

## **Assignment 1 Report**

Group Name: Aw, Snap!

Group Members: Weijia Sun, Xinyu Lyu, Mengmei Ye

1.

This is the result for Lab01-01.dll

Search or scan a URL, IP address, domain, or file hash

Sign in

DLL

32 / 67

32 engines detected this file

SHA-256f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

File nameLab01-01.dll

File size160 KB

Last analysis2019-02-15 13:19:18 UTC

Community score-143

Detection

Details

Relations

Community

Acronis	suspicious	AegisLab	Trojan.Win32.Generic.4!c
ALYac	Trojan.Agent.Waski	Antiy-AVL	Trojan/Win32.BTSGeneric
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Dldr.Waski.163840.1	CAT-QuickHeal	Trojan.IGENERIC
ClamAV	Win.Malware.Agent-6369668-0	Comodo	Malware@#2dsw4albnc61
Cylance	Unsafe	Cyren	W32/Trojan.PXBS-7022
Endgame	malicious (high confidence)	ESET-NOD32	a variant of Generic.TGEWDD
F-Secure	Trojan.TR/Dldr.Waski.163840.1	Fortinet	PossibleThreat
GData	Win32:Trojan.Agent.4L5OBS	Ikarus	Trojan.SuspectCRC
McAfee	GenericRXFO-RT1290934C61DE9	McAfee-GW-Edition	GenericRXFO-RT1290934C61DE9
Microsoft	Trojan:Win32/Occamy.C	NANO-Antivirus	Trojan.Win32.Waski.dtkvsp
Qihoo-360	Win32/Trojan.54f	Rising	Trojan.Tilken!8.F605 (CLOUD)
Sophos ML	heuristic	Symantec	Trojan.Gen.2
TheHacker	Trojan/Generic.TGEWDD	TrendMicro-HouseCall	TROJ_GEN.R002C0PLO18
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Gen.BT
Yandex	Trojan.Agent!//HTSKjKET4	Zillya	Adware.InstallCore.Win32.1036
Ad-Aware	Clean	AhnLab-V3	Clean
Alibaba	Clean	Arcabit	Clean
Avast Mobile Security	Clean	Babable	Clean
Baidu	Clean	BitDefender	Clean
Bkav	Clean	CMC	Clean
CrowdStrike Falcon	Clean	DrWeb	Clean
eGambit	Clean	Emsisoft	Clean
eScan	Clean	F-Prot	Clean
Jiangmin	Clean	K7AntiVirus	Clean
K7GW	Clean	Kaspersky	Clean
Kingsoft	Clean	Malwarebytes	Clean
Palo Alto Networks	Clean	Panda	Clean
SentinelOne	Clean	Sophos AV	Clean
SUPERAntiSpyware	Clean	TACHYON	Clean
Tencent	Clean	Trapmine	Clean
Trustlook	Clean	VBA32	Clean
ViRobot	Clean	ZoneAlarm	Clean
Zoner	Clean	Cybereason	Unable to process file type
Symantec Mobile Insight	Unable to process file type		

VirusTotal

Contact Us

How It Works

Terms of Service

Privacy Policy

Join Us

Community

Join Community

Vote and Comment

Contributors

Top Users

Latest Comments

Blog

Tools

API Scripts

YARA

Desktop Apps

Browser Extensions

Mobile App

Premium Services

Documentation

Get Started

Searching

Reports

API

Use Cases

English (US)

This is the result for Lab01-01.exe

32 / 67

SHA-256

f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba

File name

Lab01-01.dll

File size

160 KB

Last analysis

2019-02-15 13:19:18 UTC

Community score

-143

32 engines detected this file

Detection

Details

Relations

Community

Acronis	suspicious	AegisLab	Trojan.Win32.Generic.4!c
ALYac	Trojan.Agent.Waski	Antiy-AVL	Trojan/Win32.BTSGeneric
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/Dldr:Waski.163840.1	CAT-QuickHeal	Trojan.IGENERIC
ClamAV	Win.Malware.Agent-6369668-0	Comodo	Malware@#2dsw4albnce61
Cylance	Unsafe	Cyren	W32/Trojan.PXBS-7022
Endgame	malicious (high confidence)	ESET-NOD32	a variant of Generic.TGEWDD
F-Secure	Trojan.TR/Dldr:Waski.163840.1	Fortinet	PossibleThreat
GData	Win32:Trojan.Agent.4L5OBS	Ikarus	Trojan.SuspectCRC
McAfee	GenericRXFO-RT1290934C61DE9	McAfee-GW-Edition	GenericRXFO-RT1290934C61DE9
Microsoft	Trojan:Win32/Occamy.C	NANO-Antivirus	Trojan.Win32.Waski.dtkvsp
Qihoo-360	Win32/Trojan.54f	Rising	Trojan.Tilken!8.F605 (CLOUD)
Sophos ML	heuristic	Symantec	Trojan.Gen.2
TheHacker	Trojan/Generic.TGEWDD	TrendMicro-HouseCall	TROJ_GEN.R002C0PLO18
VIPRE	Trojan.Win32.Generic!BT	Webroot	W32.Gen.BT
Yandex	Trojan.Agent!//H5KjKET4	Zillya	Adware.InstallCore.Win32.1036
Ad-Aware	Clean	AhnLab-V3	Clean
Alibaba	Clean	Arcabit	Clean
Avast Mobile Security	Clean	Babable	Clean
Baidu	Clean	BitDefender	Clean
Bkav	Clean	CMC	Clean
CrowdStrike Falcon	Clean	DrWeb	Clean
eGambit	Clean	Emsisoft	Clean
eScan	Clean	F-Prot	Clean
Jiangmin	Clean	K7AntiVirus	Clean
K7GW	Clean	Kaspersky	Clean
Kingsoft	Clean	Malwarebytes	Clean
Palo Alto Networks	Clean	Panda	Clean
SentinelOne	Clean	Sophos AV	Clean
SUPERAntiSpyware	Clean	TACHYON	Clean
Tencent	Clean	Trapmine	Clean
Trustlook	Clean	VBA32	Clean
ViRobot	Clean	ZoneAlarm	Clean
Zoner	Clean	Cybereason	Unable to process file type
Symantec Mobile Insight	Unable to process file type		

VirusTotal

Contact Us

How It Works

Terms of Service

Privacy Policy

Join Us

Community

Join Community

Vote and Comment

Contributors

Top Users

Latest Comments

Blog

Tools

API Scripts

YARA

Desktop Apps

Browser Extensions

Mobile App

Premium Services

Documentation

Get Started

Searching

Reports

API

Use Cases

English (US)

Yes, both of the files match the existing antivirus signatures.

## 2

### Lab01-01.exe

#### Portable Executable Info ⓘ

##### Header

Target Machine Intel 386 or later processors and compatible processors  
Compilation Timestamp 2010-12-19 16:16:38  
Entry Point 4858  
Contained Sections 4

##### Sections

Name	Virtual Address	Virtual Size	Raw Size	Entropy	MD5
.text	4096	926	4096	1.9	65d3ddf9778db8d01e57b5825fbd93ad
.rdata	8192	147398	147456	0.03	530532a38a38ea1219e691b8f16d10e9
.data	155648	108	4096	0.11	0211086333be22ae2620b568fde46fe3
.reloc	159744	516	4096	0.26	a082f3572d17cd40272b3bcfd96b7b2d

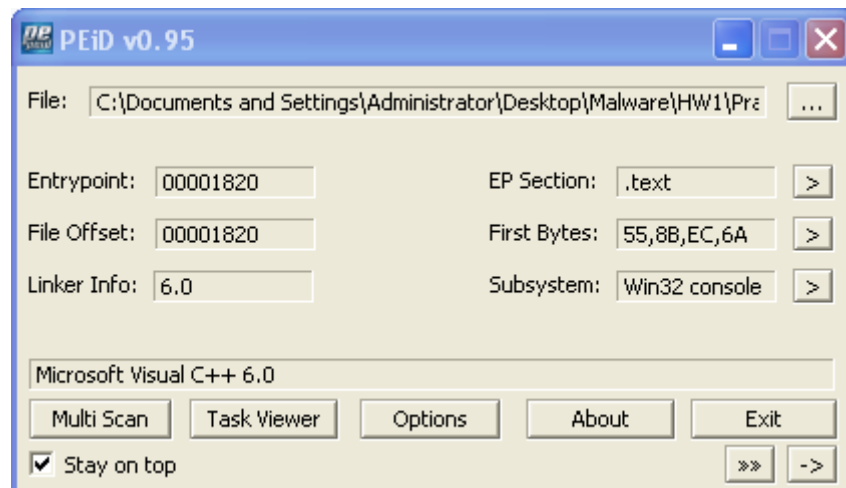
##### Imports

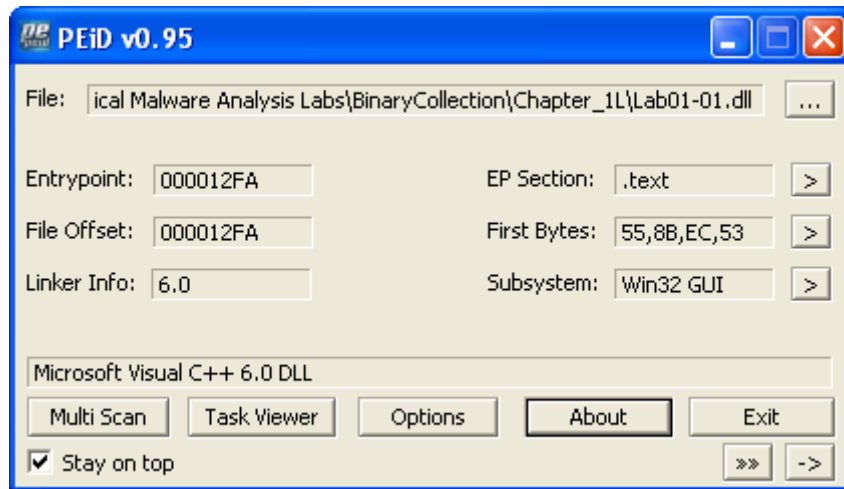
+ KERNEL32.dll  
+ MSVCRT.dll  
+ WS2\_32.dll

As is shown in the above attached figure, these files were compiled on 2010-12-19.

## 3

We used the PEiD to analyze the file. Here are the results:





From the pictures above, we can see Microsoft Visual C++ was the compiler. It also indicates that the subsystem is Win32 GUI which means the malware had a GUI before. However, there are no indicators showing these files has been packed or obfuscated.

## 4

The imports of Lab01-01.exe contain:

```
CreateFileA
FindNextFileA
FindFirstFileA
CopyFileA
```

According to these imports, this malware might want to search for a specific file and copy it.

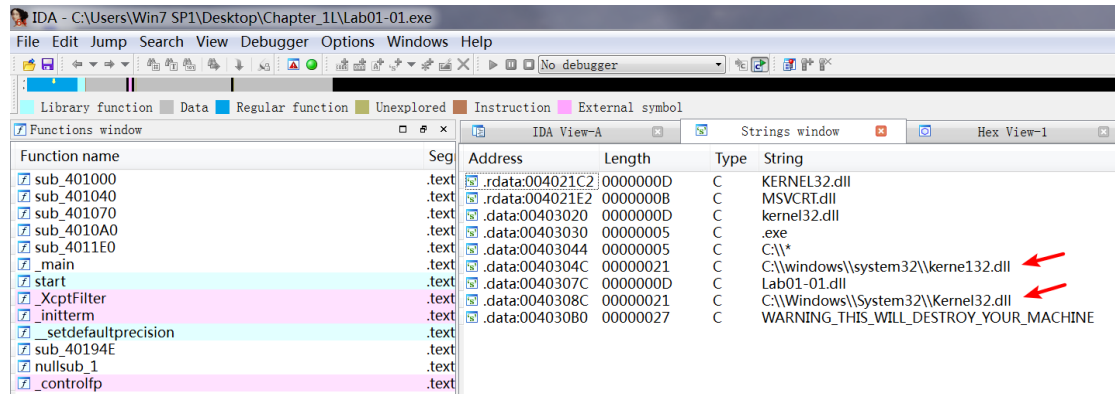
The imports of Lab01-01.dll contain:

```
Sleep
CreateProcessA
CreateMutexA
OpenMutexA
CloseHandle
socket
inet_addr
connect
send
recv
closesocket
```

According to these imports, the malware might want to communicate with a specific server since there is some import about socket connections.

## 5

Examine C:\Windows\System32\kerne132.dll for additional malicious activity. Note that the file kerne132.dll, with the number 1 instead of the letter l, is meant to look like the system file kernel32.dll. This file can be used as a host indicator to search for the malware.



## 6

The .dll file contains a reference to local IP address 127.26.152.13. Network activity to 127.26.152.13 would be a network-based indicator of the malware being present on a system.

## 7

Based on all the information above, we think the .dll file probably contains a backdoor and the .exe file is executable to install and run the dll file.

