

Forum:[Hack Forums](#)

Thread: [Problem with windows caution message on RAT](#)

Revolution99 - July 15, 2016, 4:25 am

Hello ! On my free time, i am creating a personal RAT.... for educational purposes. The problem is that everytime i am running a new version of the server(payload) on a computer of mine, windows ask the user if he wants to permit this program(my payload) to have internet access... which is fucked up because the user can see the RAT payload. What i can do for this ?? Thanks.

Vuln - July 15, 2016, 5:43 am

How are you downloading, updating and executing it? And what's causing the warning message? SmartScreen? Defender? Firewall?

Revolution99 - July 15, 2016, 7:30 am

What do you mean ? I click the server, and the server extracts the real server in the appdata folder, and execute it. I managed to take an photo of the windows "exception":

[prntscr.com/bt9sr9](#)

Vuln - July 15, 2016, 7:58 am

(Jul 15, 2016 07:30 AM)Revolution99 Wrote: [\[CITE\]](#) What do you mean ? I click the server, and the server extracts the real server in the appdata folder, and execute it. I managed to take an photo of the windows "exception":

[prntscr.com/bt9sr9](#)

My bad, I thought you were talking about a remote update feature.

With the default Windows Firewall settings only the server (the controller) should be seeing that warning message, not the client (which you seem to be calling server).

You might want to take a look at [xSilent's socket programming videos](#). And are you using a reverse connection?

Revolution99 - July 15, 2016, 11:55 am

No, i am seeing this message in the client too(server)... and that's because the server send back information to me...

Ofcourse i use "reverse connection"... this is how i make the connection between server-client.

Vuln - July 15, 2016, 4:15 pm

(Jul 15, 2016 11:55 AM)Revolution99 Wrote: [\[CITE\]](#) No, i am seeing this message in the client too(server)... and that's because the server send back information to me...

Ofcourse i use "reverse connection"... this is how i make the connection between server-client. Windows Firewall allows outbound connections by default. Unless a custom rule or policy is blocking it, there is something wrong with your code. So why don't you share it?

Revolution99 - July 16, 2016, 1:35 am

This is the link for the client: [sendspace.com/file/i6oh4f](#)

?he password is: revolution

Note that i code this only in 1 day... so it's on a really really early stage and is fucked up.

Vuln - *July 16, 2016, 6:03 am*

The controller (server) should be listening on an open port, and the client (your payload project) should be connecting to it. That way the client will bypass the default firewall restrictions, and it moves the burden of port forwarding from the client to the server. But you're doing it the other way around.

Other notes:

- There is no need to rely on a webservice to retrieve the public IP. There's `Socket.RemoteEndPoint` for that.
- Instead of using `ShowWindow` to somewhat hide the console window, you can simply change its output type (Properties>Application>Output type) to Windows Application.
- You should try to avoid deprecated/absolute methods like the `TcpListener(Int32)` constructor, unless you know what you're doing.