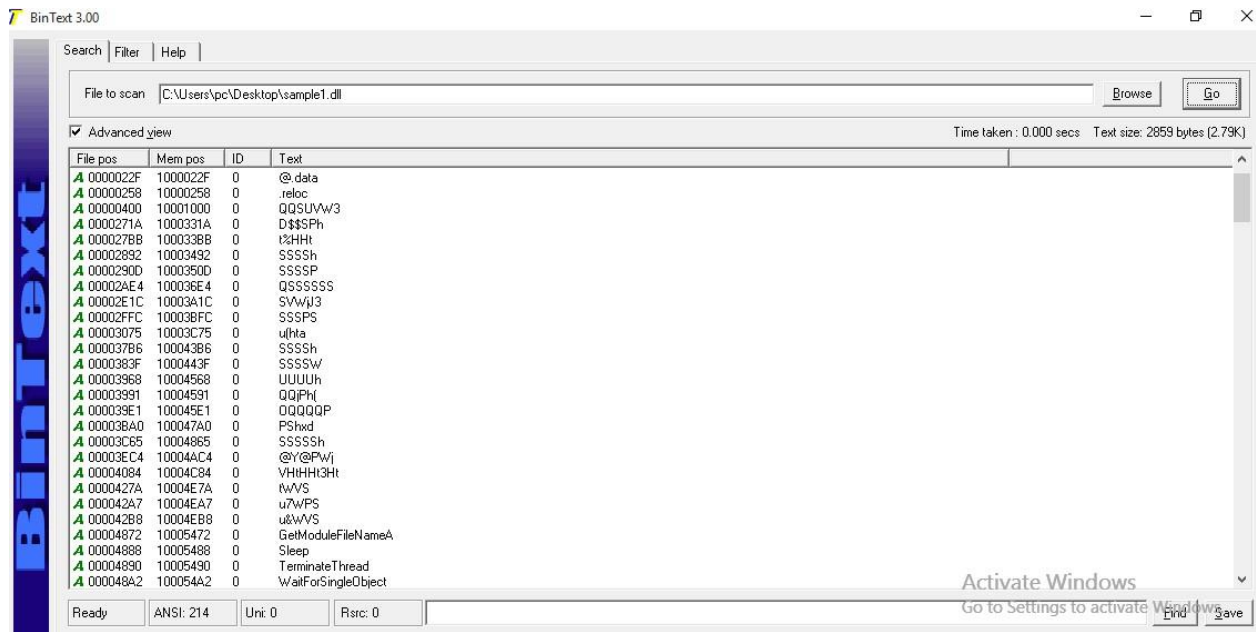
	pFile	Raw Data	Value
sample1.dll	00000060	74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20	t be run in DOS
IMAGE_DOS_HEADER	00000070	6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00	mode...\$
MS-DOS Stub Program	00000080	9A 7A 9B C0 DE 1B F5 93 DE 1B F5 93 DE 1B F5 93	.z.....
IMAGE_NT_HEADERS	00000090	A5 07 F9 93 DA 1B F5 93 5D 07 FB 93 DC 1B F5 93	.....]
Signature	000000A0	36 04 FF 93 DA 1B F5 93 DE 1B F5 93 D7 1B F5 93	6.....
IMAGE_FILE_HEADER	000000B0	DE 1B F4 93 8E 1B F5 93 BC 04 E6 93 D9 1B F5 93	.....
IMAGE_OPTIONAL_HEADER	000000C0	36 04 FE 93 DD 1B F5 93 36 04 F1 93 DD 1B F5 93	6.....6
IMAGE_SECTION_HEADER .text	000000D0	52 69 63 68 DE 1B F5 93 00 00 00 00 00 00 00 00	Rich.....
IMAGE_SECTION_HEADER .rdata	000000E0	00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00	.....PE..L
IMAGE_SECTION_HEADER .data	000000F0	29 3E A1 4C 00 00 00 00 00 00 00 00 E0 00 0E 21	)>.L.....!
IMAGE_SECTION_HEADER .reloc	00000100	0B 01 06 00 00 40 00 00 00 CA 00 00 00 00 00 00	@.....
SECTION .text	00000110	4D 4E 00 00 00 10 00 00 00 50 00 00 00 00 00 10	MN.....P
SECTION .rdata	00000120	00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00	.....0
IMPORT Address Table	00000130	04 00 00 00 00 00 00 00 00 30 01 00 00 04 00 00	.....
IMPORT Directory Table	00000140	00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00	.....
IMPORT Name Table	00000150	00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00	.....
IMPORT Hints/Names & DLL Names	00000160	00 59 00 00 A9 00 00 00 90 52 00 00 78 00 00 00	.Y.....R..x
IMAGE_EXPORT_DIRECTORY	00000170	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
EXPORT Address Table	00000180	00 00 00 00 00 00 00 00 00 20 01 00 24 07 00 00	.....\$.
EXPORT Name Pointer Table	00000190	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
EXPORT Ordinal Table	000001A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
EXPORT Names	000001B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
SECTION .data	000001C0	00 50 00 00 68 01 00 00 00 00 00 00 00 00 00 00	.P..h
SECTION .reloc	000001D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
IMAGE_BASE_RELOCATION	000001E0	2E 74 65 78 74 00 00 00 0A 3F 00 00 00 10 00 00	.text...?

# Dependency Walker



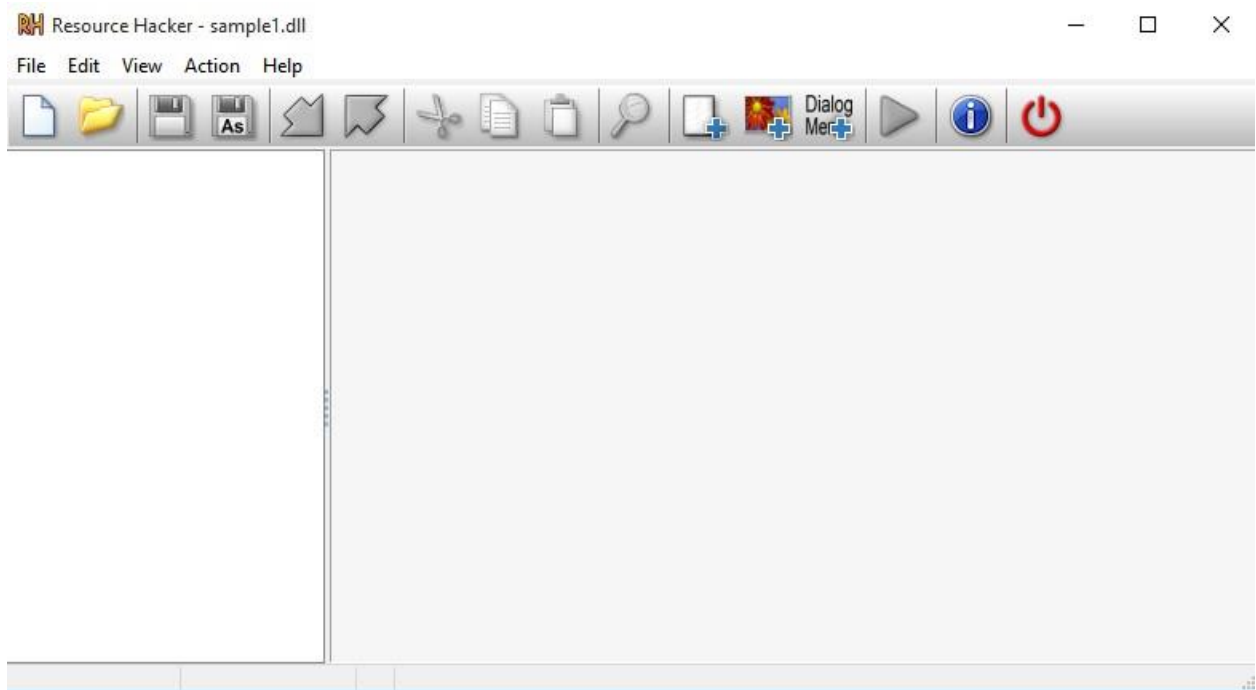
Checking for internet connection

# Check on BinText



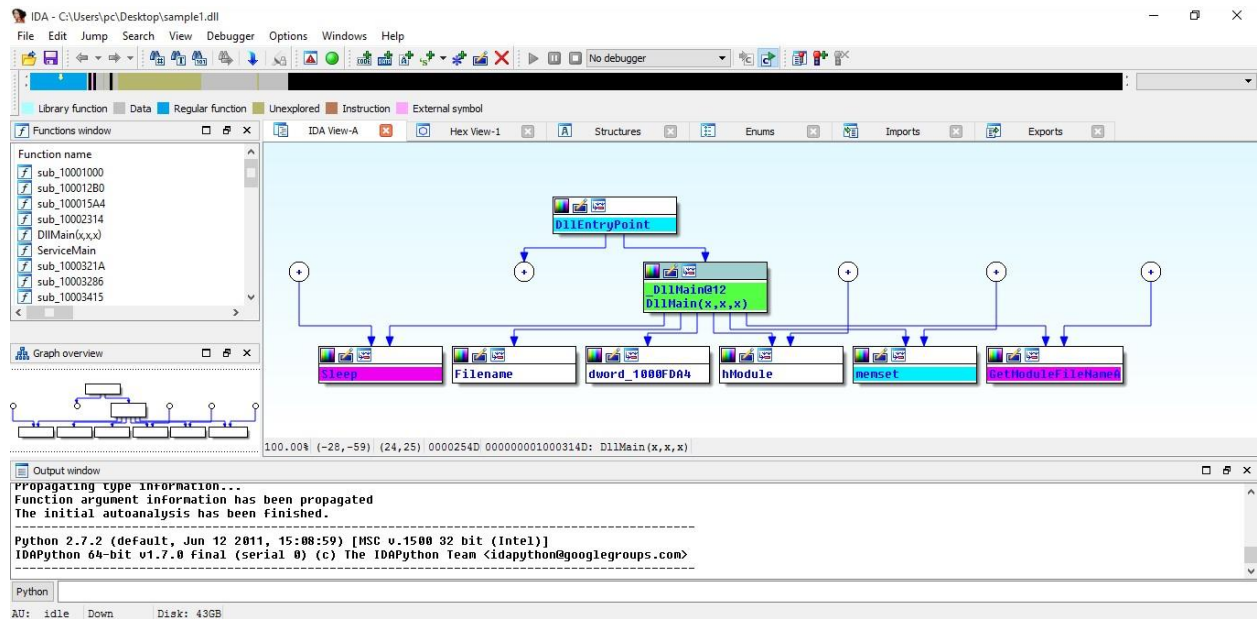


# Resource Hacker

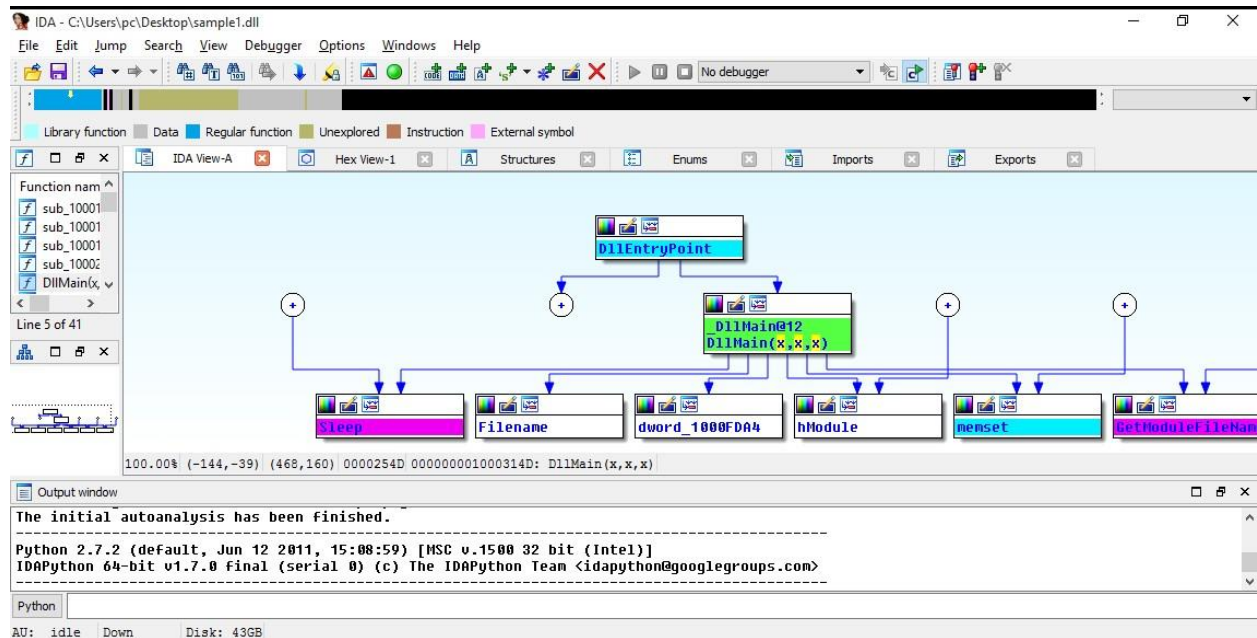


There's nothing when checked with RH

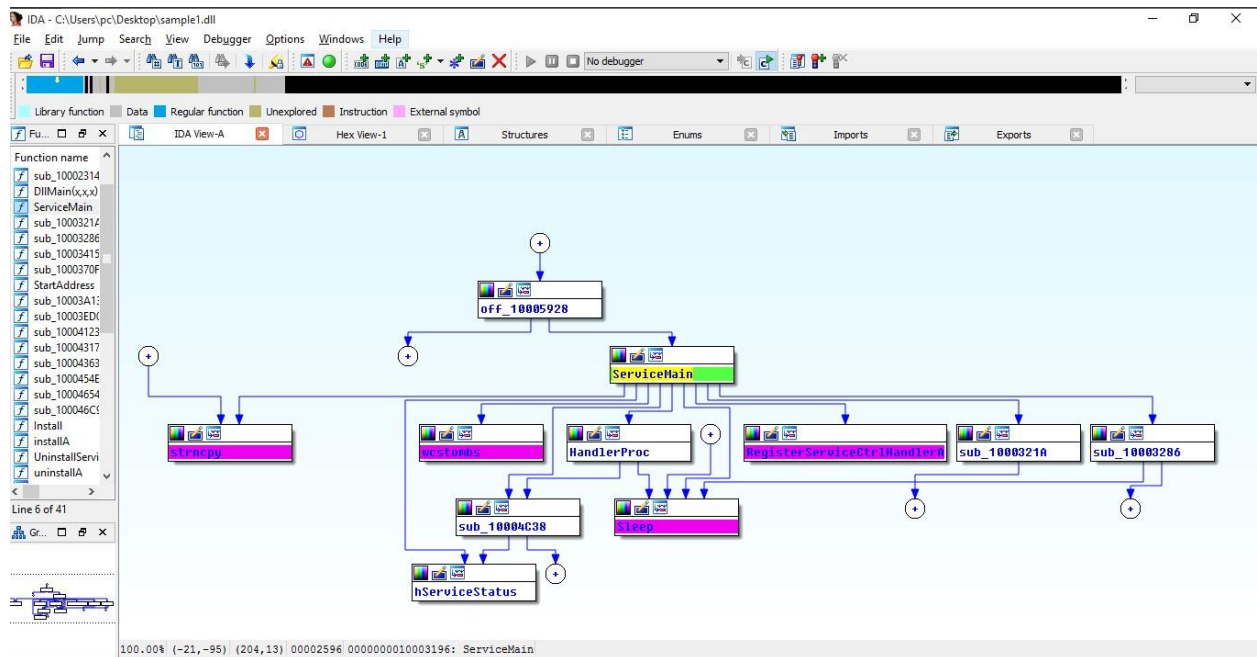
# Malware on IDA





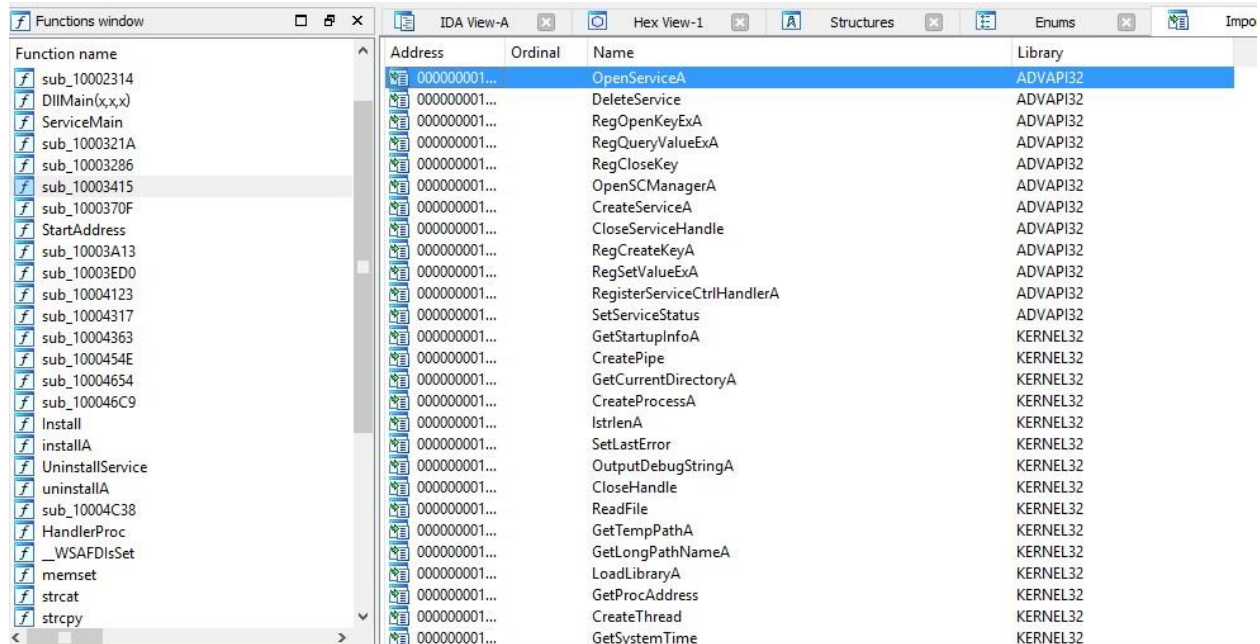


DllMain(x,x,x)

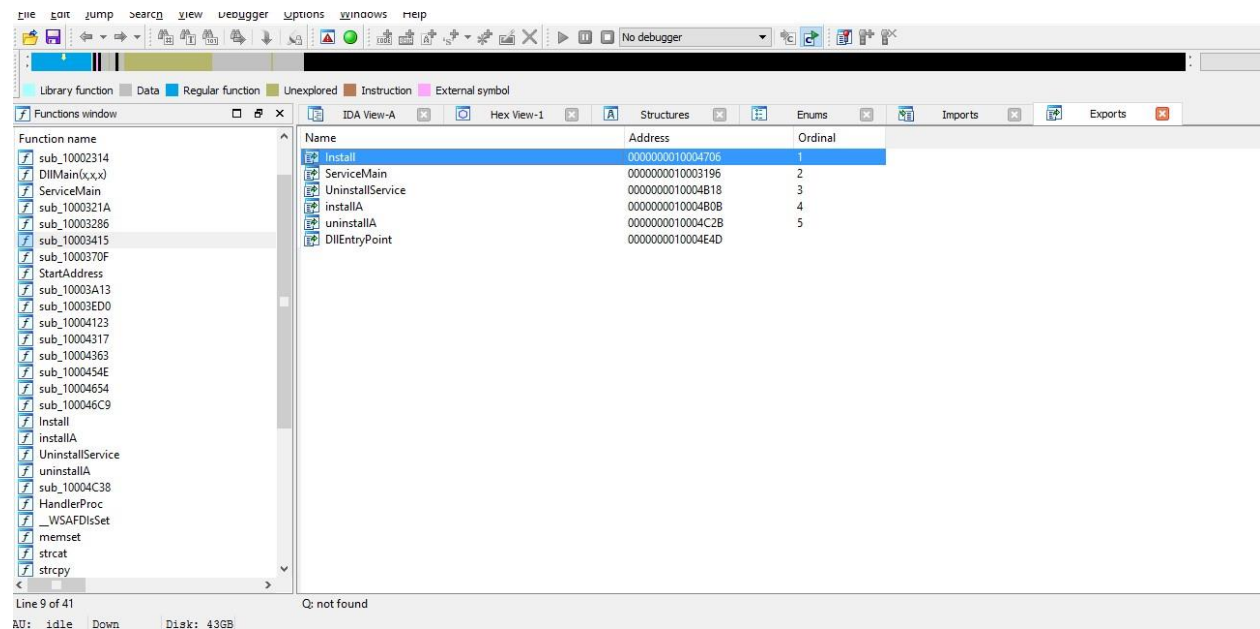


ServiceMain





## Imports



## Exports

# III. Conclusion

Created 1 service named INA+