

Forum:[Hack Forums](#)

Thread: [\[TUTORIAL\] How to RAT without port-forwarding or dynamic DNS](#)

csprv - April 13, 2019, 6:07 am

I wrote a program that lets you RAT safely without needing any port-forwarding or dynamic DNS. Basically it works like this:

- 1) The ratter (you ... duh) creates a Tor hidden service (you only need Tor for that) and configure it to forward data from the open HTTP port (80) to your RAT server (instead of a web server like you'd usually do).
- 2) The victim runs my program (I call it InfiltraTOR ... shut up, it's a great name) and it extracts the Tor client binaries and the RAT client to the victim's Temp folder.
- 3) InfiltraTOR starts TOR and starts a connection to your hidden service, connecting using Tor's SOCKS5 proxy.
- 4) InfiltraTOR starts a local TCP server and then starts the RAT client which connects to the TCP server (instead of a dynamic dns).
- 5) InfiltraTOR forwards data from the RAT client to Tor.
- 6) Your hidden service can now communicate with your RAT securely since it's been anonymized through Tor, and sends the data to your RAT server. Voila! You've now connected to your victim without needing to port-forward or get a dynamic DNS.

The downsides to this are that it adds 5MB of Tor binaries to the RAT client (or rather, the RAT client launcher) (this could be reduced to 50KB or even less, but I'm not smart enough to write my own Tor client), and also the Tor network can be kinda slow. Here is the source code (pastebin.com/dmjitUdZ). It's pretty hacky (it shows a console window ffs I'm still working on it. It's not good enough for real life ratting yet) but all you need to do is put it in a project, add the official Tor expert bundle zip file (dist.torproject.org/torbrowser/8.0.8/tor-win32-0.3.5.8.zip) as a resource named "tor", add your RAT client set up to connect to 127.0.0.1:1234 (1234 can be changed easily in the source code. There's a bunch of settings at the top, including the hidden service which you'll need to change to your hidden service) as a resource named "rat", build it, and send it to your victims (after creating a hidden service of course) aaand badabing badaboom you get a slave!

GraeskMytologi - April 13, 2019, 4:07 pm

(Apr 13, 2019 06:07 AM)csprv Wrote: [\[CITE\]](#) 4) InfiltraTOR starts a local TCP server and then starts the RAT client which connects to the TCP server (instead of a dynamic dns).

Running a server to communicate with client on the same machine 1000000 IQ ?
Also this whole tor thing has been done before

RRSS - April 13, 2019, 4:11 pm

(Apr 13, 2019 06:07 AM)csprv Wrote: [\[CITE\]](#) 6) Your hidden service can now communicate with your RAT securely since it's been anonymized through Tor, and sends the data to your RAT server. Voila! You've now connected to your victim without needing to port-forward or get a dynamic DNS. "anonymized through Tor"

how cute and naive xD

One - April 14, 2019, 8:11 am

Check out www.support-office.live

SIM-4199941 - April 14, 2019, 8:54 am

just use a offshore vpn with dedicated ip and pdf exploit

and a good crypter
and you're done

csprv - April 14, 2019, 11:48 am

(Apr 13, 2019 04:07 PM)GraeskMytologi Wrote: [\[CITE\]](#) Running a server to communicate with client on the same machine 1000000 IQ ?

Also this whole tor thing has been done before

Is there a program for that? Cause I was looking for one and I could only find ones that use drivers/use VPNs/don't run on Windows.

(Apr 13, 2019 04:11 PM)RRSS Wrote: [\[CITE\]](#) "anonymized through Tor"

how cute and naive xD
rawr xD :3

NERO - April 14, 2019, 11:53 am

You literally make no sense whatsoever.

That ain't gonna make you anonymous.

GraeskMytologi - April 14, 2019, 12:22 pm

(Apr 14, 2019 11:48 AM)csprv Wrote: [\[CITE\]](#) Is there a program for that? Cause I was looking for one and I could only find ones that use drivers/use VPNs/don't run on Windows.

Don't know if there are any around now, but you could always just code your own.

There's even alternatives to packing tor in the binary such as tor2web, just make sure to encrypt traffic if you choose to go that way unless you want the relays to be able to read it

LordDragon - April 14, 2019, 12:53 pm

(Apr 14, 2019 08:54 AM)salegrosso Wrote: [\[CITE\]](#) just use a offshore vpn with dedicated ip and pdf exploit

and a good crypter
and you're done
Thanks for this

Iera Namhorun - April 14, 2019, 8:01 pm

thank you for this Tor listener, I have been looking for this for a long time.

I need it to connect my c# application to a website on the Tor network.