**批次處理隱藏運行的11種思路**

1.基礎  
  
HideRun.vbs

1. CreateObject("WScript.Shell").Run "cmd /cD:\test.bat",0

其中D:\test.bat是你的批次處理路徑  
  
HideRun.bat

1. echo CreateObject("WScript.Shell").Run "cmd /cD:\test.bat",0>$tmp.vbs
2. cscript.exe /e:vbscript $tmp.vbs
3. del $tmp.vbs

這個批次處理其實不能使其批次處理本身隱藏，但是下面大部分隱藏調用批次處理的原理和基礎。  
  
HideRun.js

1. new ActiveXObject('WScript.Shell').Run('cmd /cD:\Test.bat',0);

複製代碼

用Javascript有什麼好處呢？js的字串變數可以用單引號，從而方便命令列作為參數調用，而且js很好的支持多行語句用 ; 分隔寫成一行。要注意的是：js要區分大小寫，方法必須用括弧，結尾必須有分號。所以就成了下面的命令：

1. mshta "javascript:new ActiveXObject('WScript.Shell').Run('cmd /cD:\test.bat',0);window.close()"

複製代碼

2.用快捷方式  
  
如果要使一個批次處理本身隱藏，可以參考附件裡的一個快捷方式，修改附件中的相關路徑即可隱藏啟動你的批次處理。可以用vbs來建立一個 .lnk，其實用批次處理也行（先echo一個vbs出來）  
  
3.利用系統服務  
  
可以用sc建立一個系統服務然後啟動這個服務來啟動批次處理。缺點是啟動服務較慢，需要管理員許可權  
查考這個帖子，  
<http://www.cn-dos.net/forum/viewthread.php?tid=21426>  
asbai 兄的大作，極大的方便了我們的使用。

1. runassrv add /cmdline:"C:\Windows\System32\cmd.exe /cD:\test.bat" /name:"mysrv"
2. net start mysrv

複製代碼

4.利用at計畫任務  
  
用at可以建立一個計畫任務，在不輸入 /interactive 參數可以後臺運行。但是建使用at必須有管理員許可權

1. at 09:10 "cmd /cD:\Test.bat"

複製代碼

然後在 9:10 系統就會自動後臺以SYSTEM許可權運行這個bat  
  
5.利用ftype檔關聯  
  
綜合上面的技術，使所有批次處理都隱藏運行

1. ftype batfile=C:\Windows\System32\mshta "javascript:new ActiveXObject('WScript.Shell').Run('cmd /c%1',0);window.close();"

複製代碼

大家可以討論下下面的思路，目前沒有明確的方法，但是理論上是可行的  
  
6.rundll32  
  
其實這個方法只是理論上估計的，這裡提出來占個位置，留個記號，等待高手研究  
rundll32可以調用 dll 裡的API，如果有個dll可以隱藏run一個exe就可以實現隱藏啟動批次處理，呵呵。目前我也沒找到方法。  
  
7.其他用戶  
  
Windows 2k/XP支持多用戶，如果能在後臺登陸另一個帳戶的桌面然後運行一個批次處理，就能完全達到隱藏的目的  
  
8.bat2vbs  
  
這個方法只是一個不是很成熟的思路。  
查考這個帖子：  
<http://www.cn-dos.net/forum/viewthread.php?tid=20769>  
這使我們產生了一個想法：把bat轉換成vbs，然後vbs生成一個臨時bat檔，然後WScript.Shell.Run隱藏啟動這個臨時bat  
  
9. .NET編譯  
  
參考這個帖子：  
<http://www.cn-dos.net/forum/viewthread.php?tid=23374>  
裡面提到了一個 .NET Warpper，我們完全可以利用系統自帶的元件把bat編譯到 exe 當中。如果bat不涉及交互，exe自然就安靜的運行了。  
  
10.注入彙編  
  
最後向大家推出的今天最隆重的，ASCII Assembly Code專家 Herbert Kleebauer 的又一力作：showwin.exe  
  
showwin.exe let you minimize/maximize/hide the command window  
within a batch program (requires W2k or better).  
  
Usage:  showwin.exe number  
  
0 SW\_HIDE  
   Hides the window and activates another window.  
  
1 SW\_SHOWNORMAL  
   Activates and displays a window. If the window is minimized or maximized,  
   the system restores it to its original size and position. An application  
   should specify this flag when displaying the window for the first time.  
  
2 SW\_SHOWMINIMIZED  
   Activates the window and displays it as a minimized window.  
  
3 SW\_MAXIMIZE  
   Maximizes the specified window.  
  
3 SW\_SHOWMAXIMIZED  
   Activates the window and displays it as a maximized window.  
  
4 SW\_SHOWNOACTIVATE  
   Displays a window in its most recent size and position. This value is  
   similar to SW\_SHOWNORMAL, except the window is not actived.  
  
5 SW\_SHOW  
   Activates the window and displays it in its current size and position.  
  
6 SW\_MINIMIZE  
   Minimizes the specified window and activates the next top-level window  
   in the Z order.  
  
7 SW\_SHOWMINNOACTIVE  
   Displays the window as a minimized window. This value is similar to  
   SW\_SHOWMINIMIZED, except the window is not activated.  
  
8 SW\_SHOWNA  
   Displays the window in its current size and position. This value is  
   similar to SW\_SHOW, except the window is not activated.  
  
9 SW\_RESTORE  
   Activates and displays the window. If the window is minimized or maximized,  
   the system restores it to its original size and position. An application  
   should specify this flag when restoring a minimized window.  
  
10 SW\_SHOWDEFAULT  
   Sets the show state based on the SW\_ value specified in the STARTUPINFO  
   structure passed to the CreateProcess function by the program that  
   started the application.  
  
11 SW\_FORCEMINIMIZE  
   Windows 2000/XP: Minimizes a window, even if the thread that owns the  
   window is not responding. This flag should only be used when minimizing  
   windows from a different thread.  
  
---------------------------------------------------------------------------  
  
A simple example:

1. :::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::::-:
2. @echo off
3. echo Bj@jzh`0X-`/PPPPPPa(DE(DM(DO(Dh(Ls(Lu(LX(LeZRR]EEEUYRX2Dx=>showwin.com
4. echo 0DxFP,0Xx.t0P,=XtGsB4o@$?PIyU WwX0GwUY Wv;ovBX2Gv0ExGIuht6>>showwin.com
5. echo T}{zE~@gwkBG@OEKcUt`E}@mqqBsy?seHBEaPhxr?@zAB`LrPEyoDt@Cj?>>showwin.com
6. echo pky\_jN@QEKpEt@ij?jySjN@REKpEt@jj?jyGjN@SEKkjtlGuNw?p@pjirz>>showwin.com
7. echo FEvAUSQ?\_YLTQ@@?~QCo\_F~RDU@?aU?@MQ\_AMy1GHs?Gw`LbLK@shM`S\_d>>showwin.com
8. echo bD\_nsDddlTr\_sPdlnTcnaTv\_xP\_ngD\_rhDhsrT\_kkDhrtT\_fmDRNCTILk?>>showwin.com
9. echo staThg\_So\_rPfnqTl`qTdq\_ShtpTrdqThV\_Sqrm@ILm?O?cOKFDP?@@?dx>>showwin.com
10. echo OdFUu?N?\_B@J@??KD?HUA?QOGB\_QO?F?SCAQO?UDF?UCE?Q\_F?DUA?CUB?>>showwin.com
11. echo OFO?FOS?DUO?IUO?FOW?RU{OWFO?mYU?wdsTeQs@OQ@?QAQ?LUA?\_F\_og~>>showwin.com
12. echo UODUO?FOSAFOeAUOyAO\_DCSHUOOQO?OCFGuHUOGFO?TUO?DRTTqrQ@kcmS>>showwin.com
13. echo gFkPFUO?ngRThVvTncmTJFvPMQDTrKDDcmqOFkkDFOSAFOeAUOyAdFFSnB>>showwin.com
14. echo sT`llTKcmTdmhTFQ@PBsdTrmnTdknTmhVTvncTwDSSOshTbnqTrrdTT~?K>>showwin.com
15. echo ?OGOQp?o??Gds?wOw?PGAtaCHQvNntQv\_w?A?it\=upkNQD??OuQsQG[i?>>showwin.com
16. echo RwrqosHy?Mjmv\@IuBlpUrHdjNAslF~mH}OKT?U??PT~OL?O?O?i?COT~B>>showwin.com
17. echo U?OCU?YF0x>>showwin.com
18. showwin.com>showwin.exe
19. del showwin.com
20. dir
21. :: wait 4 seconds
22. ping -n 4 localhost >nul
23. :: hide window
24. showwin.exe 0
25. dir /b
26. :: wait 4 seconds
27. ping -n 4 localhost >nul
28. :: show window
29. showwin.exe 5
30. :: wait 4 seconds
31. ping -n 4 localhost >nul
32. del showwin.exe

複製代碼

原帖地址在  
[http://groups.google.com/group/a ... ad/b30d93c7f43b6731](http://groups.google.com/group/alt.lang.asm/browse_thread/thread/b30d93c7f43b6731)  
問題是我後臉皮發的。嘿嘿  
不過我還沒有測試成功。估計是keyboard layout和language/code page不同造成的  
  
  
  
以上10中思路原文地址：<http://www.cn-dos.net/forum/viewthread.php?tid=23846>  
  
11、協力廠商命令列工具nircmd.exe

1. nircmd.exe exec hide "C:\test\BatHome.bat"

複製代碼

下載地址：<http://bbs.bathome.net/thread-3981-1-1.html>