

Anonymous RAT setup for dummies

As you all know, the major hazard of reverse-connecting RATs is they have to connect right back to you. And you won't always stay under the radar of system administrators. So use a VPN you say! VErY good. Except that most VPNs do not permit port forwarding of your external IP in a way that can be reliably used for reverse connecting backdoors. So what is an aspiring hacker to do? Get a VPS.

A VPS is a Virtual Private Server. A virtual server rented out to you that YOU control. You can turn it into a proxy, a VPN gateway, or simply just have it forward RAT connections to your computer. Obviously you will want an off-shore VPS that accepts anonymous payment methods like Bitcoins. You will set the dynamic dns of your RAT slaves to your VPS server, so all your RATs connect to the VPS server, thus only exposing its address and not your home IP. That way, if LEA comes looking for you, they'll hopefully hit a dead end at your VPS hoster. The paranoid shield themselves with a VPN while having RAT connections forwarded to them by the VPS. But not everyone has the money....

YOU don't have to be picky about the VPS's features, so long as it can run a barebones linux command line, that should be enough. The magic lies in SSH port forwarding, a seriously underused technique. Now Putty is a nice lightweight SSH client, so let's use that. After connecting to your VPS via SSH, in Putty, open up the menu, and click "change settings". In the window that opens, find the Connections, SSH, Tunnels. We will set up SSH Port Tunneling with the VPS so it forwards connections it receives to your computer inside the encrypted SSH connection. Don't forget to set GatewayPorts to 'yes' in sshd_config file on your VPS. This configures the SSH daemon on the VPS to bind to the proper interface and forward connections on those ports back to you when you SSH into the box. Without that, you won't be getting any connections.

So, in the Putty options for SSH port forwarding, you want a remote port forward. Source port is whatever your RAT communication port is. Destination port will be localhost:N, where N is your RAT communication port. Click add, then apply. (Note: it is assumed that future versions of Putty will work more or less in this manner. IF confused, just google SSH remote port forward.) For example, if we use port 53, you should see R53 localhost:53 somewhere on that window.

And that's it. Any RAT slaves connecting to your VPS is forwarded to your computer where your client is running, and you can hack away, safely knowing that should any authorities decide to raid "you", they will have come halfway around the world for nothing. I don't know about you, but that sure puts a smile on my face XD.

So in essence, pick any VPS you like and SSH port forward. That is pretty much the easiest way to run a RAT with an anonymous setup.

Spread this guide as far and wide as you can. Too many hackers being caught for stupidity these days. Learn to be Anonymous, or you will all die.