

Forum:[Hack Forums](#)

Thread: [Allow multiple RDP in windows 10 using or c++ \(API, cmd, powershell\)?](#)

Tr0jandog - September 13, 2019, 10:33 am

Powershell empire can do this using mimikatz, but i want a more stealthy way, and want to implement it by my own

there are some articles showing how to do this in windows setting and such, but i want to do it with just cmd, powershell or just using windows APIs in c++

basically as of right now, when i enable the rdp of someone and create another hidden user to connect to, i still cannot connect while the other user is logged in, powershell empire can fix this with mimikatz but i want to implement it just with cmd, powershell or c++, and right now it just says another user is logged on blah blah (even tho its a different user)

anyone has any article or something that i can read more about this?

i think there even should be a way to hook termsrv.dll to do this but i couldnt find anything useful..

ALSO as you can see in this video it is possible to do it with tools : [Allow Multiple Remote Desktop Sessions - Windows 10 - YouTube](#)

but i want to write a tool like that on my own, not use a GUI tool

int main() - September 13, 2019, 1:47 pm

<https://github.com/stascorp/rdpwrap>

Tr0jandog - September 14, 2019, 12:16 am

(Sep 13, 2019 01:47 PM)int main() Wrote: [\[CITE\] GitHub - stascorp/rdpwrap: RDP Wrapper Library](#)

Yes i tried too understand its code but it has too much unnecessary stuff and gui stuff in it that i dont need, was wondering if there is any blogpost or something that goes in depth into doing it and explains what are we doing?

or maybe has implemented other method? i think doing DLL injection and IAT hooking should be possible here (IAT hooking of termsrv.dll) but couldnt find anything regarding this

int main() - September 14, 2019, 12:41 am

(Sep 14, 2019 12:16 AM)Tr0jandog Wrote: [\[CITE\]](#) Yes i tried too understand its code but it has too much unnecessary stuff and gui stuff in it that i dont need, was wondering if there is any blogpost or something that goes in depth into doing it and explains what are we doing?

or maybe has implemented other method? i think doing DLL injection and IAT hooking should be possible here (IAT hooking of termsrv.dll) but couldnt find anything regarding this
you mean you want ready to paste code? i don't think so, learn the language and filter out what you dont need, its not hard.

Tr0jandog - September 14, 2019, 12:48 am

(Sep 14, 2019 12:41 AM)int main() Wrote: [\[CITE\]](#) you mean you want ready to paste code? i don't think so, learn the language and filter out what you dont need, its not hard.

hmm what i said was exactly the opposite, i said i dont want to just copy the github code, want to find some blogpost or something that explains it.. there are many parts of it that i dont understand why they are using certain lines of codes and there is no comment on it, just trying to get it by reading thousands of line of code is pretty hard task if you ask me

Anzee - September 17, 2019, 9:25 pm

(Sep 14, 2019 12:48 AM)Tr0jandog Wrote: [\[CITE\]](#) hmm what i said was exactly the opposite, i said i dont want to just copy the github code, want to find some blogpost or something that explains it.. there are many parts of it that i dont understand why they are using certain lines of codes and there is no comment on it, just trying to get it by reading thousands of line of code is pretty hard task if you ask me

You should have looked into it a bit more.

According to <https://forums.mydigitallife.net/threads/discussion-windows-10-termsrv-dll-patching.57102/> you can patch termsrv.dll manually with a hex editor and achieve multi-session with RDP. A lot of people recommend using RDPConf.exe from RDPWrap to patch and RDPCheck.exe to check the configuration.

Try this and report back.

Tr0jandog - September 17, 2019, 9:34 pm

(Sep 17, 2019 09:25 PM)Anzee Wrote: [\[CITE\]](#) You should have looked into it a bit more.

According to [\[DISCUSSION\] Windows 10 termsrv.dll Patching | My Digital Life Forums](#) you can patch termsrv.dll manually with a hex editor and achieve multi-session with RDP. A lot of people recommend using RDPConf.exe from RDPWrap to patch and RDPCheck.exe to check the configuration.

Try this and report back.

yes i saw that before, the problem with that is messing around and editing system files is a red flag for AVs, but the RDPwrap claims to achieve this without editing that termsrv.dll but doesn't say how

malpwn - September 18, 2019, 2:53 am

This :

[Vincent Yiu on Twitter: "Red Tip #344: Set HKLM\System\CurrentControlSet\Control\TerminalServer /v fSingleSessionPerUser /d 0, to allow multiple sessions on a server per user. This is useful if you want to login to the jump-host, but that guy's just on all-day-long..."](#)

Tr0jandog - September 19, 2019, 10:47 am

(Sep 18, 2019 02:53 AM)malpwn Wrote: [\[CITE\]](#) This :

[Vincent Yiu on Twitter: "Red Tip #344: Set HKLM\System\CurrentControlSet\Control\TerminalServer /v fSingleSessionPerUser /d 0, to allow multiple sessions on a server per user. This is useful if you want to login to the jump-host, but that](#)

[guy's just on all-day-long... "](#)

that doesn't allow multiple concurrent users, you still have to patch it, or at least didnt work for me