

Forum:[Hack Forums](#)

Thread: [\[FREE GUIDE\] How to Set up Quasar RAT in 2024](#)

ScrubspooF - April 15, 2024, 4:38 pm

Before you get your dick dirty get some protection. Buy a month of Mullvad VPN they do not keep logs.

<https://mullvad.net/>

Make sure you use crypto even though card payment is available.

Install mullvad on your PC

Once protected buy a bulletproof windows RDP from AnonRDP, they do not keep logs.

<http://anonrdp.com/>

You will also need a bulletproof domain for DNS. You can buy a .RU domain without KYC/ID from GreenBullet that can not be taken down and ignores spamhaus reports.

<https://greenbullet.su/cart.php?a=add&domain=register>

After your purchase open up Remote Desktop on your PC and log into your RDP using the information provided

Open windows firewall and disable it.

Open windows security center and add an exception to your downloads folder

Download Quasar on to your windows RDP and extract it to its own folder

<https://github.com/quasar/Quasar/releases/tag/v1.4.1>

Open Quasar RAT

Click "Create" inside the Certification Wizard. Click save. You only need to create a certificate once.

Click "Settings" at the top of Quasar and set your listening port. We are going to use port 2024 as an example. Click "Start Listening". Save.

Now the RAT is ready to accept new connections from clients.

Now we need to create a payload. Click "Builder" at the top of Quasar.

Leave Everything on Basic Settings tab as is.

Now go back to GreenBullet and create an "A record" to point your domain to the IP address of your VPS. This is in case your VPS IP changes, so you won't lose your clients you can update your IP again on GreenBullet in the future.

Now go back to Quasar on your RDP. Click "Connection Settings" Tab. Enter the domain you bought from GreenBullet into the IP/Domain box and set your port to what we set it to earlier (2024).

DO NOT TOUCH ANY OTHER BUILD SETTINGS.

Click "Build Client" at the bottom. Select the file name and save location for your unencrypted payload.

Now go to where you saved the payload and make a copy of that file. Run the copied file. You should get a connection (knock) from yourself inside the RAT!

To remove yourself right click the connection and select Client Management -> Uninstall

Here is a scan of what your unencrypted payload will look like:

<https://avcheck.net/id/QFDclb6pNCqm>

18/26 detected..

Now you need to crypt your payload for spreading. Lets use ScrubCrypt.

You can buy a week here: <https://scrubcrypt.su>

You should get the download and product key in the email provided at purchase.

Download ScrubCrypt to your RDP.

Open Scrubcrypt. Enter your license key.

Click the three dots in the upper right hand corner of ScrubCrypt to navigate to your unencrypted Quasar Payload.

For settings: select Hidden, Startup, UAC Bypass, and WD Exclusion.

This will run with the CMD window hidden, adds your payload to startup, will auto escalate itself to administrator priv with UAC bypass, and then, as an administrator create a windows defender exclusion for every detected drive. The defender exclusion is very important because even though ScrubCrypt is FUD with this build eventually your payload will become detected over time and with the exclusion in place windows defender will never detect anything ever again.

Click Build, save your payload for use!

Here is a scan of our crypted payload:

<https://avcheck.net/id/WmTacxqyQIEj>

0/26

Runtime:

<https://scanner.to/result/2jE8URusvueJ>

3/21 (Bypass Defender)

slezer - April 15, 2024, 9:27 pm

Should've provided a runtime scan of your crypter instead of a scantime scan, would actually be useful :)

DynamicW - April 16, 2024, 12:14 am

You should do runtime scan too yes.

joshn - April 16, 2024, 4:40 pm

Please check my thread. Been using quasar for a long while and just ran into this problem.
hackforums.net/showthread.php?tid=6268731&pid=62338012#pid62338012

Henkpapels - April 17, 2024, 3:18 am

thanks alot for this post!

ScrubspooF - April 17, 2024, 1:29 pm

(Apr 15, 2024 09:27 PM)slezer Wrote: [\[CITE\]](#) Should've provided a runtime scan of your crypter instead of a scantime scan, would actually be useful :)

Thread updated with runtime scan:

Runtime:

<https://scanner.to/result/2jE8URusvueJ>

3/21 (Bypass Defender)

axsw - May 1, 2024, 9:48 am

Would that work on virtual box instead rdp?

ScrubspooF - May 1, 2024, 9:49 am

(May 1, 2024 09:48 AM)axsw Wrote: [\[CITE\]](#) Would that work on virtual box instead rdp?
Only if you don't want anything to connect.

SHADE™ - May 2, 2024, 4:37 pm

Good thread, very smooth instructions.

Speaker - May 4, 2024, 2:10 pm

Thanks appreciate your efforts!

cYBEROPTICS - May 9, 2024, 7:39 pm

Thanks for the nice write up OP!

JoeRogan - May 16, 2024, 7:44 am

i agree but i do not know if there are any better alternatives

Mlwelsh - November 23, 2024, 11:52 am

Interesting. If connecting to another persons computer / network, do i still use my own IP address in the IP/Hostname builder.

pipoelamigo - December 6, 2024, 11:39 am

thank you very much for that

BPName - December 7, 2024, 1:01 pm

thanks alot for this post!

Jayjonjah - December 12, 2024, 7:19 am

Thanks for sharing. This is so useful

magxusss - January 29, 2026, 2:24 am

Would it be best to download it on a vm? or can i youse my normal machine?

Binance - January 29, 2026, 4:55 am

(Jan 29, 2026 03:24 AM)magxusss Wrote: [\[CITE\]](#) Would it be best to download it on a vm? or can i youse my normal machine?

Don't.

I would recommend a VPS, especially if you intend to use it maliciously.

However, be aware of the strict limitations quasar now poses.

magxusss - January 29, 2026, 7:10 am

(Jan 29, 2026 05:55 AM)Binance Wrote: [\[CITE\]](#) Don't.

I would recommend a VPS, especially if you intend to use it maliciously.

However, be aware of the strict limitations quasar now poses.

Okay thank you!

I am also going to install it on a vm

I jsut was because i want to troll my friend with it but didn't want to install it on my school laptop?

fettywap98 - January 30, 2026, 8:35 am

Thanks for the information brudda, very easy to follow along