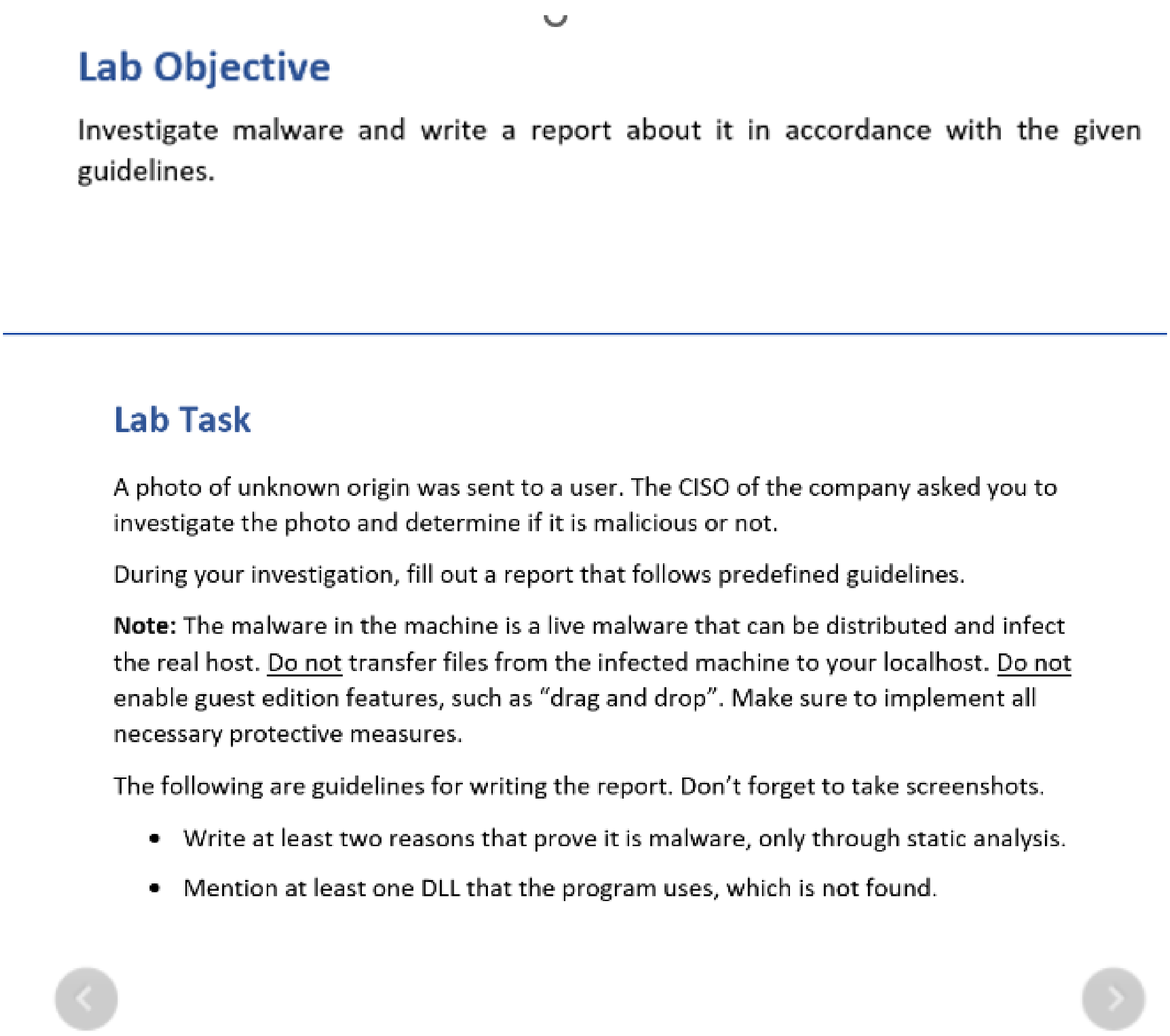
TrickySnowStorm

SIEM & SOC FINAL PROJECT

Part 2



Lab Objective

Investigate malware and write a report about it in accordance with the given guidelines.

Lab Task

A photo of unknown origin was sent to a user. The CISO of the company asked you to investigate the photo and determine if it is malicious or not.

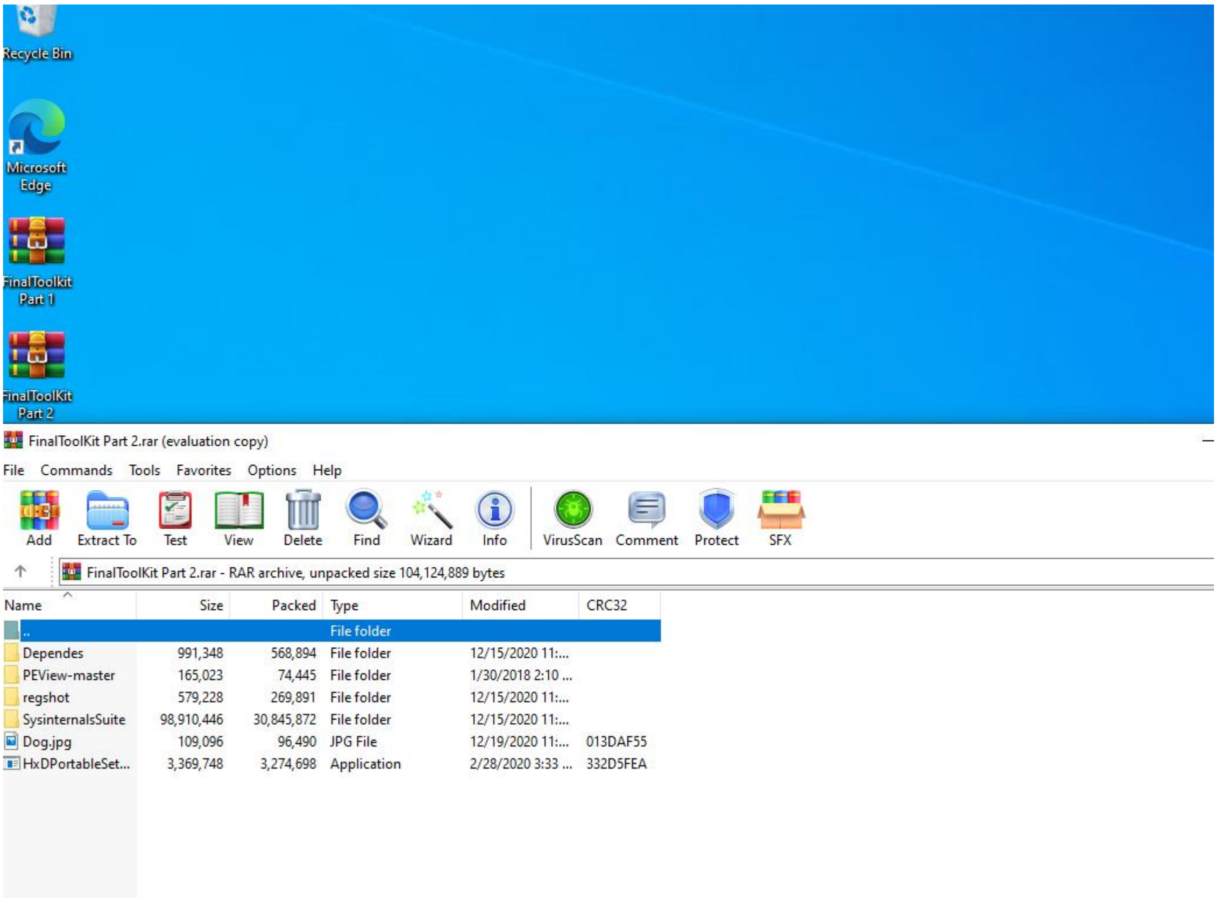
During your investigation, fill out a report that follows predefined guidelines.

Note: The malware in the machine is a live malware that can be distributed and infect the real host. Do not transfer files from the infected machine to your localhost. Do not enable guest edition features, such as "drag and drop". Make sure to implement all necessary protective measures.

The following are guidelines for writing the report. Don't forget to take screenshots.

- Write at least two reasons that prove it is malware, only through static analysis.
- Mention at least one DLL that the program uses, which is not found.

In part 2. we have got dedicated Winrar package “Final ToolKit Part2” . We can find there files and folders. Among them, dog.jpg file is found. I assume, it’s a photo, mentioned in final project, to investigate.



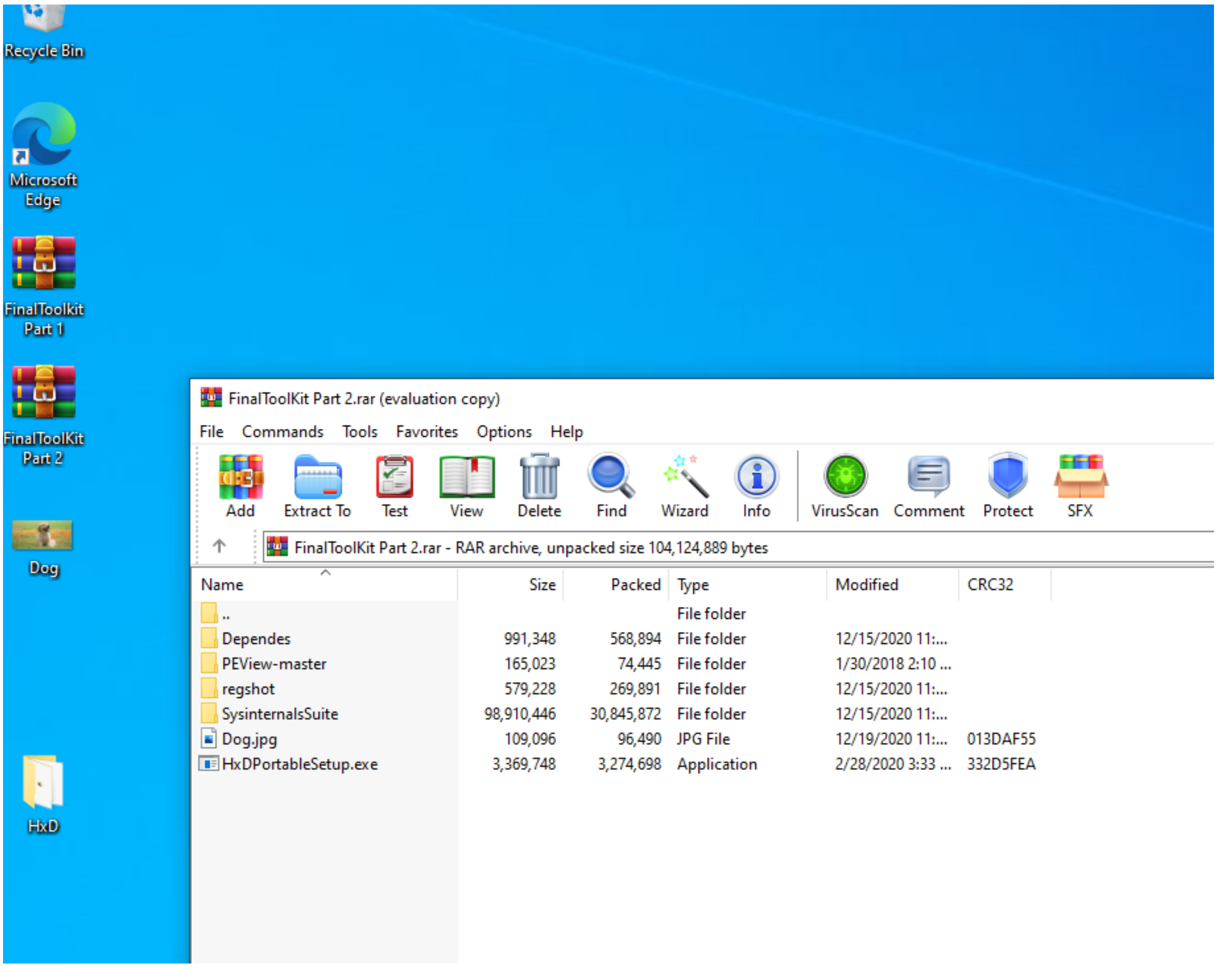
FinalToolKit Part 2.rar (evaluation copy)

FinalToolKit Part 2.rar - RAR archive, unpacked size 104,124,889 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Dependes	991,348	568,894	File folder	12/15/2020 11:...	
PEView-master	165,023	74,445	File folder	1/30/2018 2:10 ...	
regshot	579,228	269,891	File folder	12/15/2020 11:...	
SysinternalsSuite	98,910,446	30,845,872	File folder	12/15/2020 11:...	
Dog.jpg	109,096	96,490	JPG File	12/19/2020 11:...	013DAF55
HxDPortableSet...	3,369,748	3,274,698	Application	2/28/2020 3:33 ...	332D5FEA

Screenshot 1. Winrar package "Final ToolKit Part2"

To make work easier, I moved dog.jpg file on the Desktop. We can see the file as a thumbnail of a nice photo.


Recycle Bin
Microsoft Edge
FinalToolkit Part 1
FinalToolKit Part 2
Dog
HxD
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment Protect SFX

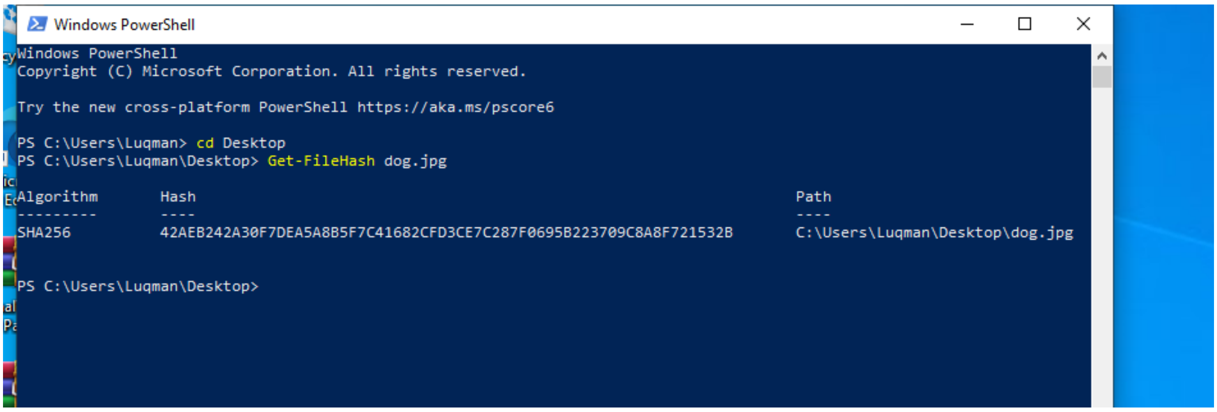
FinalToolKit Part 2.rar (evaluation copy)

FinalToolKit Part 2.rar - RAR archive, unpacked size 104,124,889 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Dependes	991,348	568,894	File folder	12/15/2020 11:...	
PEView-master	165,023	74,445	File folder	1/30/2018 2:10 ...	
regshot	579,228	269,891	File folder	12/15/2020 11:...	
SysinternalsSuite	98,910,446	30,845,872	File folder	12/15/2020 11:...	
Dog.jpg	109,096	96,490	JPG File	12/19/2020 11:...	013DAF55
HxDPortableSetup.exe	3,369,748	3,274,698	Application	2/28/2020 3:33 ...	332D5FEA

Screenshot 2. File dog.jpg on the Desktop.

Now it’s time to dive in. Let’s investigate the photo and check if it’s malicious or not. But first find out what the hash of dog.jpg file is (it would be easier to identification):


Windows PowerShell

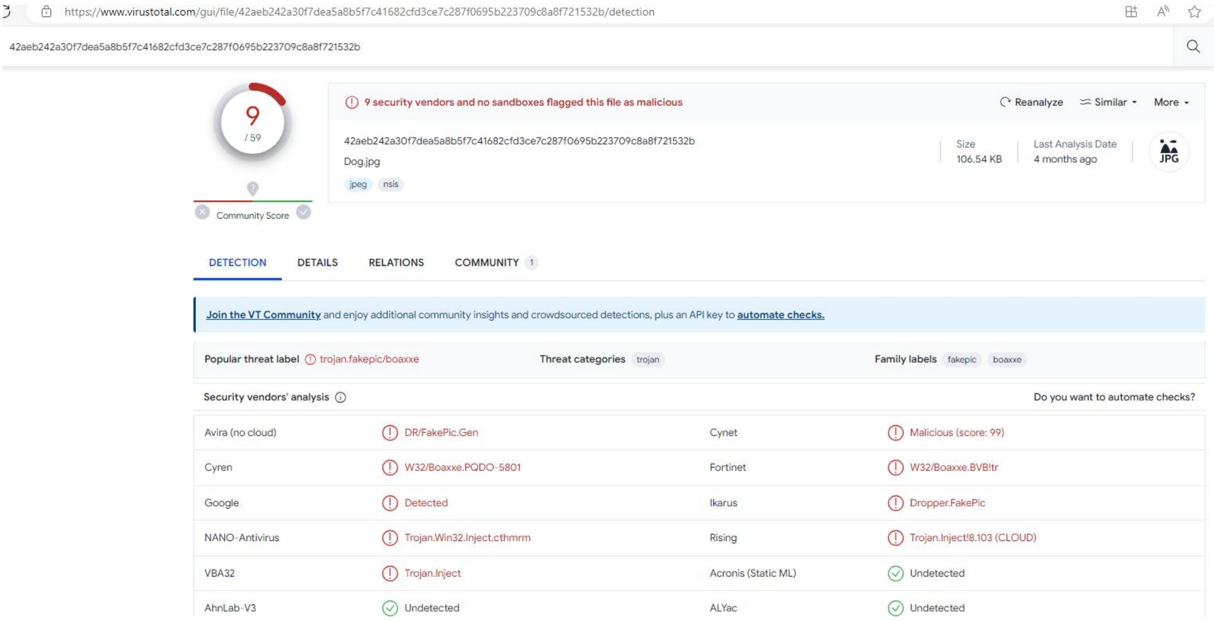
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Luqman> cd Desktop
PS C:\Users\Luqman\Desktop> Get-FileHash dog.jpg

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          42AEB242A30F7DEA5A8B5F7C41682CFD3CE7C287F0695B223709C8A8F721532B       C:\Users\Luqman\Desktop\dog.jpg


PS C:\Users\Luqman\Desktop>
```

Screenshot 3. HashSHA256 of dog.jpg

A. Let’s check what virustotal tell us about them:

.

WARNING!!! dog.jpg is a threat, category: trojan.



https://www.virustotal.com/gui/file/42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c8a8f721532b/detection

42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c8a8f721532b

9 / 59

Community Score

9 security vendors and no sandboxes flagged this file as malicious

42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c8a8f721532b

Dog.jpg

jpeg nsis

Size 106.54 KB

Last Analysis Date 4 months ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.fakepic/boaxxe

Threat categories trojan

Family labels fakepic boaxxe

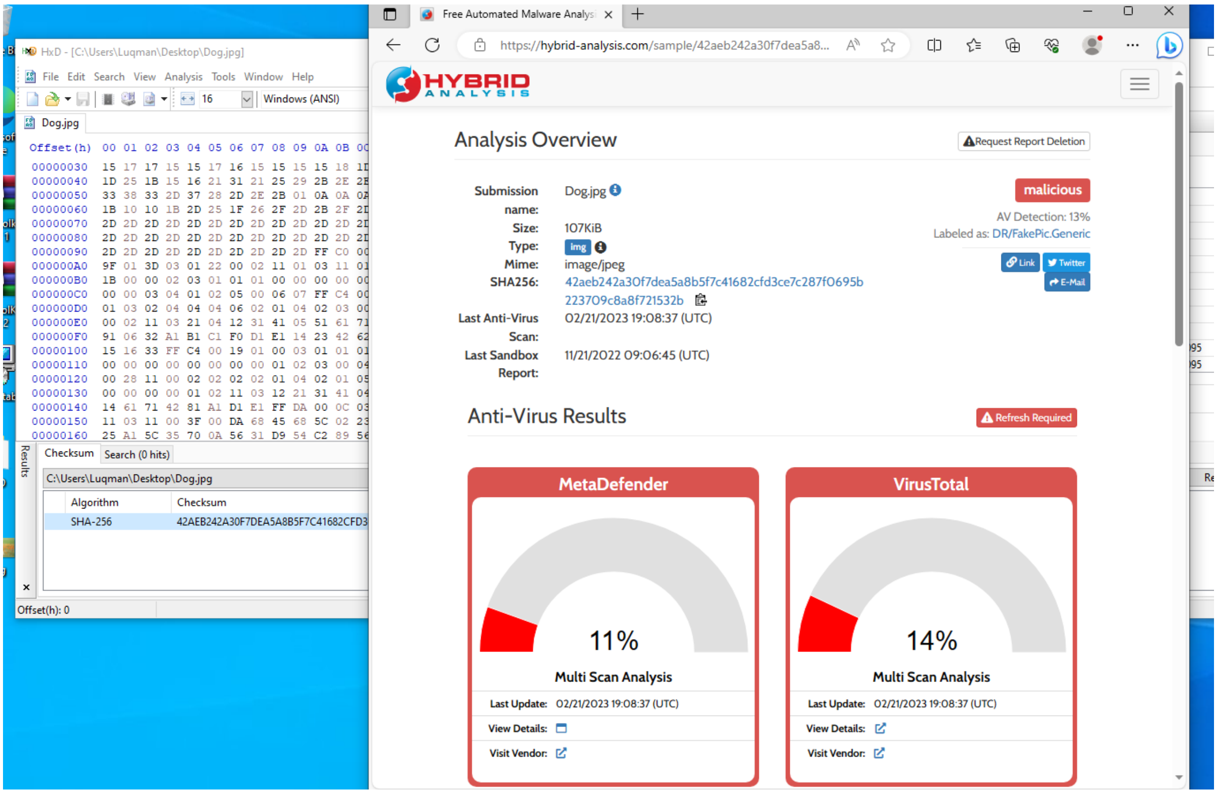
Security vendors' analysis

Do you want to automate checks?

Avira (no cloud)	DR/FakePic.Gen	Cynet	Malicious (score: 99)
Cyren	W32/Boaxxe.PQDO-5801	Fortinet	W32/Boaxxe.BVB!tr
Google	Detected	Ikarus	Dropper.FakePic
NANO-Antivirus	Trojan.Win32.Inject.cthmrm	Rising	Trojan.Inject!8.103 (CLOUD)
VBA32	Trojan.Inject	Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected	ALYac	✓ Undetected

Screenshot 4. Virus total about dog.jpg

B. Hybrid Analysis website: marked it as malicious



HxD - [C:\Users\Luqman\Desktop\Dog.jpg]

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C
00000030  15 17 17 15 15 17 16 15 15 15 15 18 1D
00000040  1D 25 1B 15 16 21 31 21 25 29 2B 2E 2E
00000050  33 38 33 2D 37 28 2D 2E 2B 01 0A 0A 0A
00000060  1B 10 10 1B 2D 25 1F 26 2F 2D 2B 2F 2D
00000070  2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D
00000080  2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D 2D
00000090  2D 2D 2D 2D 2D 2D 2D 2D 2D 2D FF C0 00
000000A0  9F 01 3D 03 01 22 00 02 11 01 03 11 01
000000B0  1B 00 00 02 03 01 01 01 00 00 00 00 00
000000C0  00 00 03 04 01 02 05 00 06 07 FF C4 00
000000D0  01 03 02 04 04 04 06 02 01 04 02 03 00
000000E0  00 02 11 03 21 04 12 31 41 05 51 61 71
000000F0  91 06 32 A1 B1 C1 F0 D1 E1 14 23 42 62
00000100  15 16 33 FF C4 00 19 01 00 03 01 01 01
00000110  00 00 00 00 00 00 00 00 01 02 03 00 04
00000120  00 28 11 00 02 02 02 02 01 04 02 01 05
00000130  00 00 00 00 01 02 11 03 12 21 31 41 04
00000140  14 61 71 42 81 A1 D1 E1 FF DA 00 0C 03
00000150  11 03 11 00 3F 00 DA 68 45 68 5C 02 23
00000160  25 A1 5C 35 70 0A 56 31 D9 54 C2 89 56
```

Checksum | Search (0 hits)

C:\Users\Luqman\Desktop\Dog.jpg

Algorithm	Checksum
SHA-256	42AEB242A30F7DEA5A8B5F7C41682CFD3

Offset(h): 0

Free Automated Malware Analys

https://hybrid-analysis.com/sample/42aeb242a30f7dea5a8...

Analysis Overview

Request Report Deletion

Submission name:	Dog.jpg
Size:	107KiB
Type:	img
Mime:	image/jpeg
SHA256:	42aeb242a30f7dea5a8b5f7c41682cfd3ce7c287f0695b223709c8a8f721532b
Last Anti-Virus Scan:	02/21/2023 19:08:37 (UTC)
Last Sandbox Report:	11/21/2022 09:06:45 (UTC)

malicious

AV Detection: 13%

Labeled as: DR/FakePic.Generic

Anti-Virus Results

Refresh Required

MetaDefender

11%

Multi Scan Analysis

Last Update: 02/21/2023 19:08:37 (UTC)

View Details:

Visit Vendor:

VirusTotal

14%

Multi Scan Analysis

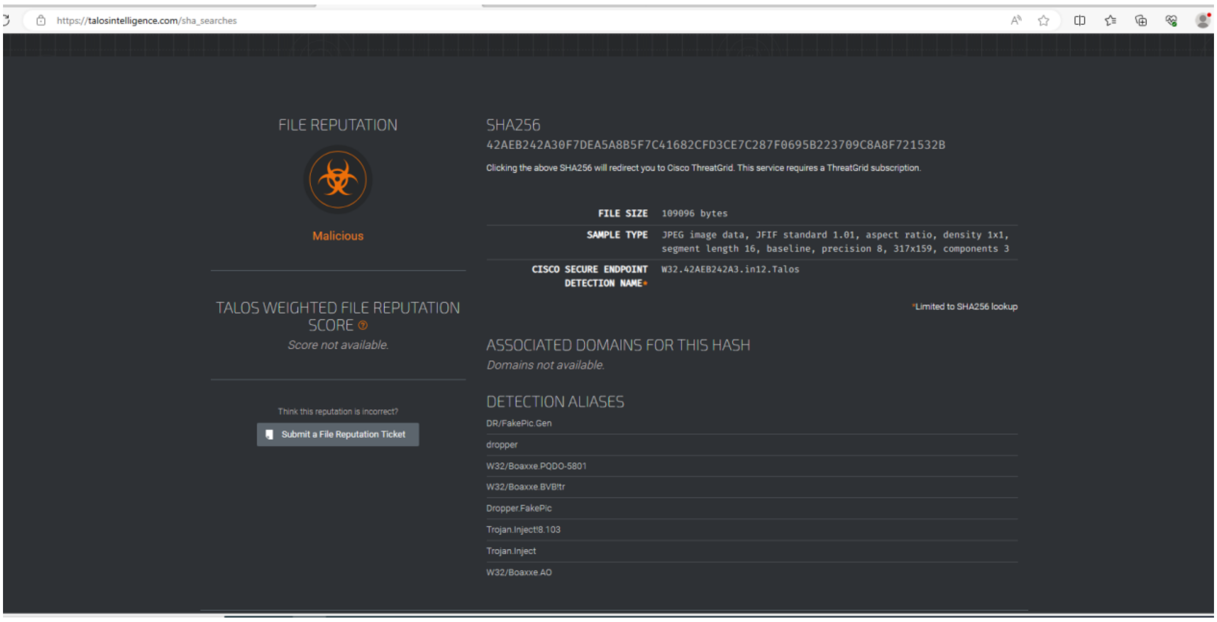
Last Update: 02/21/2023 19:08:37 (UTC)

View Details:

Visit Vendor:

Screenshot 5. Hybrid analysis website about dog.jpg.

C. Talosintelligence.com -> marked it as trojan



https://talosintelligence.com/sha_searches

FILE REPUTATION

Malicious

TALOS WEIGHTED FILE REPUTATION SCORE

Score not available.

Think this reputation is incorrect?

Submit a File Reputation Ticket

SHA256

42AEB242A30F7DEA5A8B5F7C41682CFD3CE7C287F0695B223709C8A8F721532B

Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.

FILE SIZE	109096 bytes
SAMPLE TYPE	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 317x159, components 3
CISCO SECURE ENDPOINT DETECTION NAME*	W32.42AEB242A3.in12.Talos

*Limited to SHA256 lookup

ASSOCIATED DOMAINS FOR THIS HASH

Domains not available.

DETECTION ALIASES

DR/FakePic.Gen

dropper

W32/Boaxxe.PQDO-5801

W32/Boaxxe.BVB!tr

Dropper.FakePic

Trojan.Inject!8.103

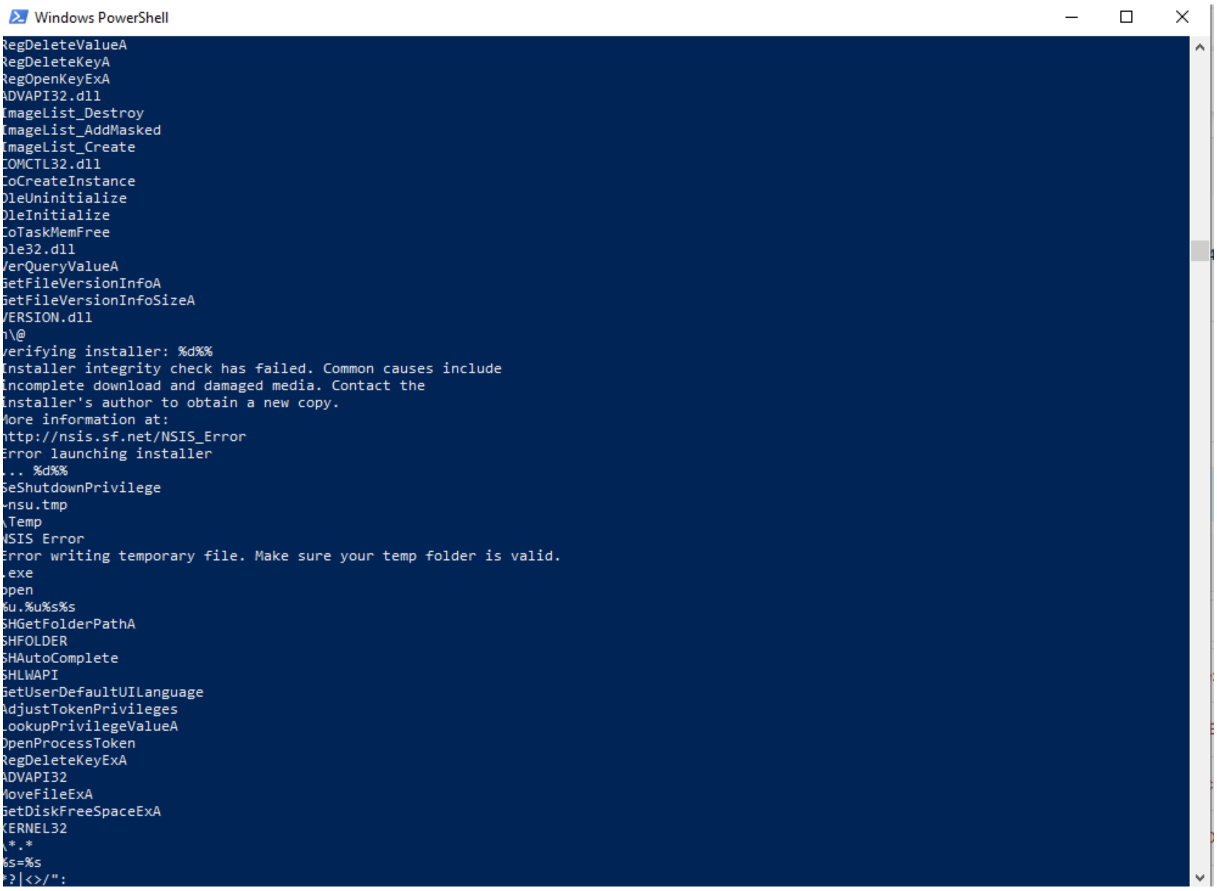
Trojan.Inject

W32/Boaxxe.AO

Screenshot 6. Talos Intelligence website about dog.jpg.

D. Strings:

Very interesting things were found (http, open process token etc.) -> point to a malicious file.

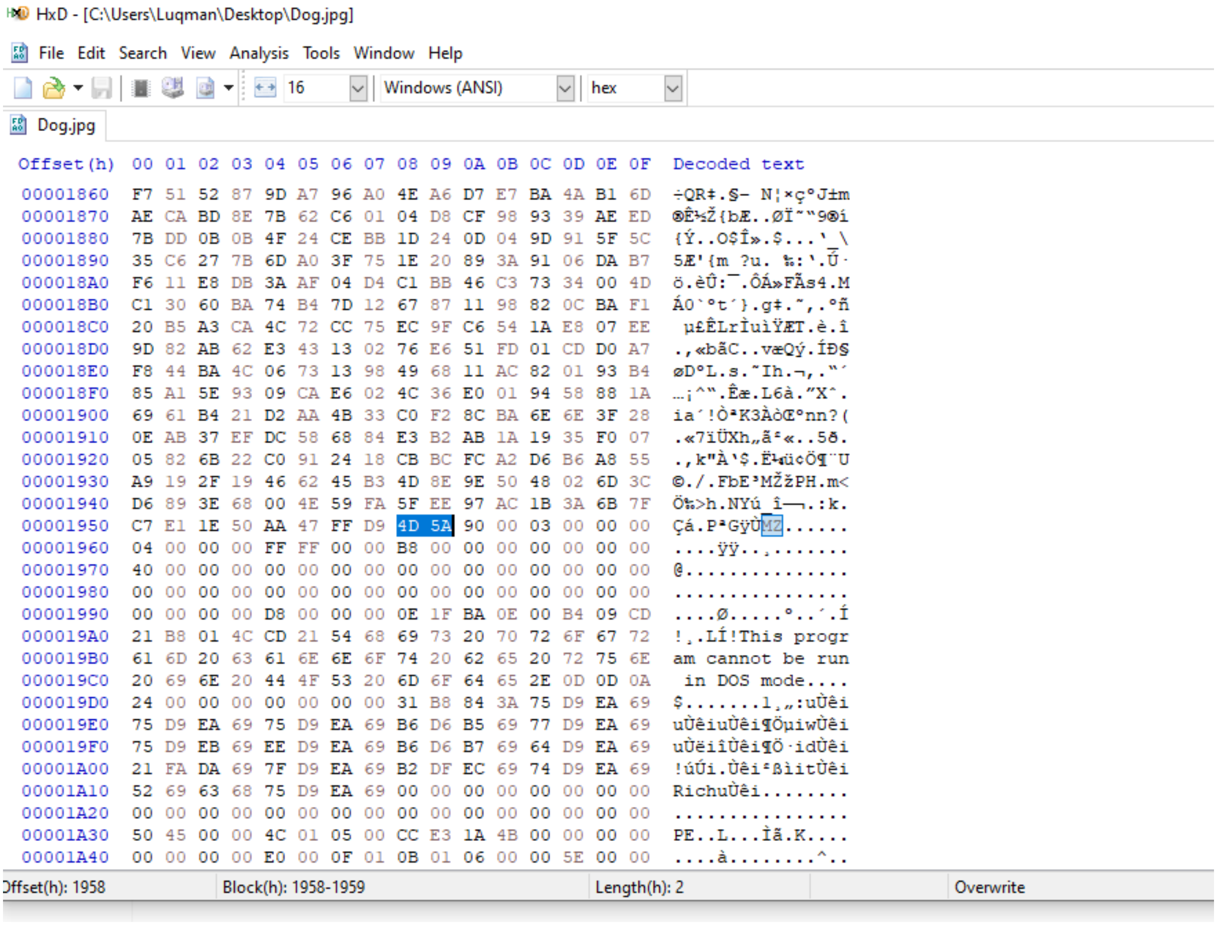


```
RegDeleteValueA
RegDeleteKeyA
RegOpenKeyExA
ADVAPI32.dll
ImageList_Destroy
ImageList_AddMasked
ImageList_Create
COMCTL32.dll
CoCreateInstance
OleUninitialize
OleInitialize
CoTaskMemFree
ole32.dll
VerQueryValueA
GetFileVersionInfoA
GetFileVersionInfoSizeA
VERSION.dll
n\@
verifying installer: %d%%
Installer integrity check has failed. Common causes include
incomplete download and damaged media. Contact the
installer's author to obtain a new copy.
More information at:
http://nsis.sf.net/NSIS_Error
Error launching installer
... %d%%
SeShutdownPrivilege
~nsu.tmp
\Temp
NSIS Error
Error writing temporary file. Make sure your temp folder is valid.
.exe
open
%u.%u%s%s
SHGetFolderPathA
SHFOLDER
SHAutoComplete
SHLWAPI
GetUserDefaultUILanguage
AdjustTokenPrivileges
LookupPrivilegeValueA
OpenProcessToken
RegDeleteKeyExA
ADVAPI32
MoveFileExA
GetDiskFreeSpaceExA
KERNEL32
\*.*
%s=%s
*?|<>/":
```

Screenshot 7. Strings analysis

E. Hex Editor – looking for magic bytes

“4D 5A” were found -> it means it is not a .jpg file. It’s .exe file (portable executable).
“50 45 00 00” -> also are there -> point to an .exe file

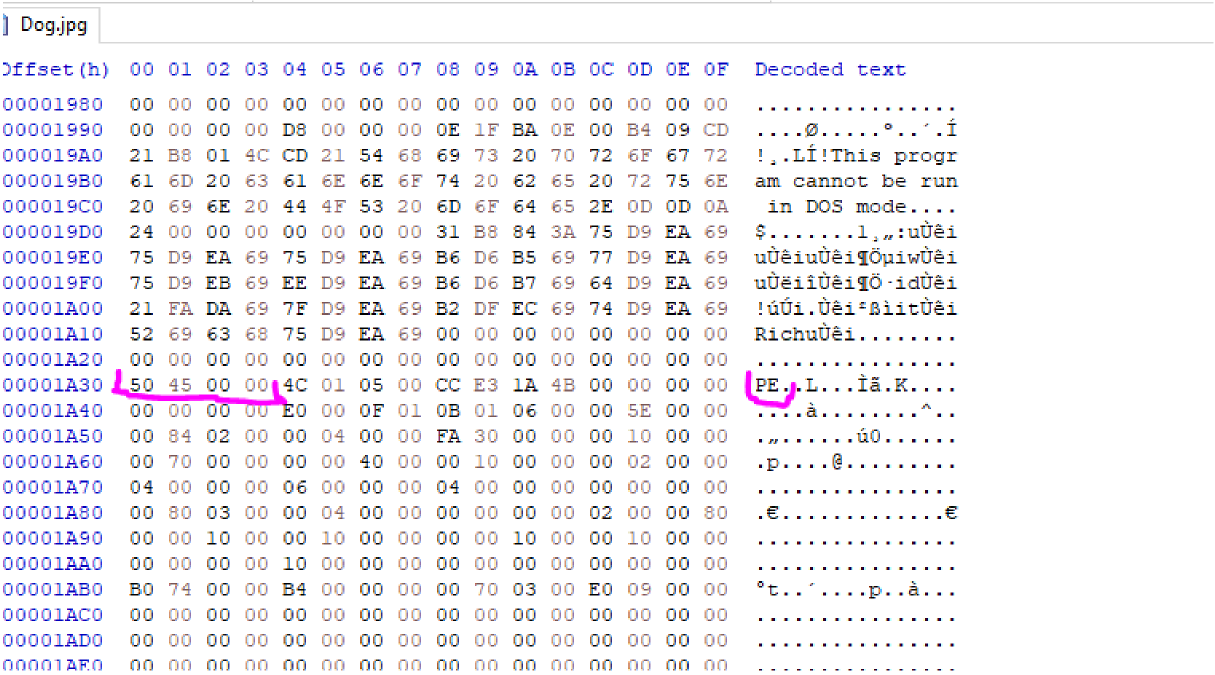


HxD - [C:\Users\Luqman\Desktop\Dog.jpg]

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00001860  F7 51 52 87 9D A7 96 A0 4E A6 D7 E7 BA 4A B1 6D  ÷QR‡.§– N¦×ç°J±m
00001870  AE CA BD 8E 7B 62 C6 01 04 D8 CF 98 93 39 AE ED  ®Ê½Ž{bÆ..ØÏ˜“9®í
00001880  7B DD 0B 0B 4F 24 CE BB 1D 24 0D 04 9D 91 5F 5C  {Ý..O$Î».$...‘_\
00001890  35 C6 27 7B 6D A0 3F 75 1E 20 89 3A 91 06 DA B7  5Æ'{m ?u. ‰:‘.Ú·
000018A0  F6 11 E8 DB 3A AF 04 D4 C1 BB 46 C3 73 34 00 4D  ö.èÛ:¯.ÔÁ»FÃs4.M
000018B0  C1 30 60 BA 74 B4 7D 12 67 87 11 98 82 0C BA F1  Á0`ºt´}.g‡.˜‚.ºñ
000018C0  20 B5 A3 CA 4C 72 CC 75 EC 9F C6 54 1A E8 07 EE   µ£ÊLrÌuìŸÆT.è.î
000018D0  9D 82 AB 62 E3 43 13 02 76 E6 51 FD 01 CD D0 A7  .‚«bãC..væQý.ÍÐ§
000018E0  F8 44 BA 4C 06 73 13 98 49 68 11 AC 82 01 93 B4  øDºL.s.˜Ih.¬‚.“´
000018F0  85 A1 5E 93 09 CA E6 02 4C 36 E0 01 94 58 88 1A  …¡^“.Êæ.L6à.”Xˆ.
00001900  69 61 B4 21 D2 AA 4B 33 C0 F2 8C BA 6E 6E 3F 28  ia´!ÒªK3ÀòŒºnn?(
00001910  0E AB 37 EF DC 58 68 84 E3 B2 AB 1A 19 35 F0 07  .«7ïÜXh„ã²«..5ð.
00001920  05 82 6B 22 C0 91 24 18 CB BC FC A2 D6 B6 A8 55  .‚k"À‘$.Ë¼ü¢Ö¶¨U
00001930  A9 19 2F 19 46 62 45 B3 4D 8E 9E 50 48 02 6D 3C  ©./.FbE³MŽžPH.m<
00001940  D6 89 3E 68 00 4E 59 FA 5F EE 97 AC 1B 3A 6B 7F  Ö‰>h.NYú_î—¬.:k.
00001950  C7 E1 1E 50 AA 47 FF D9 4D 5A 90 00 03 00 00 00  Çá.PªGÿÙMZ......
00001960  04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00  ....ÿÿ..¸.......
00001970  40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  @...............
00001980  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001990  00 00 00 00 D8 00 00 00 0E 1F BA 0E 00 B4 09 CD  ....Ø.....º..´.Í
000019A0  21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72  !¸.LÍ!This progr
000019B0  61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E  am cannot be run
000019C0  20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A   in DOS mode....
000019D0  24 00 00 00 00 00 00 00 31 B8 84 3A 75 D9 EA 69  $.......1¸„:uÙêi
000019E0  75 D9 EA 69 75 D9 EA 69 B6 D6 B5 69 77 D9 EA 69  uÙêiuÙêi¶ÖµiwÙêi
000019F0  75 D9 EB 69 EE D9 EA 69 B6 D6 B7 69 64 D9 EA 69  uÙëiîÙêi¶Ö·idÙêi
00001A00  21 FA DA 69 7F D9 EA 69 B2 DF EC 69 74 D9 EA 69  !úÚi.Ùêi²ßìitÙêi
00001A10  52 69 63 68 75 D9 EA 69 00 00 00 00 00 00 00 00  RichuÙêi........
00001A20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001A30  50 45 00 00 4C 01 05 00 CC E3 1A 4B 00 00 00 00  PE..L...Ìã.K....
00001A40  00 00 00 00 E0 00 0F 01 0B 01 06 00 00 5E 00 00  ....à........^..
```

Offset(h): 1958 Block(h): 1958-1959 Length(h): 2 Overwrite

Screenshot 8. Magic bytes “4D 5A”.

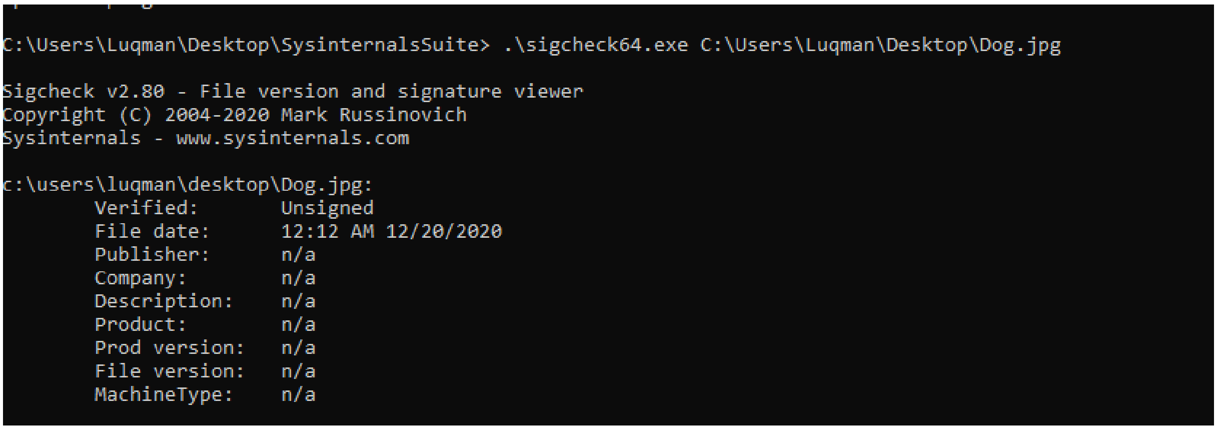


```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00001980  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001990  00 00 00 00 D8 00 00 00 0E 1F BA 0E 00 B4 09 CD  ....Ø.....º..´.Í
000019A0  21 B8 01 4C CD 21 54 68 69 73 20 70 72 6F 67 72  !¸.LÍ!This progr
000019B0  61 6D 20 63 61 6E 6E 6F 74 20 62 65 20 72 75 6E  am cannot be run
000019C0  20 69 6E 20 44 4F 53 20 6D 6F 64 65 2E 0D 0D 0A   in DOS mode....
000019D0  24 00 00 00 00 00 00 00 31 B8 84 3A 75 D9 EA 69  $.......1¸„:uÙêi
000019E0  75 D9 EA 69 75 D9 EA 69 B6 D6 B5 69 77 D9 EA 69  uÙêiuÙêi¶ÖµiwÙêi
000019F0  75 D9 EB 69 EE D9 EA 69 B6 D6 B7 69 64 D9 EA 69  uÙëiîÙêi¶Ö·idÙêi
00001A00  21 FA DA 69 7F D9 EA 69 B2 DF EC 69 74 D9 EA 69  !úÚi.Ùêi²ßìitÙêi
00001A10  52 69 63 68 75 D9 EA 69 00 00 00 00 00 00 00 00  RichuÙêi........
00001A20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001A30  50 45 00 00 4C 01 05 00 CC E3 1A 4B 00 00 00 00  PE..L...Ìã.K....
00001A40  00 00 00 00 E0 00 0F 01 0B 01 06 00 00 5E 00 00  ....à........^..
00001A50  00 84 02 00 00 04 00 00 FA 30 00 00 00 10 00 00  .„......ú0......
00001A60  00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00  .p....@.........
00001A70  04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00  ................
00001A80  00 80 03 00 00 04 00 00 00 00 00 00 02 00 00 80  .€.............€
00001A90  00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00  ................
00001AA0  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00  ................
00001AB0  B0 74 00 00 B4 00 00 00 00 70 03 00 E0 09 00 00  °t..´....p..à...
00001AC0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001AD0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00001AE0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Screenshot 9. “50 45 00 00” found

F. Sigcheck analysis

There is no verified signature and it’s suspicious because legal software are signed.



```
C:\Users\Luqman\Desktop\SysinternalsSuite> .\sigcheck64.exe C:\Users\Luqman\Desktop\Dog.jpg

Sigcheck v2.80 - File version and signature viewer
Copyright (C) 2004-2020 Mark Russinovich
Sysinternals - www.sysinternals.com

c:\users\luqman\desktop\Dog.jpg:
        Verified:       Unsigned
        File date:      12:12 AM 12/20/2020
        Publisher:      n/a
        Company:        n/a
        Description:    n/a
        Product:        n/a
        Prod version:   n/a
        File version:   n/a
        MachineType:    n/a
```

Screenshot 10. Looking for verified signature.

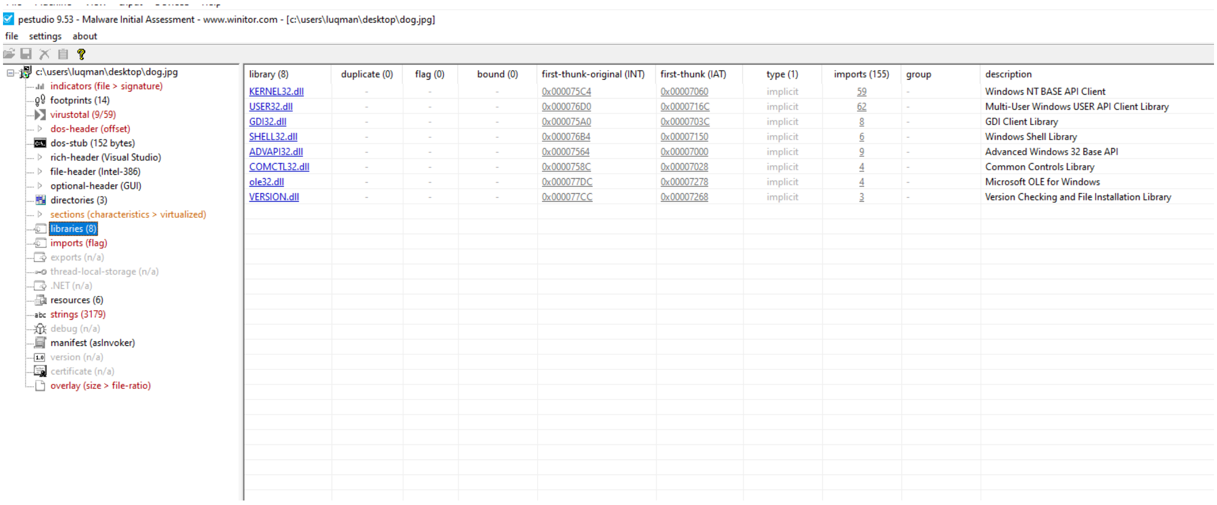
Summary:

Using some static analysis tools, mentioned above, I can admit, dog.jpg file is a malicious file. I’ve checked few independent website sources, examined the file directly and everything has indicated that it is not nice dog picture but a real threat.

Now let's go to another part of our job and check if there are any dlls that program uses and they are not found?

I wasn’t quite sure how to understand this part of task, so I did it into two ways:

a) I’ve examined the file using PEstudio (I had downloaded it). On the screenshot below are listed libraries used by dog.jpg (libraries can be seen also via Hex Editor).

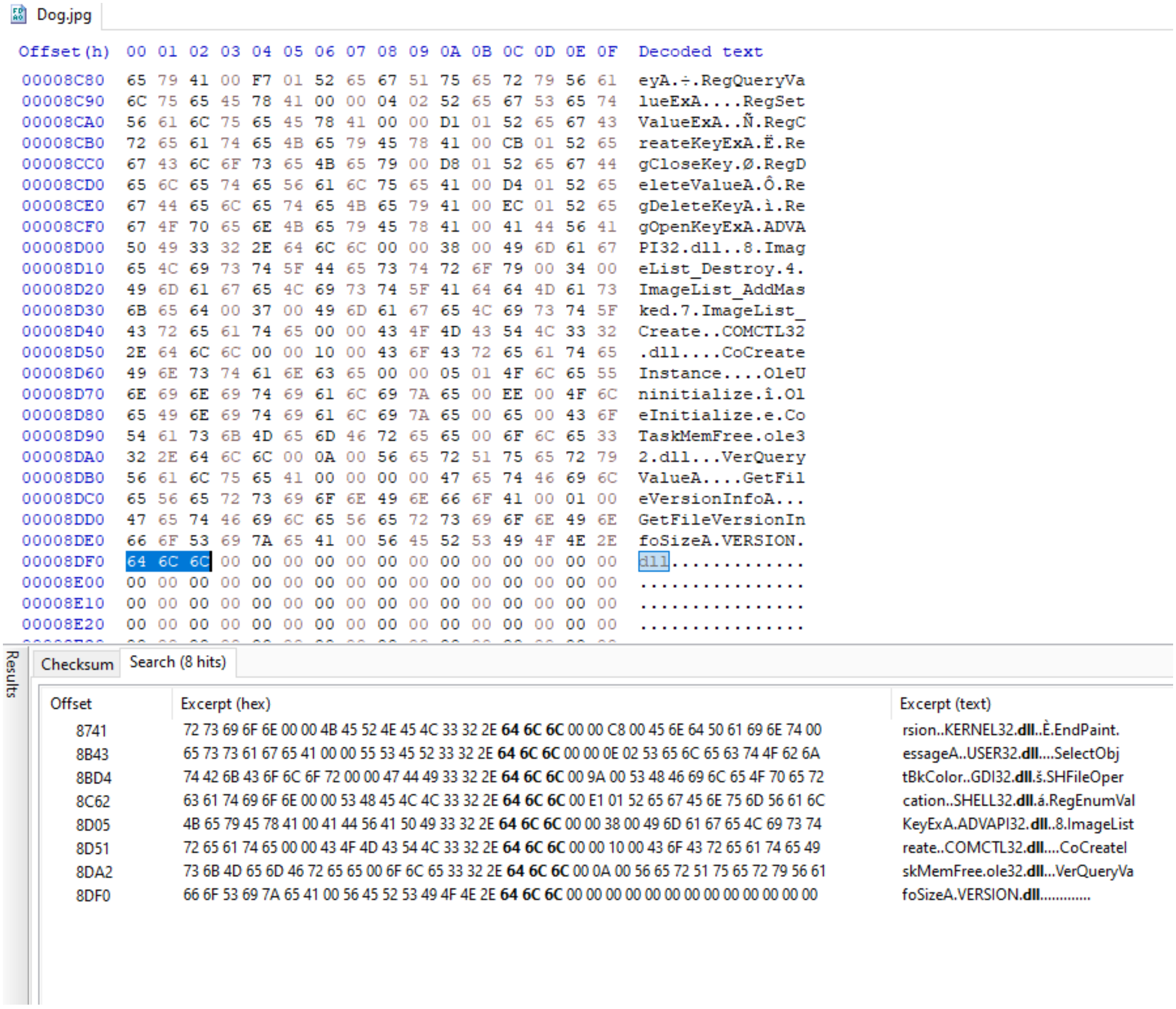


pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\luqman\desktop\dog.jpg]

```
c:\users\luqman\desktop\dog.jpg
  indicators (file > signature)
  footprints (14)
  virustotal (9/59)
  dos-header (offset)
  dos-stub (152 bytes)
  rich-header (Visual Studio)
  file-header (Intel-386)
  optional-header (GUI)
  directories (3)
  sections (characteristics > virtualized)
  libraries (8)
  imports (flag)
  exports (n/a)
  thread-local-storage (n/a)
  .NET (n/a)
  resources (6)
  strings (3179)
  debug (n/a)
  manifest (asInvoker)
  version (n/a)
  certificate (n/a)
  overlay (size > file-ratio)
```

library (8)	duplicate (0)	flag (0)	bound (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (155)	group	description
KERNEL32.dll	-	-	-	0x000075C4	0x00007060	implicit	59	-	Windows NT BASE API Client
USER32.dll	-	-	-	0x000076D0	0x0000716C	implicit	62	-	Multi-User Windows USER API Client Library
GDI32.dll	-	-	-	0x000075A0	0x0000703C	implicit	8	-	GDI Client Library
SHELL32.dll	-	-	-	0x000076B4	0x00007150	implicit	6	-	Windows Shell Library
ADVAPI32.dll	-	-	-	0x00007564	0x00007000	implicit	9	-	Advanced Windows 32 Base API
COMCTL32.dll	-	-	-	0x0000758C	0x00007028	implicit	4	-	Common Controls Library
ole32.dll	-	-	-	0x000077DC	0x00007278	implicit	4	-	Microsoft OLE for Windows
VERSION.dll	-	-	-	0x000077CC	0x00007268	implicit	3	-	Version Checking and File Installation Library

Screenshot 11. Libraries used by dog.jpg via PEStudio



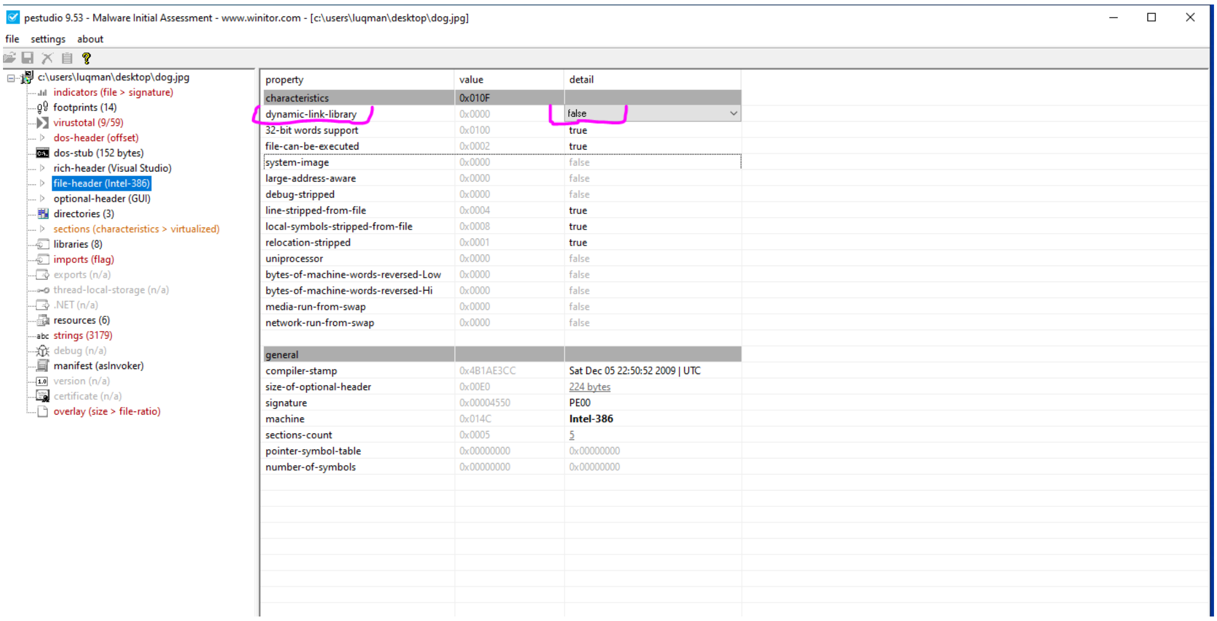
Dog.jpg

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00008C80  65 79 41 00 F7 01 52 65 67 51 75 65 72 79 56 61  eyA.÷.RegQueryVa
00008C90  6C 75 65 45 78 41 00 00 04 02 52 65 67 53 65 74  lueExA....RegSet
00008CA0  56 61 6C 75 65 45 78 41 00 00 D1 01 52 65 67 43  ValueExA..Ñ.RegC
00008CB0  72 65 61 74 65 4B 65 79 45 78 41 00 CB 01 52 65  reateKeyExA.Ë.Re
00008CC0  67 43 6C 6F 73 65 4B 65 79 00 D8 01 52 65 67 44  gCloseKey.Ø.RegD
00008CD0  65 6C 65 74 65 56 61 6C 75 65 41 00 D4 01 52 65  eleteValueA.Ô.Re
00008CE0  67 44 65 6C 65 74 65 4B 65 79 41 00 EC 01 52 65  gDeleteKeyA.ì.Re
00008CF0  67 4F 70 65 6E 4B 65 79 45 78 41 00 41 44 56 41  gOpenKeyExA.ADVA
00008D00  50 49 33 32 2E 64 6C 6C 00 00 38 00 49 6D 61 67  PI32.dll..8.Imag
00008D10  65 4C 69 73 74 5F 44 65 73 74 72 6F 79 00 34 00  eList_Destroy.4.
00008D20  49 6D 61 67 65 4C 69 73 74 5F 41 64 64 4D 61 73  ImageList_AddMas
00008D30  6B 65 64 00 37 00 49 6D 61 67 65 4C 69 73 74 5F  ked.7.ImageList_
00008D40  43 72 65 61 74 65 00 00 43 4F 4D 43 54 4C 33 32  Create..COMCTL32
00008D50  2E 64 6C 6C 00 00 10 00 43 6F 43 72 65 61 74 65  .dll....CoCreate
00008D60  49 6E 73 74 61 6E 63 65 00 00 05 01 4F 6C 65 55  Instance....OleU
00008D70  6E 69 6E 69 74 69 61 6C 69 7A 65 00 EE 00 4F 6C  ninitialize.î.Ol
00008D80  65 49 6E 69 74 69 61 6C 69 7A 65 00 65 00 43 6F  eInitialize.e.Co
00008D90  54 61 73 6B 4D 65 6D 46 72 65 65 00 6F 6C 65 33  TaskMemFree.ole3
00008DA0  32 2E 64 6C 6C 00 0A 00 56 65 72 51 75 65 72 79  2.dll...VerQuery
00008DB0  56 61 6C 75 65 41 00 00 00 00 47 65 74 46 69 6C  ValueA....GetFil
00008DC0  65 56 65 72 73 69 6F 6E 49 6E 66 6F 41 00 01 00  eVersionInfoA...
00008DD0  47 65 74 46 69 6C 65 56 65 72 73 69 6F 6E 49 6E  GetFileVersionIn
00008DE0  66 6F 53 69 7A 65 41 00 56 45 52 53 49 4F 4E 2E  foSizeA.VERSION.
00008DF0  64 6C 6C 00 00 00 00 00 00 00 00 00 00 00 00 00  dll.............
00008E00  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00008E10  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00008E20  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Offset	Excerpt (hex)	Excerpt (text)
8741	72 73 69 6F 6E 00 00 4B 45 52 4E 45 4C 33 32 2E **64 6C 6C** 00 00 C8 00 45 6E 64 50 61 69 6E 74 00	rsion..KERNEL32.**dll**..È.EndPaint.
8B43	65 73 73 61 67 65 41 00 00 55 53 45 52 33 32 2E **64 6C 6C** 00 00 0E 02 53 65 6C 65 63 74 4F 62 6A	essageA..USER32.**dll**....SelectObj
8BD4	74 42 6B 43 6F 6C 6F 72 00 00 47 44 49 33 32 2E **64 6C 6C** 00 9A 00 53 48 46 69 6C 65 4F 70 65 72	tBkColor..GDI32.**dll**.š.SHFileOper
8C62	63 61 74 69 6F 6E 00 00 53 48 45 4C 4C 33 32 2E **64 6C 6C** 00 E1 01 52 65 67 45 6E 75 6D 56 61 6C	cation..SHELL32.**dll**.á.RegEnumVal
8D05	4B 65 79 45 78 41 00 41 44 56 41 50 49 33 32 2E **64 6C 6C** 00 00 38 00 49 6D 61 67 65 4C 69 73 74	KeyExA.ADVAPI32.**dll**..8.ImageList
8D51	72 65 61 74 65 00 00 43 4F 4D 43 54 4C 33 32 2E **64 6C 6C** 00 00 10 00 43 6F 43 72 65 61 74 65 49	reate..COMCTL32.**dll**....CoCreateI
8DA2	73 6B 4D 65 6D 46 72 65 65 00 6F 6C 65 33 32 2E **64 6C 6C** 00 0A 00 56 65 72 51 75 65 72 79 56 61	skMemFree.ole32.**dll**...VerQueryVa
8DF0	66 6F 53 69 7A 65 41 00 56 45 52 53 49 4F 4E 2E **64 6C 6C** 00 00 00 00 00 00 00 00 00 00 00 00 00	foSizeA.VERSION.**dll**............

Screenshot 11a. Libraries used by dog.jpg via Hex Editor

Look closer, value of dynamic-link-library is set as FALSE. What does it mean?


pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\luqman\desktop\dog.jpg]
file
settings
about

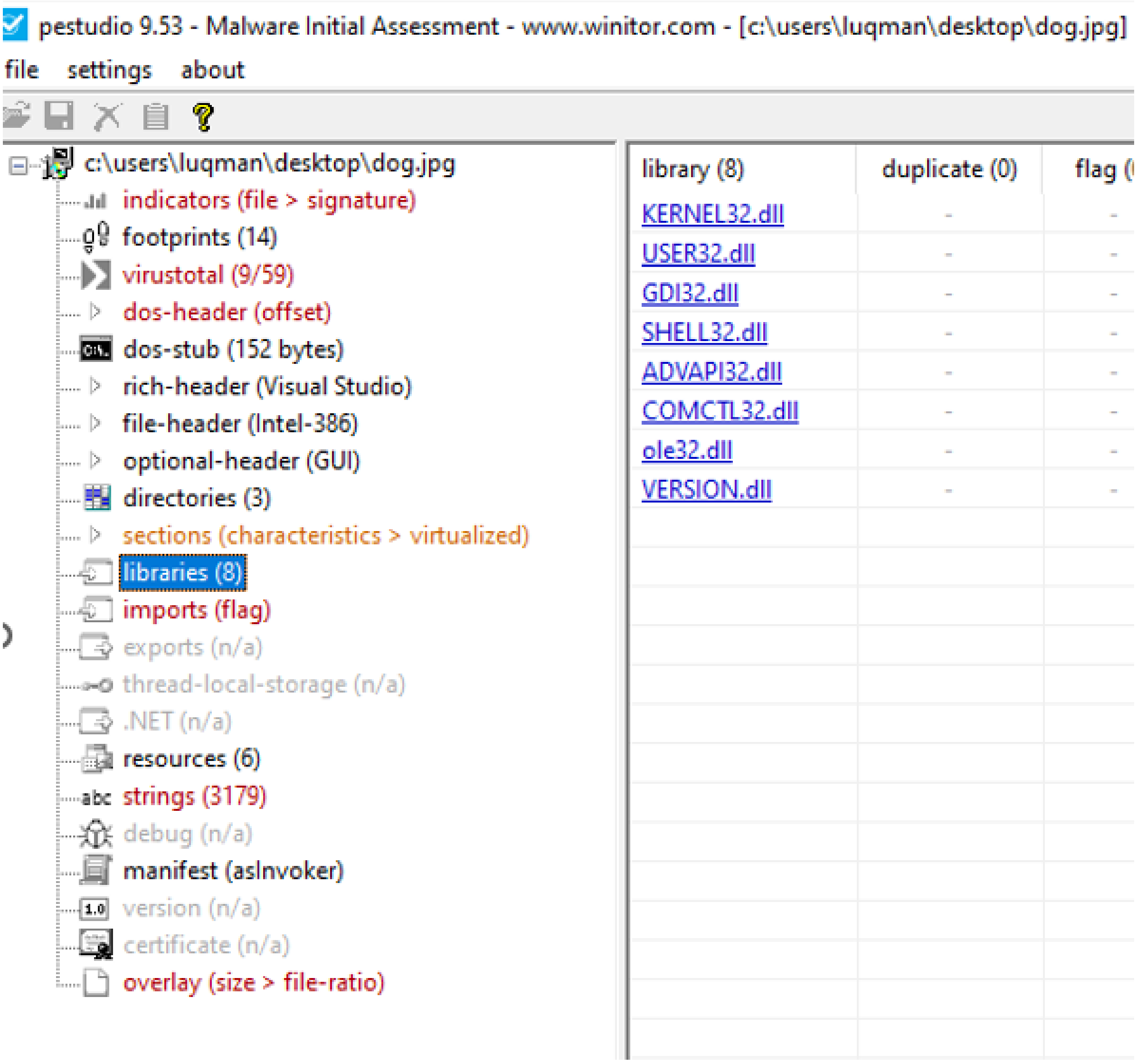
```
c:\users\luqman\desktop\dog.jpg
    indicators (file > signature)
    footprints (14)
    virustotal (9/59)
    dos-header (offset)
    dos-stub (152 bytes)
    rich-header (Visual Studio)
    file-header (Intel-386)
    optional-header (GUI)
    directories (3)
    sections (characteristics > virtualized)
    libraries (8)
    imports (flag)
    exports (n/a)
    thread-local-storage (n/a)
    .NET (n/a)
    resources (6)
    strings (3179)
    debug (n/a)
    manifest (asInvoker)
    version (n/a)
    certificate (n/a)
    overlay (size > file-ratio)
```

property	value	detail
characteristics	0x010F	
dynamic-link-library	0x0000	false
32-bit words support	0x0100	true
file-can-be-executed	0x0002	true
system-image	0x0000	false
large-address-aware	0x0000	false
debug-stripped	0x0000	false
line-stripped-from-file	0x0004	true
local-symbols-stripped-from-file	0x0008	true
relocation-stripped	0x0001	true
uniprocessor	0x0000	false
bytes-of-machine-words-reversed-Low	0x0000	false
bytes-of-machine-words-reversed-Hi	0x0000	false
media-run-from-swap	0x0000	false
network-run-from-swap	0x0000	false
general		
compiler-stamp	0x4B1AE3CC	Sat Dec 05 22:50:52 2009 | UTC
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	**Intel-386**
sections-count	0x0005	5
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000

Screenshot 12. Dynamic link Library set as false

When the system starts a program that uses load-time dynamic linking, uses the information the linker placed in the file to locate the names of the DLLs and use them. In this case, it is set as FALSE value, it means the application will not start. If required DLL cannot be located, system terminates the process and displays a dialog box that reports the error to the user.

On the screenshot below are dlls used by the file but cannot be found:



pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\luqman\desktop\dog.jpg]

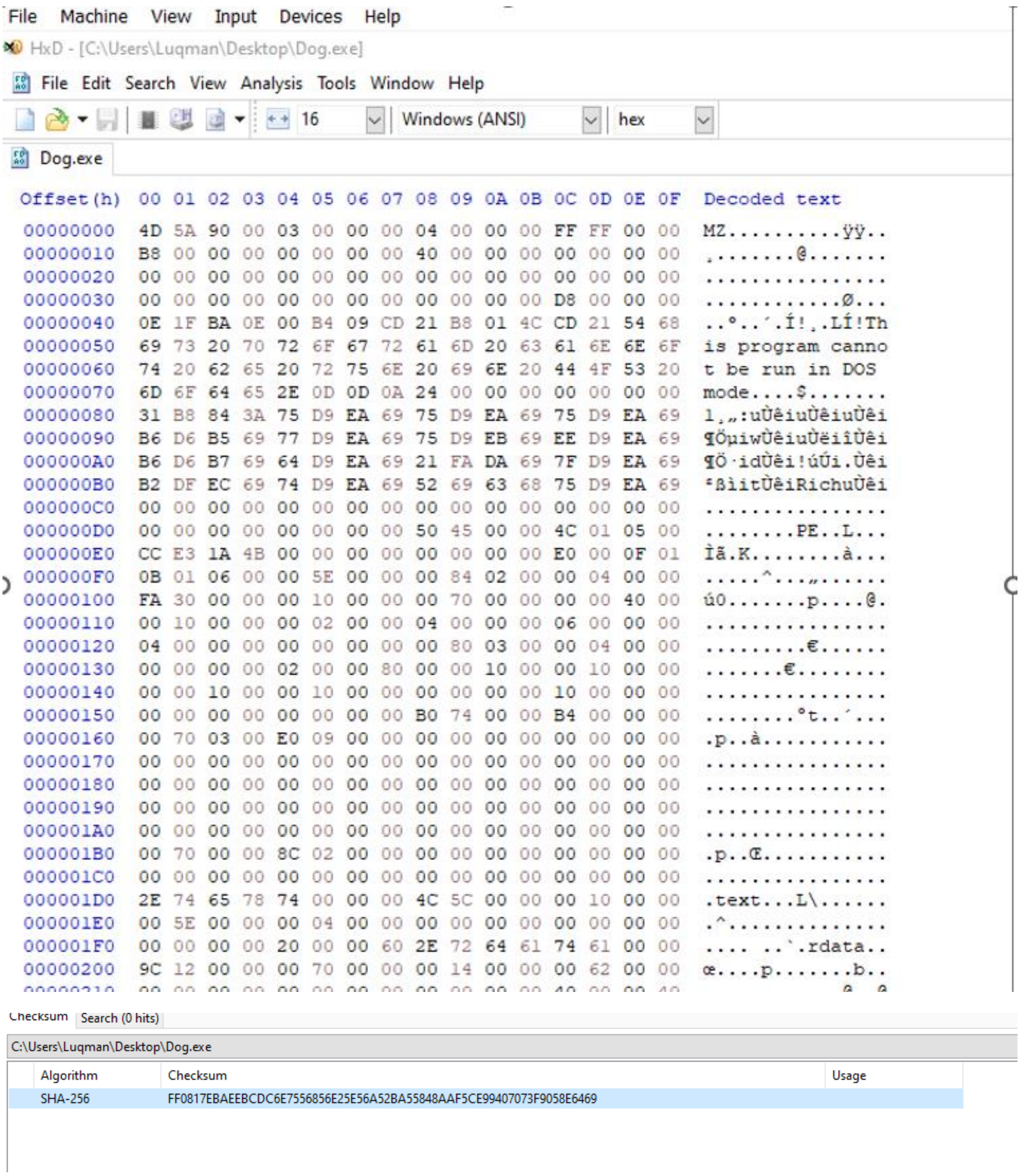
c:\users\luqman\desktop\dog.jpg

- indicators (file > signature)
- footprints (14)
- virustotal (9/59)
- dos-header (offset)
- dos-stub (152 bytes)
- rich-header (Visual Studio)
- file-header (Intel-386)
- optional-header (GUI)
- directories (3)
- sections (characteristics > virtualized)
- libraries (8)
- imports (flag)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (6)
- strings (3179)
- debug (n/a)
- manifest (asInvoker)
- version (n/a)
- certificate (n/a)
- overlay (size > file-ratio)

library (8)	duplicate (0)	flag (
KERNEL32.dll	-	-
USER32.dll	-	-
GDI32.dll	-	-
SHELL32.dll	-	-
ADVAPI32.dll	-	-
COMCTL32.dll	-	-
ole32.dll	-	-
VERSION.dll	-	-

Screenshot 13. Libraries used by dog.jpg

b) We can also consider this task from another point of view. Using Hex editor, I removed part of bytes, leaving only bytes responsible for malicious part (starts with 4D 5A – magic bytes) and saved it as dog.exe

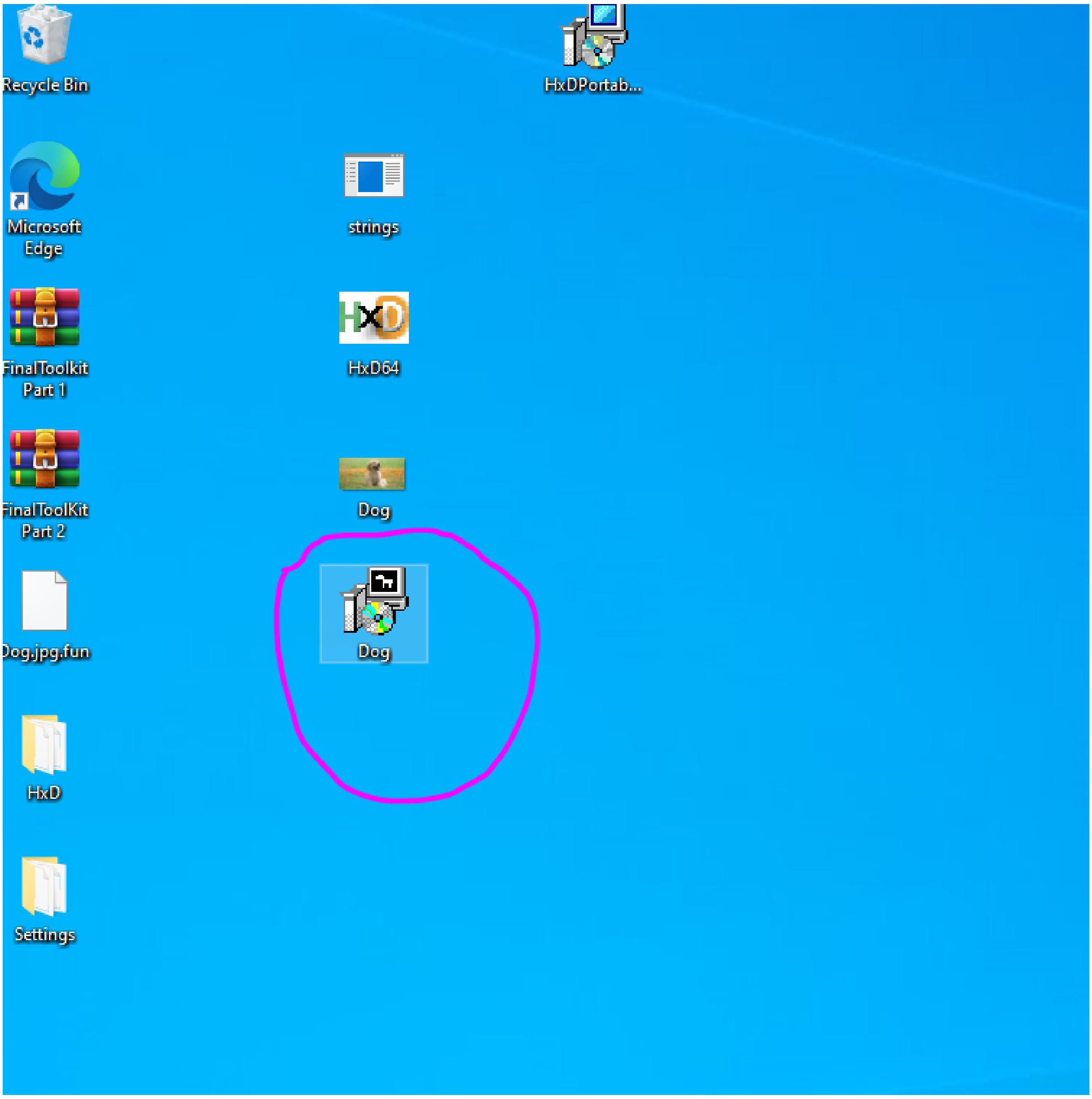

File Machine View Input Devices Help
HxD - [C:\Users\Luqman\Desktop\Dog.exe]
File Edit Search View Analysis Tools Window Help
16
Windows (ANSI)
hex
Dog.exe
Checksum
Search (0 hits)

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
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 D8 00 00 00  ............Ø...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!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....$.......
00000080  31 B8 84 3A 75 D9 EA 69 75 D9 EA 69 75 D9 EA 69  1¸„:uÙêiuÙêiuÙêi
00000090  B6 D6 B5 69 77 D9 EA 69 75 D9 EB 69 EE D9 EA 69  ¶ÖµiwÙêiuÙëiîÙêi
000000A0  B6 D6 B7 69 64 D9 EA 69 21 FA DA 69 7F D9 EA 69  ¶Ö·idÙêi!úÚi.Ùêi
000000B0  B2 DF EC 69 74 D9 EA 69 52 69 63 68 75 D9 EA 69  ²ßìitÙêiRichuÙêi
000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000D0  00 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00  ........PE..L...
000000E0  CC E3 1A 4B 00 00 00 00 00 00 00 00 E0 00 0F 01  Ìã.K........à...
000000F0  0B 01 06 00 00 5E 00 00 00 84 02 00 00 04 00 00  .....^...„......
00000100  FA 30 00 00 00 10 00 00 00 70 00 00 00 00 40 00  ú0.......p....@.
00000110  00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00  ................
00000120  04 00 00 00 00 00 00 00 00 80 03 00 00 04 00 00  .........€......
00000130  00 00 00 00 02 00 00 80 00 00 10 00 00 10 00 00  .......€........
00000140  00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00  ................
00000150  00 00 00 00 00 00 00 00 B0 74 00 00 B4 00 00 00  ........°t..´...
00000160  00 70 03 00 E0 09 00 00 00 00 00 00 00 00 00 00  .p..à...........
00000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001B0  00 70 00 00 8C 02 00 00 00 00 00 00 00 00 00 00  .p..Œ...........
000001C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001D0  2E 74 65 78 74 00 00 00 4C 5C 00 00 00 10 00 00  .text...L\......
000001E0  00 5E 00 00 00 04 00 00 00 00 00 00 00 00 00 00  .^..............
000001F0  00 00 00 00 20 00 00 60 2E 72 64 61 74 61 00 00  .... ..`.rdata..
00000200  9C 12 00 00 00 70 00 00 00 14 00 00 00 62 00 00  œ....p.......b..
00000210  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40  ............@..@
```

C:\Users\Luqman\Desktop\Dog.exe

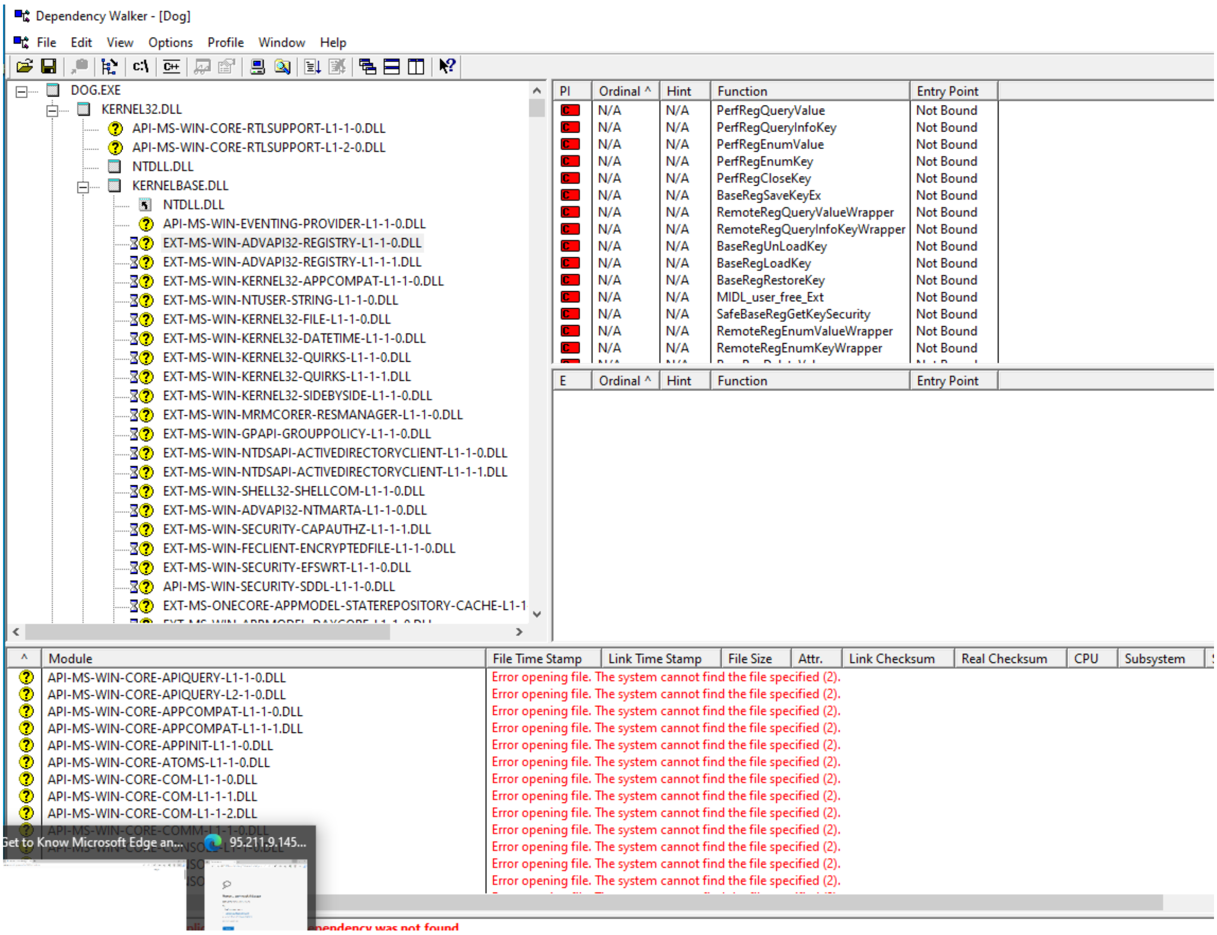
Algorithm	Checksum	Usage
SHA-256	FF0817EBAEEBCDC6E7556856E25E56A52BA55848AAF5CE99407073F9058E6469	

Screenshot 14. Creating file Dog.exe by by partially deleting bytes from dog.jpg



Screenshot 15. Dog.exe file

View in Dependency Walker:


Dependency Walker - [Dog]
File Edit View Options Profile Window Help
Get to Know Microsoft Edge an...
95.211.9.145...

```
DOG.EXE
  KERNEL32.DLL
    API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
    API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
    NTDLL.DLL
    KERNELBASE.DLL
      NTDLL.DLL
      API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
      EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
      EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-1.DLL
      EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
      EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
      EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
      EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
      EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
      EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL
      EXT-MS-WIN-KERNEL32-SIDEBYSIDE-L1-1-0.DLL
      EXT-MS-WIN-MRMCORER-RESMANAGER-L1-1-0.DLL
      EXT-MS-WIN-GPAPI-GROUPPOLICY-L1-1-0.DLL
      EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-0.DLL
      EXT-MS-WIN-NTDSAPI-ACTIVEDIRECTORYCLIENT-L1-1-1.DLL
      EXT-MS-WIN-SHELL32-SHELLCOM-L1-1-0.DLL
      EXT-MS-WIN-ADVAPI32-NTMARTA-L1-1-0.DLL
      EXT-MS-WIN-SECURITY-CAPAUTHZ-L1-1-1.DLL
      EXT-MS-WIN-FECLIENT-ENCRYPTEDFILE-L1-1-0.DLL
      EXT-MS-WIN-SECURITY-EFSWRT-L1-1-0.DLL
      API-MS-WIN-SECURITY-SDDL-L1-1-0.DLL
      EXT-MS-ONECORE-APPMODEL-STATEREPOSITORY-CACHE-L1-1
```

PI	Ordinal ^	Hint	Function	Entry Point
🟥	N/A	N/A	PerfRegQueryValue	Not Bound
🟥	N/A	N/A	PerfRegQueryInfoKey	Not Bound
🟥	N/A	N/A	PerfRegEnumValue	Not Bound
🟥	N/A	N/A	PerfRegEnumKey	Not Bound
🟥	N/A	N/A	PerfRegCloseKey	Not Bound
🟥	N/A	N/A	BaseRegSaveKeyEx	Not Bound
🟥	N/A	N/A	RemoteRegQueryValueWrapper	Not Bound
🟥	N/A	N/A	RemoteRegQueryInfoKeyWrapper	Not Bound
🟥	N/A	N/A	BaseRegUnLoadKey	Not Bound
🟥	N/A	N/A	BaseRegLoadKey	Not Bound
🟥	N/A	N/A	BaseRegRestoreKey	Not Bound
🟥	N/A	N/A	MIDL_user_free_Ext	Not Bound
🟥	N/A	N/A	SafeBaseRegGetKeySecurity	Not Bound
🟥	N/A	N/A	RemoteRegEnumValueWrapper	Not Bound
🟥	N/A	N/A	RemoteRegEnumKeyWrapper	Not Bound

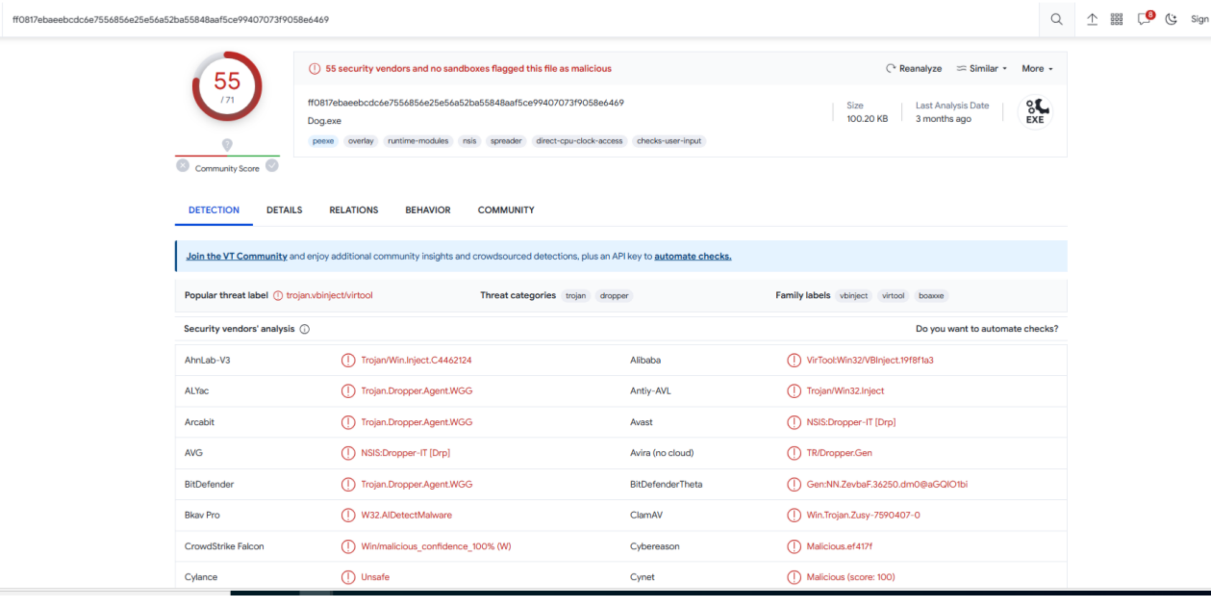
E	Ordinal ^	Hint	Function	Entry Point

^	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-APIQUERY-L2-1-0.DLL	Error opening file. The system cannot find the file specified (2).							
?	API-MS-WIN-CORE-APPCOMPAT-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-COM-L1-1-0.DLL	Error opening file. The system cannot find the file specified (2).							
?	API-MS-WIN-CORE-COM-L1-1-1.DLL	Error opening file. The system cannot find the file specified (2).							
?	API-MS-WIN-CORE-COM-L1-1-2.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).							
?	API-MS-WIN-CORE-CONSOL...	Error opening file. The system cannot find the file specified (2).							
		Error opening file. The system cannot find the file specified (2).							
		Error opening file. The system cannot find the file specified (2).							

...pendency was not found

Screenshot 16. Dog.exe analysing in Dependency Walker

And now, using hash of this file we can check virustotal.com:



55 security vendors and no sandboxes flagged this file as malicious

ff0817ebaeebcdc6e7556856e25e56a52ba55848aaf5ce99407073f9058e6469

Dog.exe

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

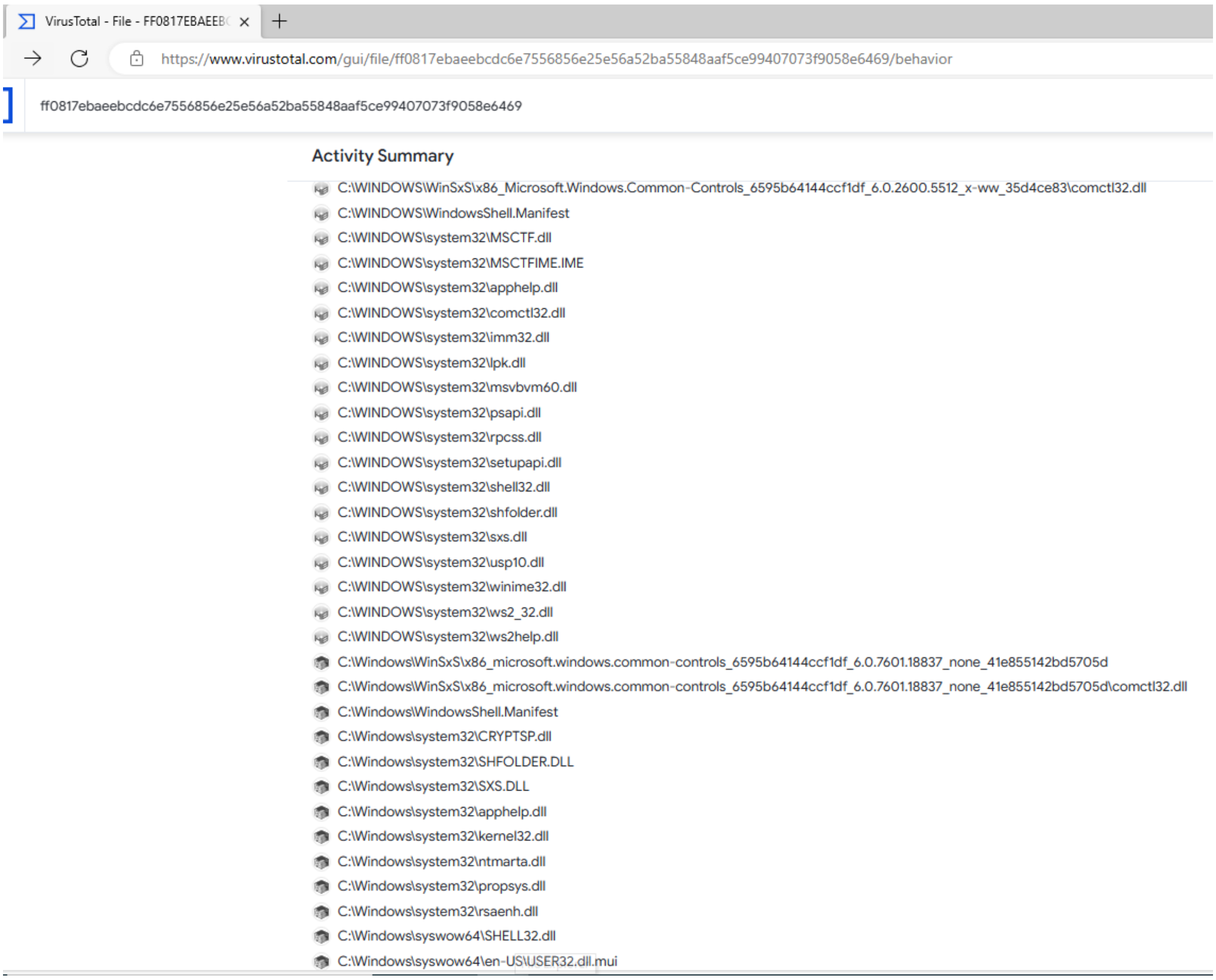
Popular threat label trojan.vbinject/virtool Threat categories trojan dropper Family labels vbinject virtool boaxxe

Security vendors' analysis Do you want to automate checks?

AhnLab-V3	Trojan/Win.Inject.C4462124	Alibaba	VirTool:Win32/VBInject.19f8f1a3
ALYac	Trojan.Dropper.Agent.WGG	Antiy-AVL	Trojan/Win32.Inject
Arcabit	Trojan.Dropper.Agent.WGG	Avast	NSIS:Dropper-IT [Drp]
AVG	NSIS:Dropper-IT [Drp]	Avira (no cloud)	TR/Dropper.Gen
BitDefender	Trojan.Dropper.Agent.WGG	BitDefenderTheta	Gen:NN.ZevbaF.36250.dm0@aGQIO1bi
Bkav Pro	W32.AIDetectMalware	ClamAV	Win.Trojan.Zusy-7590407-0
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.ef417f
Cylance	Unsafe	Cynet	Malicious (score: 100)

Screenshot 17. Dog.exe marked as malicious – virus total

And in Activity Summary - “files opened” tab more dlls are mentioned. They weren’t found during earlier analysis dog.jpg:


VirusTotal - File - FF0817EBAEEB
https://www.virustotal.com/gui/file/ff0817ebaeebcdc6e7556856e25e56a52ba55848aaf5ce99407073f9058e6469/behavior
ff0817ebaeebcdc6e7556856e25e56a52ba55848aaf5ce99407073f9058e6469

Activity Summary

```
C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2600.5512_x-ww_35d4ce83\comctl32.dll
C:\WINDOWS\WindowsShell.Manifest
C:\WINDOWS\system32\MSCTF.dll
C:\WINDOWS\system32\MSCTFIME.IME
C:\WINDOWS\system32\apphelp.dll
C:\WINDOWS\system32\comctl32.dll
C:\WINDOWS\system32\imm32.dll
C:\WINDOWS\system32\lpk.dll
C:\WINDOWS\system32\msvbvm60.dll
C:\WINDOWS\system32\psapi.dll
C:\WINDOWS\system32\rpcss.dll
C:\WINDOWS\system32\setupapi.dll
C:\WINDOWS\system32\shell32.dll
C:\WINDOWS\system32\shfolder.dll
C:\WINDOWS\system32\sxs.dll
C:\WINDOWS\system32\usp10.dll
C:\WINDOWS\system32\winime32.dll
C:\WINDOWS\system32\ws2_32.dll
C:\WINDOWS\system32\ws2help.dll
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d
C:\Windows\WinSxS\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.18837_none_41e855142bd5705d\comctl32.dll
C:\Windows\WindowsShell.Manifest
C:\Windows\system32\CRYPTSP.dll
C:\Windows\system32\SHFOLDER.DLL
C:\Windows\system32\SXS.DLL
C:\Windows\system32\apphelp.dll
C:\Windows\system32\kernel32.dll
C:\Windows\system32\ntmarta.dll
C:\Windows\system32\propsys.dll
C:\Windows\system32\rsaenh.dll
C:\Windows\syswow64\SHELL32.dll
C:\Windows\syswow64\en-US\USER32.dll.mui
```