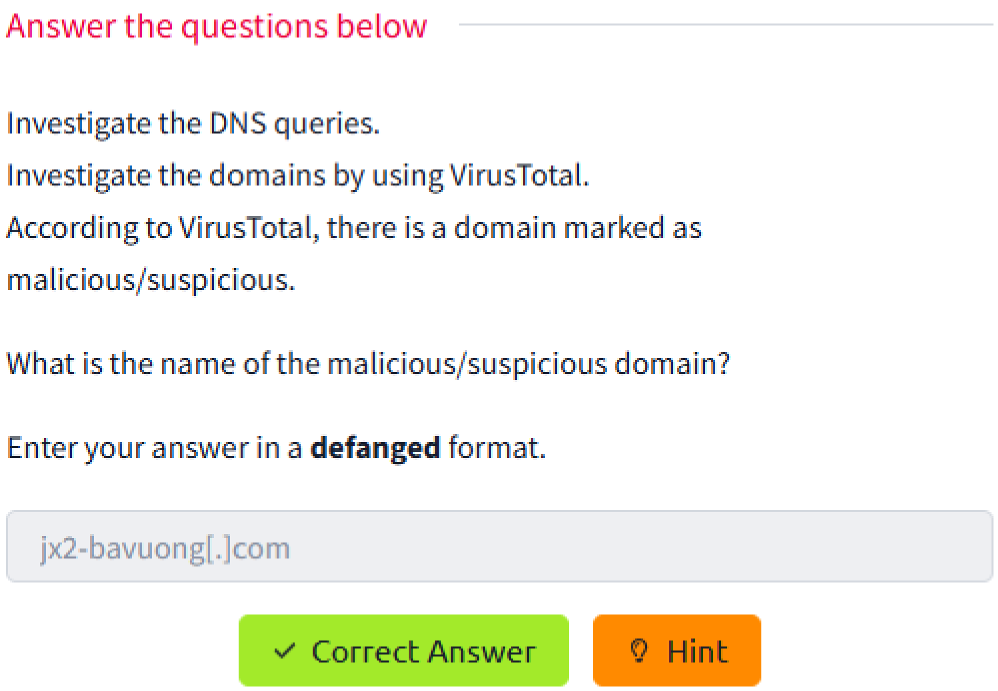
TShark Challenge II: Directory



Answer the questions below

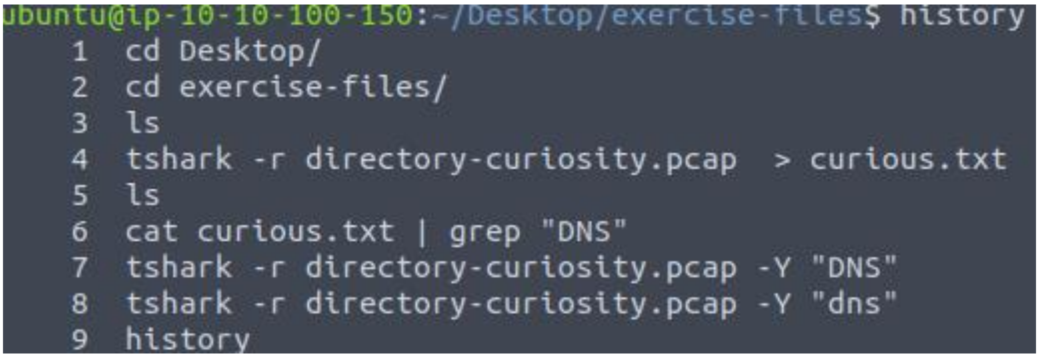
Investigate the DNS queries.
Investigate the domains by using VirusTotal.
According to VirusTotal, there is a domain marked as malicious/suspicious.

What is the name of the malicious/suspicious domain?

Enter your answer in a **defanged** format.

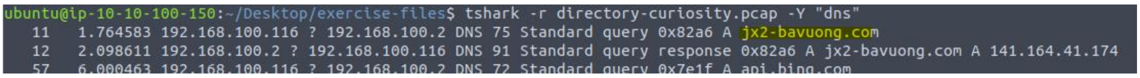
jx2-bavuong[.]com

First thing I did is to go to the correct directory. I created a .txt to make the search easy.

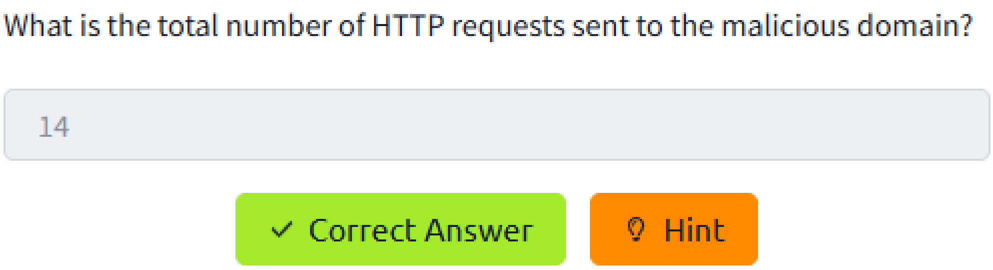


```
ubuntu@ip-10-10-100-150:~/Desktop/exercise-files$ history
    1  cd Desktop/
    2  cd exercise-files/
    3  ls
    4  tshark -r directory-curiosity.pcap  > curious.txt
    5  ls
    6  cat curious.txt | grep "DNS"
    7  tshark -r directory-curiosity.pcap -Y "DNS"
    8  tshark -r directory-curiosity.pcap -Y "dns"
    9  history
```

I used this command and I find this domain that was suspicious for me.

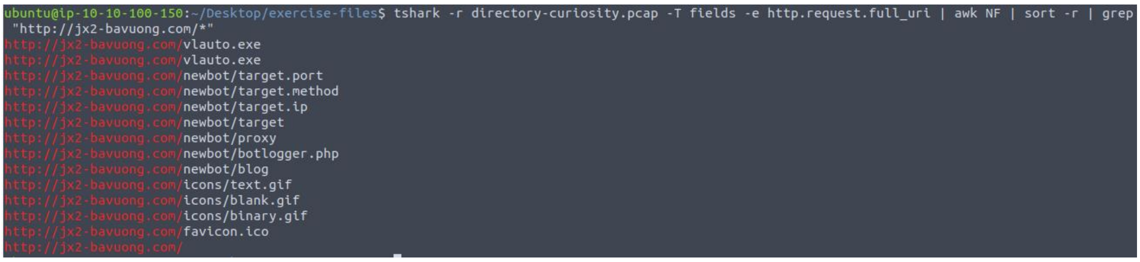


```
ubuntu@ip-10-10-100-150:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap -Y "dns"
   11   1.764583 192.168.100.116 ? 192.168.100.2 DNS 75 Standard query 0x82a6 A jx2-bavuong.com
   12   2.098611 192.168.100.2 ? 192.168.100.116 DNS 91 Standard query response 0x82a6 A jx2-bavuong.com A 141.164.41.174
   57   6.000463 192.168.100.116 ? 192.168.100.2 DNS 72 Standard query 0x7e1f A api.bing.com
```



What is the total number of HTTP requests sent to the malicious domain?

14



```
ubuntu@ip-10-10-100-150:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap -T fields -e http.request.full_uri | awk NF | sort -r | grep
 "http://jx2-bavuong.com/*"
http://jx2-bavuong.com/vlauto.exe
http://jx2-bavuong.com/vlauto.exe
http://jx2-bavuong.com/newbot/target.port
http://jx2-bavuong.com/newbot/target.method
http://jx2-bavuong.com/newbot/target.ip
http://jx2-bavuong.com/newbot/target
http://jx2-bavuong.com/newbot/proxy
http://jx2-bavuong.com/newbot/botlogger.php
http://jx2-bavuong.com/newbot/blog
http://jx2-bavuong.com/icons/text.gif
http://jx2-bavuong.com/icons/blank.gif
http://jx2-bavuong.com/icons/binary.gif
http://jx2-bavuong.com/favicon.ico
http://jx2-bavuong.com/
```

To have more details of what I did with this command:

tshark -r directory-curiosity.pcap -T fields -e http.request.full_uri:

- Uses **tshark** (Wireshark's command-line tool) to read the network capture file (directory-curiosity.pcap).
- It extracts all **full HTTP request URIs** (http.request.full_uri) from the packets.
- The output is formatted into **fields** (-T fields), meaning each URI gets its own line.

□ **| awk NF**:

- The **pipe |** sends the output of tshark as input to awk.
- **awk NF** filters out any blank lines, ensuring only lines with actual URIs are processed further. (NF stands for "Number of Fields"; if a line has fields, it's not empty, so awk prints it).

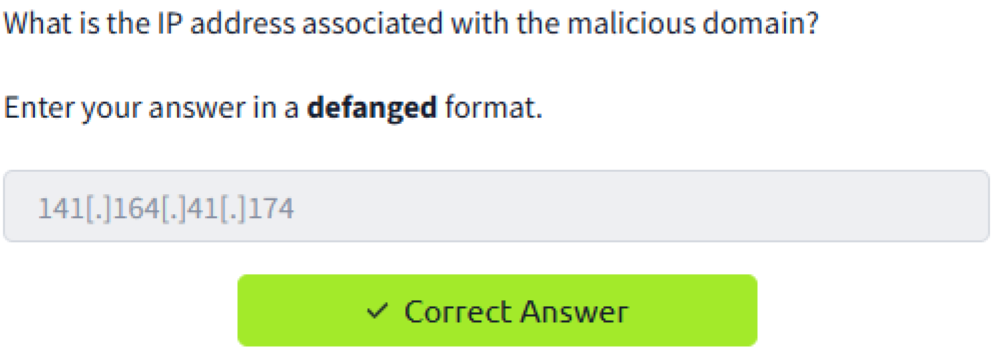
□ **| sort -r**:

- The **pipe |** sends the filtered URIs to sort.
- **sort -r** sorts these URIs in **reverse alphabetical order**.

□ **| grep "http://jx2-bavuong.com/*"**:

- The **pipe |** sends the sorted URIs to grep.
- **grep "http://jx2-bavuong.com/*"** filters the list to show only those URIs that contain the string "http://jx2-bavuong.com/".

The command reads network traffic, pulls out all the complete website addresses (URIs) from HTTP requests, removes any empty entries, sorts them in reverse order, and then displays only those URIs that belong to the jx2-bavuong.com domain.

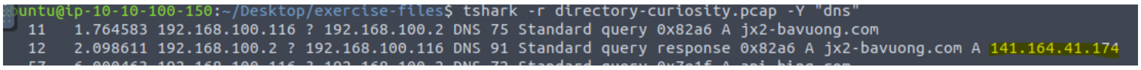


What is the IP address associated with the malicious domain?

Enter your answer in a **defanged** format.

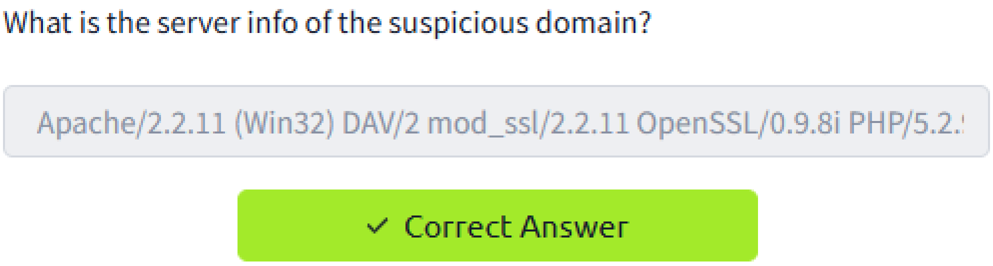
141[.]164[.]41[.]174

✓ Correct Answer



```
untu@ip-10-10-100-150:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap -Y "dns"
  11   1.764583 192.168.100.116 ? 192.168.100.2 DNS 75 Standard query 0x82a6 A jx2-bavuong.com
  12   2.098611 192.168.100.2 ? 192.168.100.116 DNS 91 Standard query response 0x82a6 A jx2-bavuong.com A 141.164.41.174
  57   6.000463 192.168.100.116 ? 192.168.100.2 DNS 73 Standard query 0x7e1f A api.bing.com
```

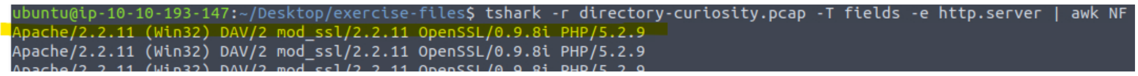
I find the answer also with the first command that I used.



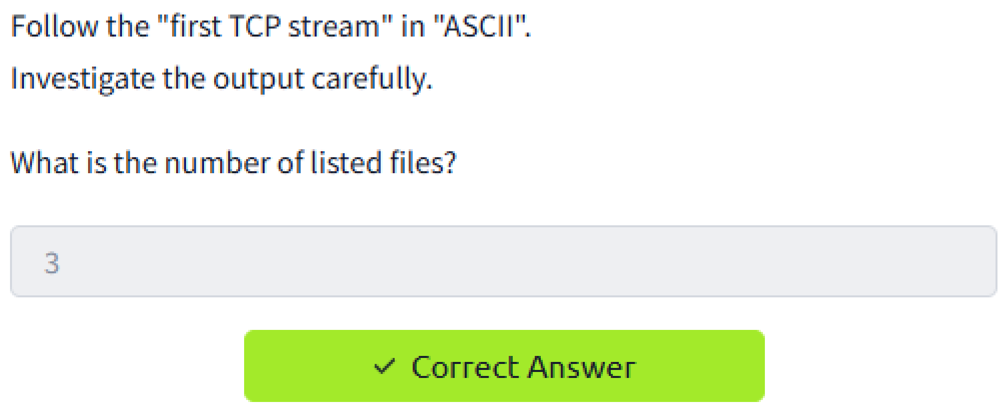
What is the server info of the suspicious domain?

Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.

✓ Correct Answer



```
ubuntu@ip-10-10-193-147:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap -T fields -e http.server | awk NF
Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9
```

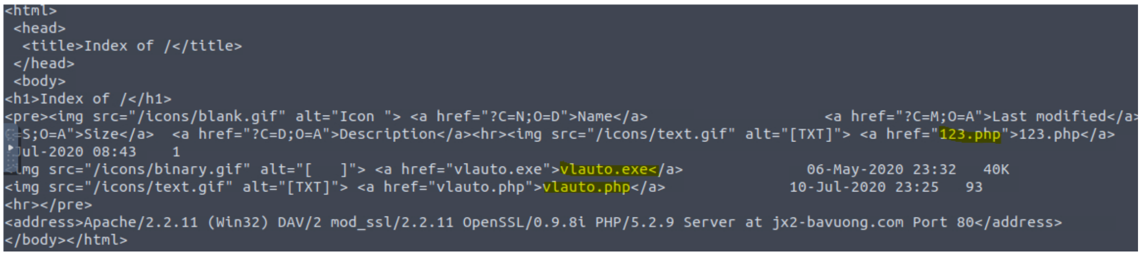


Follow the "first TCP stream" in "ASCII".

Investigate the output carefully.

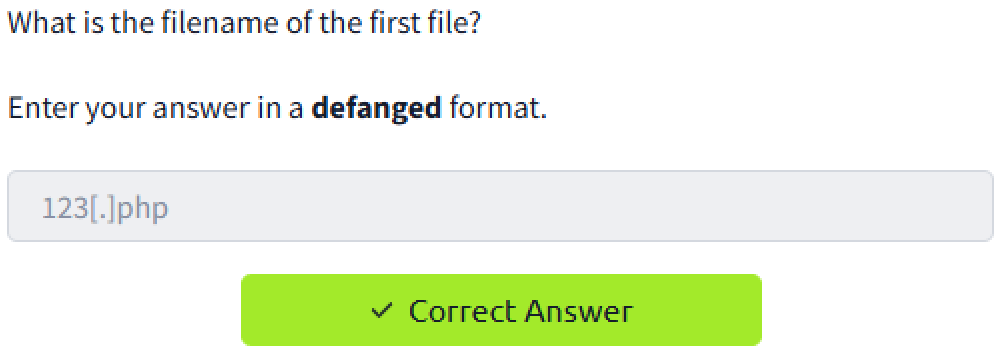
What is the number of listed files?

3



```
<html>
 <head>
  <title>Index of /</title>
 </head>
 <body>
<h1>Index of /</h1>
<pre><img src="/icons/blank.gif" alt="Icon "> <a href="?C=N;O=D">Name</a>                    <a href="?C=M;O=A">Last modified</a>
S;O=A">Size</a>  <a href="?C=D;O=A">Description</a><hr><img src="/icons/text.gif" alt="[TXT]"> <a href="123.php">123.php</a>
Jul-2020 08:43    1
mg src="/icons/binary.gif" alt="[   ]"> <a href="vlauto.exe">vlauto.exe</a>              06-May-2020 23:32   40K
<img src="/icons/text.gif" alt="[TXT]"> <a href="vlauto.php">vlauto.php</a>              10-Jul-2020 23:25   93
<hr></pre>
<address>Apache/2.2.11 (Win32) DAV/2 mod_ssl/2.2.11 OpenSSL/0.9.8i PHP/5.2.9 Server at jx2-bavuong.com Port 80</address>
</body></html>
```

I could find 3 files for this question with this command: tshark -r directory-curiosity.pcap -z follow,tcp,ascii,0 -q

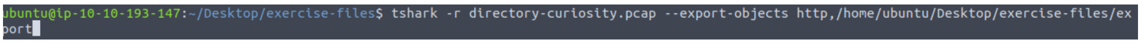


What is the filename of the first file?

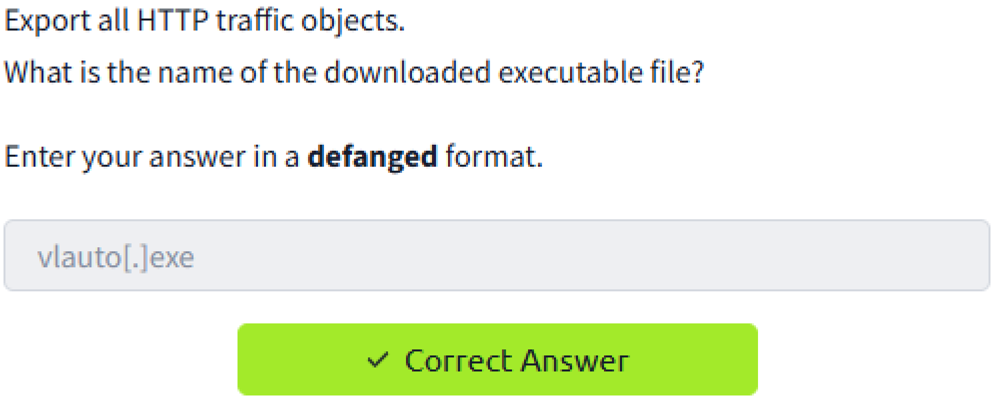
Enter your answer in a **defanged** format.

123[.]php

Now I export the http and I used this command



```
ubuntu@ip-10-10-193-147:~/Desktop/exercise-files$ tshark -r directory-curiosity.pcap --export-objects http,/home/ubuntu/Desktop/exercise-files/ex
port
```



Export all HTTP traffic objects.

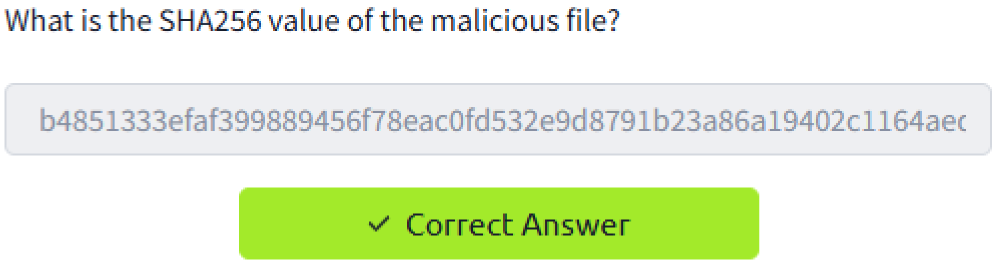
What is the name of the downloaded executable file?

Enter your answer in a **defanged** format.

vlauto[.]exe

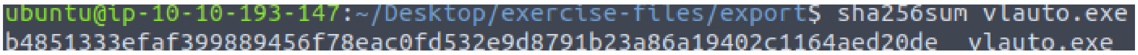
In the new export directory I could find the executable.

To know the sha256 value I just need it to run a simple command.



What is the SHA256 value of the malicious file?

b4851333efaf399889456f78eac0fd532e9d8791b23a86a19402c1164aec



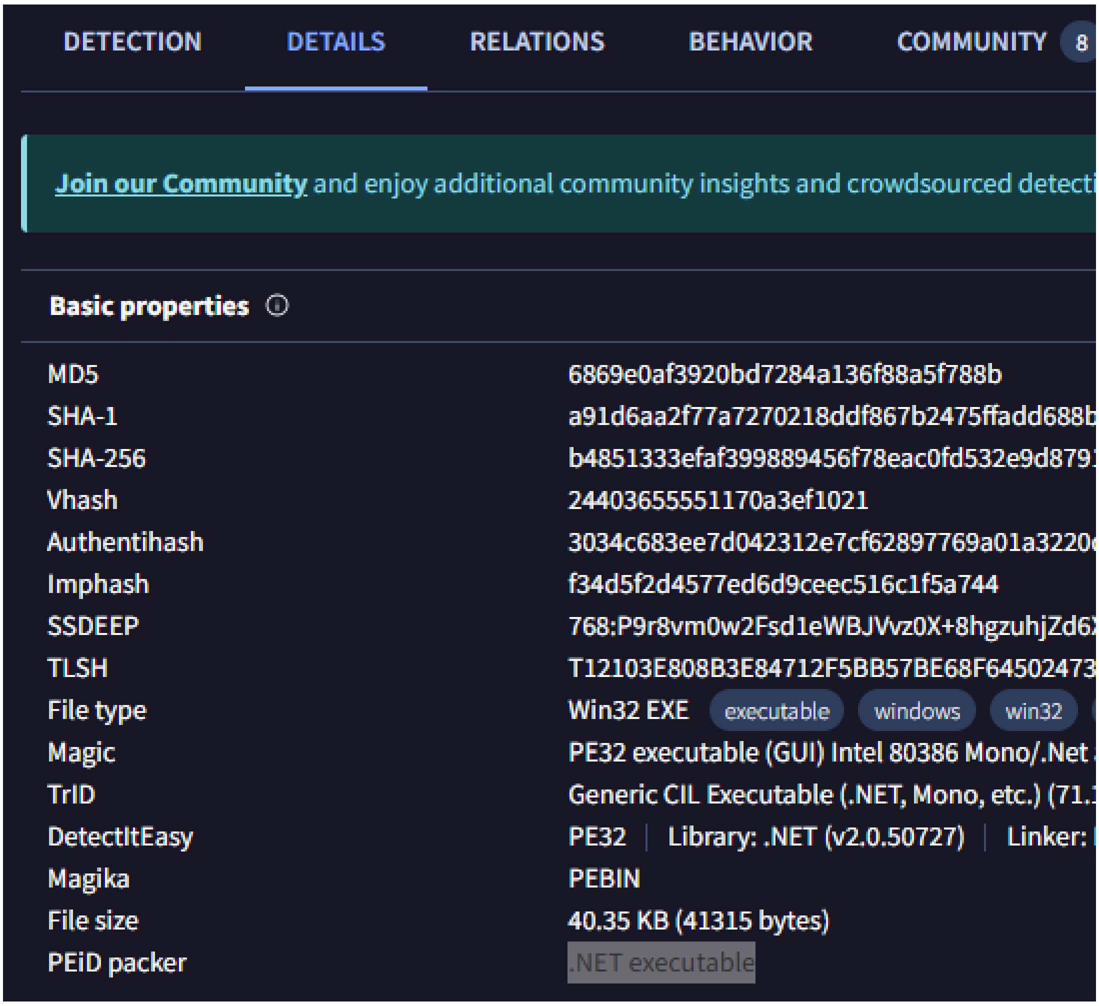
```
ubuntu@ip-10-10-193-147:~/Desktop/exercise-files/export$ sha256sum vlauto.exe
b4851333efaf399889456f78eac0fd532e9d8791b23a86a19402c1164aed20de  vlauto.exe
```

Search the SHA256 value of the file on VirtusTotal.

What is the "PEiD packer" value?

.NET executable

✓ Correct Answer



Join our Community and enjoy additional community insights and crowdsourced detecti

Basic properties ⓘ

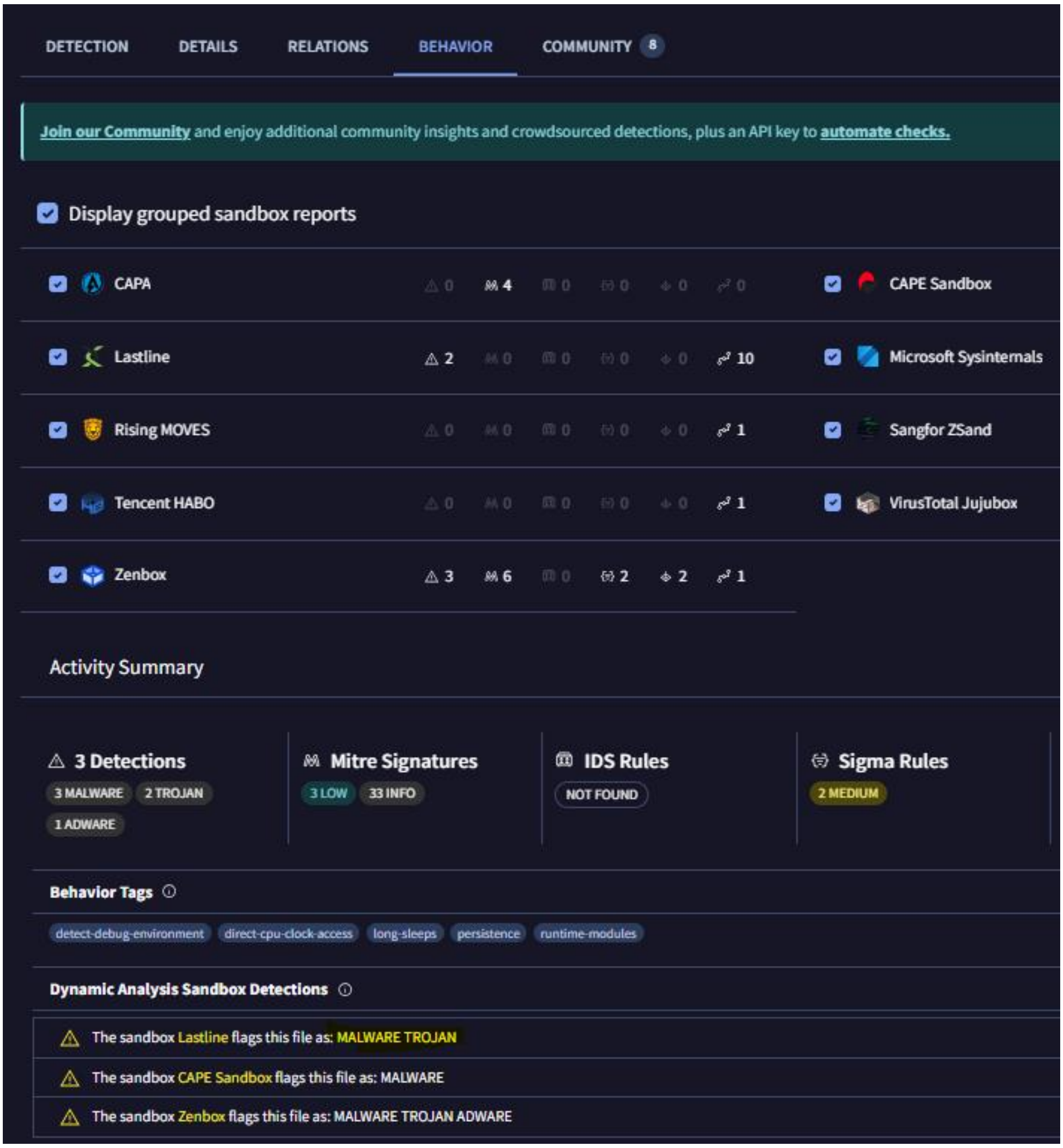
MD5	6869e0af3920bd7284a136f88a5f788b
SHA-1	a91d6aa2f77a7270218ddf867b2475ffadd688b
SHA-256	b4851333efaf399889456f78eac0fd532e9d879
Vhash	24403655551170a3ef1021
Authentihash	3034c683ee7d042312e7cf62897769a01a3220
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	768:P9r8vm0w2Fsd1eWBJVvz0X+8hgzuhjZd6
TLSH	T12103E808B3E84712F5BB57BE68F64502473
File type	Win32 EXE executable windows win32
Magic	PE32 executable (GUI) Intel 80386 Mono/.Net
TrID	Generic CIL Executable (.NET, Mono, etc.) (71.
DetectItEasy	PE32 | Library: .NET (v2.0.50727) | Linker:
Magika	PEBIN
File size	40.35 KB (41315 bytes)
PEiD packer	.NET executable

Search the SHA256 value of the file on VirtusTotal.

What does the "Lastline Sandbox" flag this as?

MALWARE TROJAN

Loading...



DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 8

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

☑ Display grouped sandbox reports

☑ CAPA	⚠ 0	4	0	0	0	0	☑ CAPE Sandbox
☑ Lastline	⚠ 2	0	0	0	0	10	☑ Microsoft Sysinternals
☑ Rising MOVES	⚠ 0	0	0	0	0	1	☑ Sangfor ZSand
☑ Tencent HABO	⚠ 0	0	0	0	0	1	☑ VirusTotal Jujubox
☑ Zenbox	⚠ 3	6	0	2	2	1	

Activity Summary

⚠ 3 Detections
3 MALWARE 2 TROJAN
1 ADWARE

Mitre Signatures
3 LOW 33 INFO

IDS Rules
NOT FOUND

Sigma Rules
2 MEDIUM

Behavior Tags ⓘ

detect-debug-environment direct-cpu-clock-access long-sleeps persistence runtime-modules

Dynamic Analysis Sandbox Detections ⓘ

⚠ The sandbox Lastline flags this file as: MALWARE TROJAN

⚠ The sandbox CAPE Sandbox flags this file as: MALWARE

⚠ The sandbox Zenbox flags this file as: MALWARE TROJAN ADWARE