OVERVIEW:

This lab focuses on analyzing potentially malicious files to determine their impact and behavior using various cybersecurity tools. Through hands-on investigation, we aim to identify threats, understand their execution, and explore methods to mitigate risks.

In the first activity, I examined a test malware file (*eicar.com*) by obtaining its hash and checking its reputation on VirusTotal. This helps demonstrate how antivirus solutions detect threats and underscores the importance of using hashes instead of uploading sensitive files.

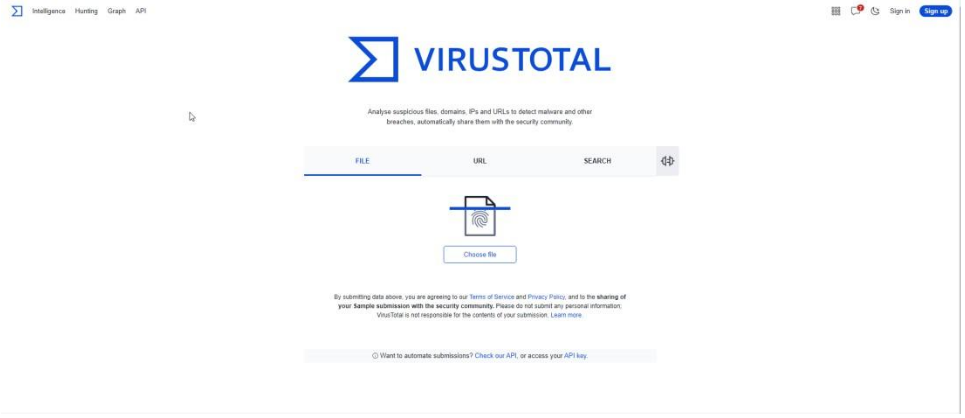
Next, I explored the Any.Run platform, which provides an interactive sandbox environment for analyzing publicly submitted malware samples. This allowed me to observe how different malware interacts with systems, including registry modifications, file changes, network activity, and overall system behavior.

Finally, I analyzed *504lab.exe*, a program designed to mimic malware behavior, to gain a better understanding of how malicious software operates. By investigating its execution, I can identify key behavioral patterns and learn techniques for detecting and mitigating potential threats.

This lab enhanced my ability to recognize and analyze suspicious files, reinforcing best practices for identifying and responding to cybersecurity threats.

ANALYSIS:

Act1. Using VirusTotal to determine if file is malicious

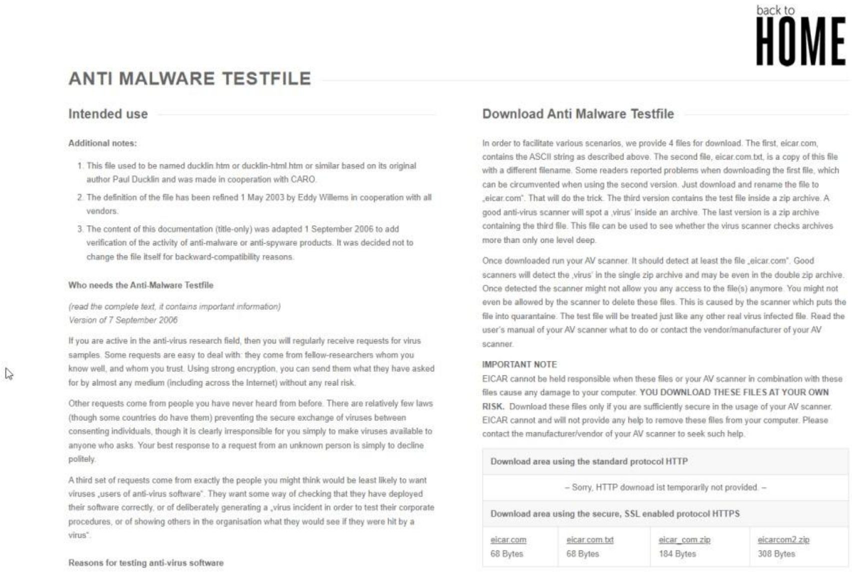


Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, or access your API key.

Download the éclair file



ANTI MALWARE TESTFILE

Intended use

Additional notes:

1. This file used to be named ducklin.htm or ducklin-html.htm or similar based on its original author Paul Ducklin and was made in cooperation with CARO.
2. The definition of the file has been refined 1 May 2003 by Eddy Willems in cooperation with all vendors.
3. The content of this documentation (title-only) was adapted 1 September 2006 to add verification of the activity of anti-malware or anti-spyware products. It was decided not to change the file itself for backward-compatibility reasons.

Who needs the Anti-Malware Testfile

(read the complete text, it contains important information)
Version of 7 September 2006

If you are active in the anti-virus research field, then you will regularly receive requests for virus samples. Some requests are easy to deal with: they come from fellow-researchers whom you know well, and whom you trust. Using strong encryption, you can send them what they have asked for by almost any medium (including across the Internet) without any real risk.

Other requests come from people you have never heard from before. There are relatively few laws (though some countries do have them) preventing the secure exchange of viruses between consenting individuals, though it is clearly irresponsible for you simply to make viruses available to anyone who asks. Your best response to a request from an unknown person is simply to decline politely.

A third set of requests come from exactly the people you might think would be least likely to want viruses „users of anti-virus software". They want some way of checking that they have deployed their software correctly, or of deliberately generating a „virus incident in order to test their corporate procedures, or of showing others in the organisation what they would see if they were hit by a virus".

Reasons for testing anti-virus software

Download Anti Malware Testfile

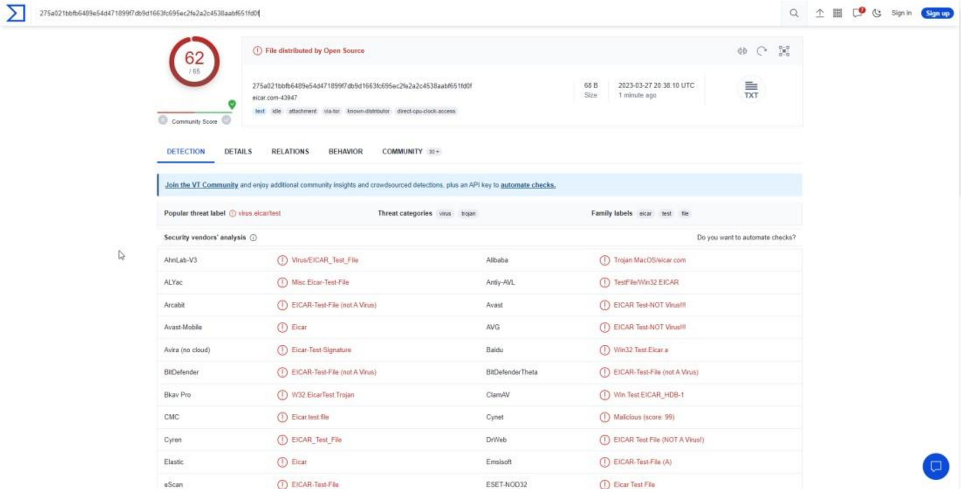
In order to facilitate various scenarios, we provide 4 files for download. The first, eicar.com, contains the ASCII string as described above. The second file, eicar.com.txt, is a copy of this file with a different filename. Some readers reported problems when downloading the first file, which can be circumvented when using the second version. Just download and rename the file to „eicar.com". That will do the trick. The third version contains the test file inside a zip archive. A good anti-virus scanner will spot a ‚virus' inside an archive. The last version is a zip archive containing the third file. This file can be used to see whether the virus scanner checks archives more than only one level deep.

Once downloaded run your AV scanner. It should detect at least the file „eicar.com". Good scanners will detect the ‚virus' in the single zip archive and may be even in the double zip archive. Once detected the scanner might not allow you any access to the file(s) anymore. You might not even be allowed by the scanner to delete these files. This is caused by the scanner which puts the file into quarantaine. The test file will be treated just like any other real virus infected file. Read the user's manual of your AV scanner what to do or contact the vendor/manufacturer of your AV scanner.

IMPORTANT NOTE
EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. **YOU DOWNLOAD THESE FILES AT YOUR OWN RISK.** Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

Download area using the standard protocol HTTP			
– Sorry, HTTP downoad ist temporarily not provided. –			
Download area using the secure, SSL enabled protocol HTTPS			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

Results of scan



275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f

62 / 65

Community Score

File distributed by Open Source

275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
eicar.com-43947
text idle attachment via-tor known-distributor direct-cpu-clock-access

68 B Size

2023-03-27 20:38:10 UTC
1 minute ago

TXT

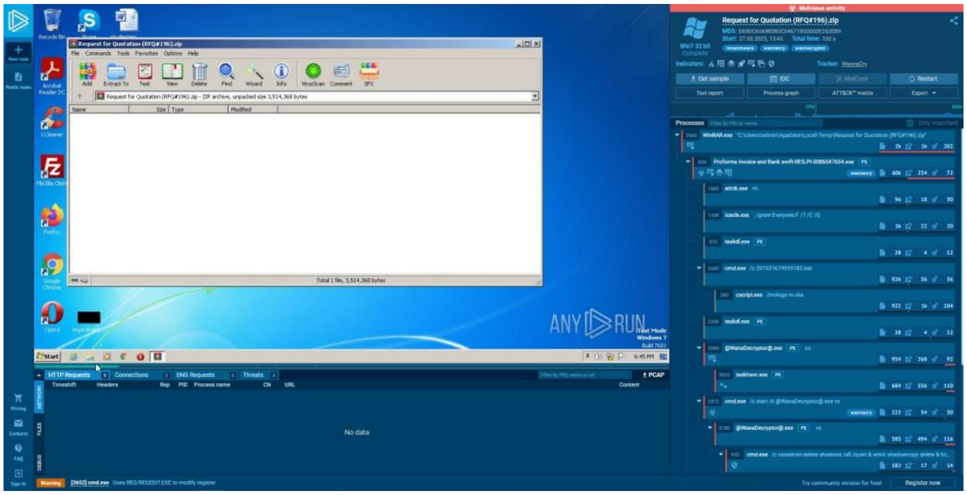
Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label virus.eicar/test | Threat categories virus trojan | Family labels eicar test file

Security vendors' analysis | Do you want to automate checks?

AhnLab-V3	Virus/EICAR_Test_File	Alibaba	Trojan:MacOS/eicar.com
ALYac	Misc.Eicar-Test-File	Antiy-AVL	TestFile/Win32.EICAR
Arcabit	EICAR-Test-File (not A Virus)	Avast	EICAR Test-NOT Virus!!!
Avast-Mobile	Eicar	AVG	EICAR Test-NOT Virus!!!
Avira (no cloud)	Eicar-Test-Signature	Baidu	Win32.Test.Eicar.a
BitDefender	EICAR-Test-File (not A Virus)	BitDefenderTheta	EICAR-Test-File (not A Virus)
Bkav Pro	W32.EicarTest.Trojan	ClamAV	Win.Test.EICAR_HDB-1
CMC	Eicar.test.file	Cynet	Malicious (score: 99)
Cyren	EICAR_Test_File	DrWeb	EICAR Test File (NOT A Virus!)
Elastic	Eicar	Emsisoft	EICAR-Test-File (A)
eScan	EICAR-Test-File	ESET-NOD32	Eicar Test File

Act2. Examine publicly submitted samples on the AnyRun platform



Request for Quotation (RFQ#196).zip
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
Name Size Type Modified
ANY RUN
Test Mode
Windows 7
Build 7601
Start
HTTP Requests
Connections
DNS Requests
Threats
PCAP
No data

Request for Quotation (RFQ#196).zip - ZIP archive, unpacked size 3,514,368 bytes

Total 1 file, 3,514,368 bytes

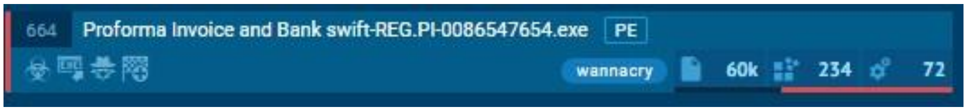
Malicious activity

Request for Quotation (RFQ#196).zip
Start: 27.03.2023, 13:45 Total time: 102 s
Win7 32 bit Complete
ransomware wannacry wannacryptor
Tracker: WannaCry

```
WinRAR.exe "C:\Users\admin\AppData\Local\Temp\Request for Quotation (RFQ#196).zip"   2k 1k 202
  Proforma Invoice and Bank swift-REG.PI-0086547654.exe PE   wannacry 60k 234 72
    attrib.exe +h                                              96 18 30
    icacls.exe ./grant Everyone:F /T /C /Q                     1k 22 20
    taskdl.exe PE                                              28 4 12
    cmd.exe /c 201531679939183.bat                             926 36 36
      cscript.exe //nologo m.vbs                               922 1k 104
    taskdl.exe PE                                              28 4 12
    @WanaDecryptor@.exe PE co                                  954 268 92
      taskhsvc.exe PE                                          684 556 110
    cmd.exe /c start /b @WanaDecryptor@.exe vs        wannacry 222 34 30
      @WanaDecryptor@.exe PE vs                                585 494 116
        cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bc...   182 17 14
```

Warning [3652] cmd.exe Uses REG/REGEDIT.EXE to modify register

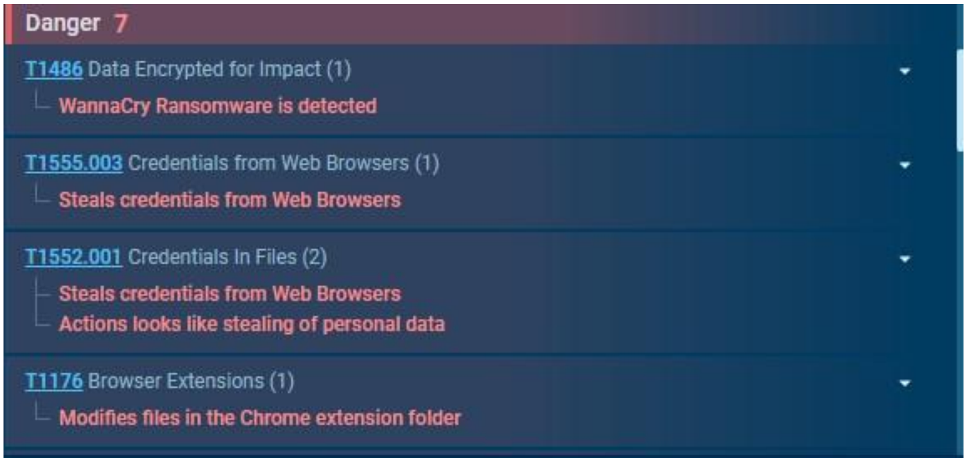
Looking at this capture it appears to be a ransomware executable file. The file posing as an invoice however it is actuall a wannacry executable file.



664 Proforma Invoice and Bank swift-REG.PI-0086547654.exe PE

wannacry 60k 234 72

It appears to steal credentials and personal data from the machine.



Danger 7

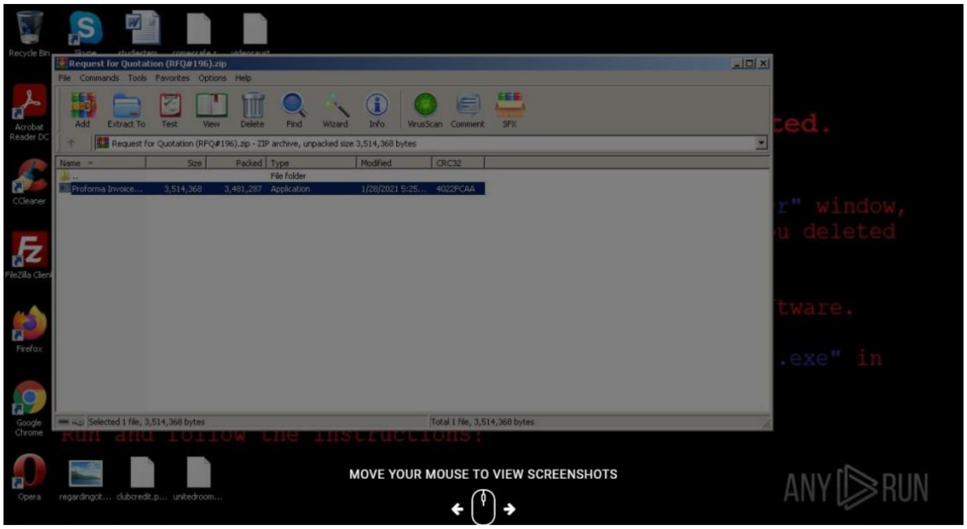
T1486 Data Encrypted for Impact (1)
- WannaCry Ransomware is detected

T1555.003 Credentials from Web Browsers (1)
- Steals credentials from Web Browsers

T1552.001 Credentials In Files (2)
- Steals credentials from Web Browsers
- Actions looks like stealing of personal data

T1176 Browser Extensions (1)
- Modifies files in the Chrome extension folder

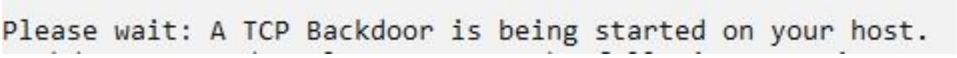
It then encrypts them.


Recycle Bin
Skype
Acrobat Reader DC
CCleaner
FileZilla Client
Firefox
Google Chrome
Opera
Request for Quotation (RFQ#196).zip
File Commands Tools Favorites Options Help
Add
Extract To
Test
View
Delete
Find
Wizard
Info
VirusScan
Comment
SFX
Request for Quotation (RFQ#196).zip - ZIP archive, unpacked size 3,514,368 bytes
Name
Size
Packed
Type
Modified
CRC32
File folder
Proforma Invoice... 3,514,368 3,481,287 Application 1/28/2021 5:25... 4022FCAA
Selected 1 file, 3,514,368 bytes
Total 1 file, 3,514,368 bytes
MOVE YOUR MOUSE TO VIEW SCREENSHOTS
ANY RUN

Act 3. On a Windows based machine run and analyze the 504lab.exe file

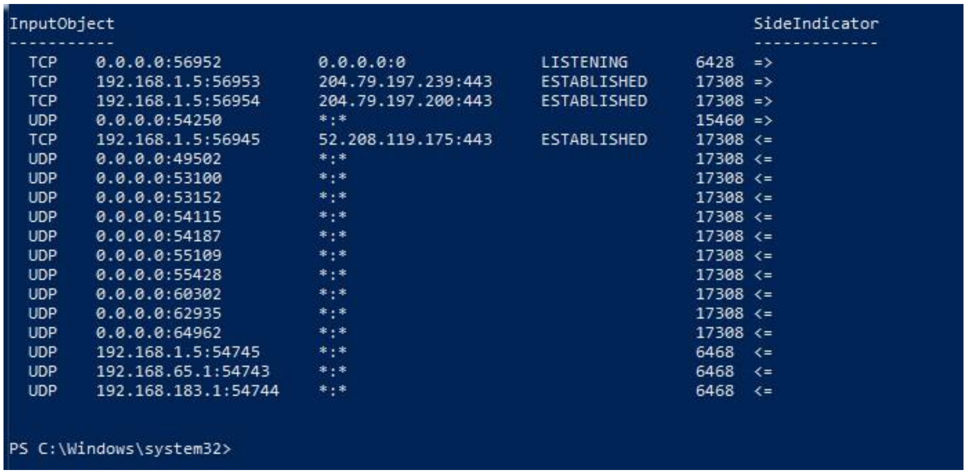
Download the 504lab.exe file.

Run the File. It should start a TCP backdoor.



```
Please wait: A TCP Backdoor is being started on your host.
```

Using Netstat you should be able to see the process that it is running on.



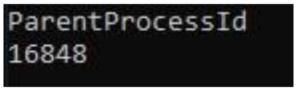
```
InputObject                                                                 SideIndicator
-----------                                                                 -------------
  TCP    0.0.0.0:56952          0.0.0.0:0              LISTENING       6428  =>
  TCP    192.168.1.5:56953      204.79.197.239:443     ESTABLISHED     17308 =>
  TCP    192.168.1.5:56954      204.79.197.200:443     ESTABLISHED     17308 =>
  UDP    0.0.0.0:54250          *:*                                    15460 =>
  TCP    192.168.1.5:56945      52.208.119.175:443     ESTABLISHED     17308 <=
  UDP    0.0.0.0:49502          *:*                                    17308 <=
  UDP    0.0.0.0:53100          *:*                                    17308 <=
  UDP    0.0.0.0:53152          *:*                                    17308 <=
  UDP    0.0.0.0:54115          *:*                                    17308 <=
  UDP    0.0.0.0:54187          *:*                                    17308 <=
  UDP    0.0.0.0:55109          *:*                                    17308 <=
  UDP    0.0.0.0:55428          *:*                                    17308 <=
  UDP    0.0.0.0:60302          *:*                                    17308 <=
  UDP    0.0.0.0:62935          *:*                                    17308 <=
  UDP    0.0.0.0:64962          *:*                                    17308 <=
  UDP    192.168.1.5:54745      *:*                                    6468  <=
  UDP    192.168.65.1:54743     *:*                                    6468  <=
  UDP    192.168.183.1:54744    *:*                                    6468  <=


PS C:\Windows\system32>
```

Find the process id number of the backdoor.

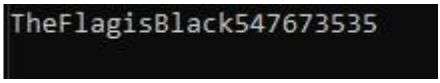
6428

Find the parent process using “wmic proceess where (processid = 6428) get parentprocessid ”



```
ParentProcessId
16848
```

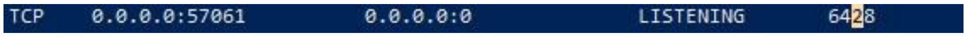
Use netcat ot connect to the backdoor TCP port using nc 127.0.0.1 56952



```
TheFlagisBlack547673535
```

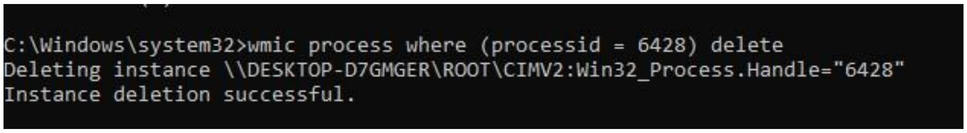
is returned

Use netstat –nao again to see what it is listening on now. It should display a different port.



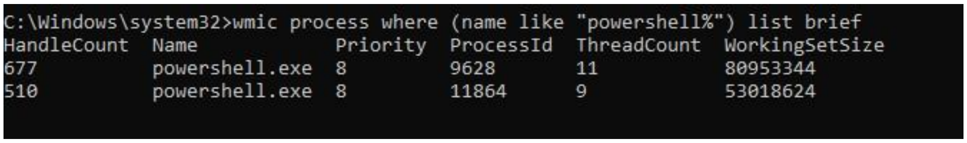
```
TCP    0.0.0.0:57061          0.0.0.0:0              LISTENING       6428
```

Use wmic to kill the process

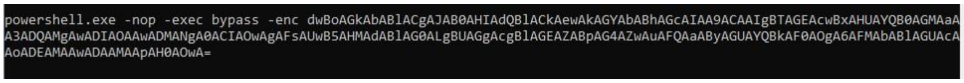


```
C:\Windows\system32>wmic process where (processid = 6428) delete
Deleting instance \\DESKTOP-D7GMGER\ROOT\CIMV2:Win32_Process.Handle="6428"
Instance deletion successful.
```

New Process is created that isn't listen on a port.



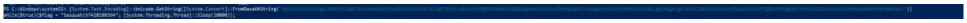
```
C:\Windows\system32>wmic process where (name like "powershell%") list brief
HandleCount  Name            Priority  ProcessId  ThreadCount  WorkingSetSize
677          powershell.exe  8         9628       11           80953344
510          powershell.exe  8         11864      9            53018624
```



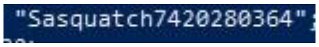
```
powershell.exe -nop -exec bypass -enc dwBoAGkAbABlACgAJAB0AHIAdQBlACkAewAkAGYAbABhAGcAIAA9ACAAIgBTAGEAcwBxAHUAYQB0AGMAaA
A3ADQAMgAwADIAOAAwADMANgA0ACIAOwAgAFsAUwB5AHMAdABlAG0ALgBUAGgAcgBlAGEAZABpAG4AZwAuAFQAaAByAGUAYQBkAF0AOgA6AFMAbABlAGUAcA
AoADEAMAAwADAAMAApAH0AOwA=
```

Decode

A final flag with sasquache will be displayed.

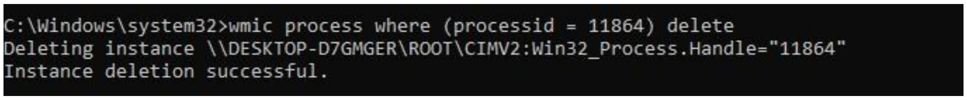


```
PS C:\Windows\system32> [System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String('[illegible]'))
while($true){$flag = "Sasquatch7420280364"; [System.Threading.Thread]::Sleep(10000)};
```

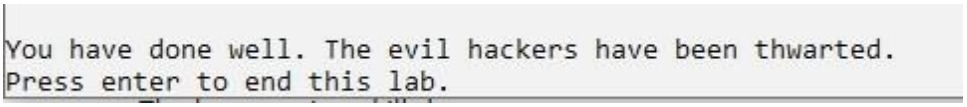


```
"Sasquatch7420280364";
```

The last step is to kill the process.



```
C:\Windows\system32>wmic process where (processid = 11864) delete
Deleting instance \\DESKTOP-D7GMGER\ROOT\CIMV2:Win32_Process.Handle="11864"
Instance deletion successful.
```



```
You have done well. The evil hackers have been thwarted.
Press enter to end this lab.
```