

Forum:[Hack Forums](#)

Thread: [Which RAT add exception at Windows firewall?](#)

ciccio - September 14, 2018, 7:10 am

Hi,

I search a RAT with this function:

add your self in autorun;

add an exception for your self at the firewall of windows.

Not necessary UAC bypass or injection.

Now I bypass my request with Install Shield or similar software...but to long and complicate.

Thanks for your help.

Best regards.

Jacque Fresco - September 14, 2018, 7:51 am

(Sep 14, 2018 07:10 AM)ciccio Wrote: [\[CITE\]](#) 1. add your self in autorun;

2. add an exception for your self at the firewall of windows.

1. What do you mean with add to autorun? Do you mean that the RAT should be able to start on Windows start? if yes then almost every RAT does that.

2. choose any rat you like that does the other requirement and then write a little batch script that does create the exeption:

<https://lizardsystems.com/articles/configure-windows-firewall-using-command-line/>

__Digital__ - September 14, 2018, 9:32 am

I would just use powershell to interact with windows firewall and windows defender, you will need andmin or system rights to add exceptions etc

3DES - September 14, 2018, 10:44 am

Adding exception to firewall is retarded and EXTREMELY detected method to bypass firewall.

Jacque Fresco - September 14, 2018, 12:22 pm

(Sep 14, 2018 10:44 AM)3DES Wrote: [\[CITE\]](#) Adding exception to firewall is retarded and EXTREMELY detected method to bypass firewall.

if you say so. I believe that ONLY your method is detected. It is always possible, you just need to dig around ^^

it is for example possible to trick AV's with GUI's and titles likes "install XXX program" with checkboxes like "Implement Rule into the Firewall?" and when ever the user clicks somewhere on the desktop the gui disappears and the implementation takes place. Of course the GUI will never being visible to the user. This is enough to trick a couple of AV's. therefore your "EXTREMELY" is nonsense.

Note: There is always a way in. This is same why it is not possible to make a computer 100% safe.

You can look at my last thread and you will see that i managed it to even uninstall 3 different AV's without any notification to the USER.