

Forum:[Hack Forums](#)

Thread: [What protocol do rats use and how do they work.](#)

will is god - April 19, 2017, 6:27 pm

Hi, ive made my own rat with c# using tcp/ip. Ive noticed this only works if the victim is on the same network as me. I use their ipv4 address to connect to their computer.

Do rats genrally use tcp/ip too? do they require port forwarding? do they port forward automaticly?

What if i put it on a victims computer and port foward, would i then have to connect to their computer using their routers public ip address, but then what happens if they change network, i wont be able to connect to them anymore?

If anyone can help me out with some info id appriciate it

Mr. Kim - April 19, 2017, 7:31 pm

(Apr 19, 2017 06:27 PM)will is god Wrote: [\[CITE\]](#) Hi, ive made my own rat with c# using tcp/ip. Ive noticed this only works if the victim is on the same network as me. I use their ipv4 address to connect to their computer.

Do rats genrally use tcp/ip too? do they require port forwarding? do they port forward automaticly?

What if i put it on a victims computer and port foward, would i then have to connect to their computer using their routers public ip address, but then what happens if they change network, i wont be able to connect to them anymore?

If anyone can help me out with some info id appriciate it

If you want to "call in" they will need to forward the ports. If, however, they "call back" to you then you port forward. RATs have the clients connect back to them, preventing any need to forward ports on the client's machine.

will is god - April 19, 2017, 7:38 pm

Wouldnt that mean i would have to put my ip in the program? so the client knows where to call me

Not Your Average Orange - April 19, 2017, 7:48 pm

(Apr 19, 2017 07:38 PM)will is god Wrote: [\[CITE\]](#) Wouldnt that mean i would have to put my ip in the program? so the client knows where to call me

I'm not a rat dev but I think that's one of the reasons why you crypt a stub, so the victim doesn't see the source code. Also, you could use a VPN.

will is god - April 19, 2017, 7:52 pm

yeh i could eaiser use an anti decompiler but my main worry was what if my ip changes? i would lose their connection forever?

Elite Hacker 69 - April 19, 2017, 7:54 pm

(Apr 19, 2017 07:48 PM)Not Your Average Orange Wrote: [\[CITE\]](#) I'm not a rat dev but I think that's one of the reasons why you crypt a stub, so the victim doesn't see the source code. Also, you could use a VPN.

Well pretty sure you crypt a stub so antiviruses can't detect patterns that viruses have.

'Cynical - April 19, 2017, 8:10 pm

(Apr 19, 2017 07:52 PM)will is god Wrote: [\[CITE\]](#) yeh i could eaiser use an anti decompiler but my main worry was what if my ip changes? i would lose their connection forever?

This is where DNS applications like DynDNS come into play.

Basically setup a domain that automatically propagates to your new IP if your IP changes.

will is god - April 19, 2017, 8:18 pm

(Apr 19, 2017 08:10 PM)Cynical Wrote: [\[CITE\]](#) This is where DNS applications like DynDNS come into play.

Basically setup a domain that automatically propagates to your new IP if your IP changes.

hmm ok i get the jist of this, Is there any alternatives to changing your ip on their machine? I was thinking i could set up a website with a free domain where the only thing on the page was my ip, that way the client could eaisily set up a new http request or whatever it is and read it html code, trim the string and use that and from there and i could change it from my end. Problem is, if the website goes down im back to square one.

I was also thinking of an email address where the client reads the latest email which would just contain my ip address and i could just send a new email to that address whenever i get a new ip, problem is with gmail is that it will flag as suspicious when someone logs in from a place outside your location area and not let the client read anything in the inbox

Im not trying program a professional rat or anything, just something that works and is semi reliable

Mr. Kim - April 20, 2017, 6:01 am

(Apr 19, 2017 07:38 PM)will is god Wrote: [\[CITE\]](#) Wouldnt that mean i would have to put my ip in the program? so the client knows where to call me

Yes, that's what it means. It's not ideal but there's going to be a track back to you if you create or use a RAT.

razorfsh - April 20, 2017, 4:18 pm

(Apr 19, 2017 06:27 PM)will is god Wrote: [\[CITE\]](#) Hi, ive made my own rat with c# using tcp/ip. Ive noticed this only works if the victim is on the same network as me. I use their ipv4 address to connect to their computer.

Do rats genrally use tcp/ip too? do they require port forwarding? do they port forward automaticly?

What if i put it on a victims computer and port foward, would i then have to connect to their computer using their routers public ip address, but then what happens if they change network, i wont be able to connect to them anymore?

If anyone can help me out with some info id appriciate it
Everything on the internet uses at least TCP/IP, if it is to route reliably
(you can use UDP/ICMP, but delivery is by design... flakey)

port forwarding is something you have to understand to program in. it is usually dynamic, since the route may change , or in many cases the host IP changes, both at the client machine & the FW
This means that generally it is the target machine that needs to instigate the connection to get round NAT etc.

Stop thinking about networks and think more about path finding ants, consider the target machine the 'nest', once you have that picture in your head, translate each section of the ants journey to networking.

tcsh - April 20, 2017, 4:26 pm

It's actually pretty simple, most rats use a reverse connection - TCP/IP.

This means the client (the stub running on the target computer) will call to a specific ip address on a specific port - hence you don't need to port forward or mess around with the firewall on the client end.

The server (you, who's listening on the port for a connection) accept the call the client makes and establish a connection.

Since you're the one listening, you need to have the port open so the communication can take place, hence you need to portforward and stuff.

Now, if you don't want your IP to be in the client, or if you have a dynamic IP address that keeps changing, then you need to implement DNS in your rat / client. This way, the client calls the DNS (hostname) - not your IP.

Then, on your end you need to host something to sync up your IP address (regardless which one it is at that time) with the DNS hostname you provided the client.

Hence, you use services like no-ip, dyndns and so forth, which provide a utility for you to sync your local ip to the hostname you chose from them.

You can't do this part any other way, the client HAS to call SOMEWHERE or else the connection won't establish.

You don't want your IP in the client? That's fine, you a DNS. However, they will have your IP (the dns service) - because you sync to it, but the client won't know it, unless he monitors tcp/ip connections and then he can see it clearly as night and day.

Since you seem confused about this very basic part I'm assuming you used a public source for your rat and/or are very new to them and still learning stuff out. Either way, you should really read up on the basics and understand the functionality before trying to run a RAT, regardless if you use a public source or your own. Heck, it's more difficult using a public source because you have to learn the original coders thinking and style, most of the time, aside from the actual rat basics in your language of choice and so forth.

And to address your second post, I find it more of a hassle to try stuff like email, free websites and so forth. At this point your easiest option is a DNS service. If you don't want to use one available, make your own ;)

Hope I helped :)

Capt. Murphy - April 20, 2017, 4:53 pm

I haven't read all the responses you got, and I dare state the obvious, but start a vm with some decompiling tools and check the code out of some free RAT... Nothing too new tho as it may escape the vm.

--Edit: Nevermind. Obviously the code will be encoded. I don't deal with RATs, but I figured that would be a basic step in avoiding re... Stupid me...

Asdethprime - April 21, 2017, 2:51 am

TCP/IP is the protocol that you would be using, after all the program (RAT) has to communicate information.

If you are worried about giving out your IP you can get the RAT to email you the needed information instead. That is , if you are using the RAT for information gathering rather than taking control of their machine.

Stitch is actually quite a good , free framework, that might be useful to you.

<https://github.com/nathanlopez/Stitch>

Another very good platform for building malwares and experimenting with them is Metasploit Venom (msfvenom) which is free and reliable.

Use something like Veil Evasion for encoding.

PlaySkool - April 21, 2017, 4:03 pm

Something that hasn't been mentioned is that features like desktop streaming, mic capture, and webcam streaming should use UDP, not TCP. A dual socket setup is recommended.

The reason for this is that TCP resends dropped packets, which makes sense for data, but for streams such as video and audio, it's much better to miss a couple frames than it is to pause for a 5 second buffer.