

Forum:[Hack Forums](#)

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

ScrubspooF - April 15, 2024, 5:18 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)

Dystortion - April 15, 2024, 6:56 pm

Very informative - utilisation can be done for most other RATs. side question: is quasar archived now, thought I remember seeing? obviously doesn't damage to tool too much for future uses

V?rt - April 15, 2024, 7:20 pm

What a great tutorial. I've had quasar for like 1-2 years now and never figured out how to use it lol. Now I kinda wanna follow these to say I finally did it.

anaumarcin - April 17, 2024, 11:02 am

scrubcrypt is unfortunately down... what else ?

US3R1 - April 17, 2024, 11:06 am

The forum post was exemplary in both substance and presentation. It provided a comprehensive analysis of the topic, incorporating relevant data and perspectives to offer a well-rounded view. The author's clear and concise writing style made complex ideas accessible to all readers, fostering understanding and engagement. Furthermore, the post encouraged constructive dialogue by acknowledging counterarguments and inviting diverse viewpoints. Its organization and formatting enhanced readability, ensuring that key points were easily discernible. Overall, the post demonstrated a high level of expertise and contributed significantly to the forum's intellectual discourse, setting a commendable standard for future discussions.

anaumarcin - April 17, 2024, 11:52 am

(Apr 17, 2024 11:06 AM)US3R1 Wrote: [\[CITE\]](#) The forum post was exemplary in both substance and presentation. It provided a comprehensive analysis of the topic, incorporating relevant data and perspectives to offer a well-rounded view. The author's clear and concise writing style made complex ideas accessible to all readers, fostering understanding and engagement. Furthermore, the post encouraged constructive dialogue by acknowledging counterarguments and inviting diverse viewpoints. Its organization and formatting enhanced readability, ensuring that key points were easily discernible. Overall, the post demonstrated a high level of expertise and contributed significantly to the forum's intellectual discourse, setting a commendable standard for future discussions.

??? ??Lool

Tentco - April 17, 2024, 12:31 pm

(Apr 17, 2024 11:02 AM)anaumarcin Wrote: [\[CITE\]](#) scrubcrypt is unfortunately down... what else ?
It's not down, the domain has been switched.
Check the original thread after few hrs, it is being updated.

ScrubspooF - April 17, 2024, 12:48 pm

(Apr 17, 2024 11:02 AM)anaumarcin Wrote: [\[CITE\]](#) scrubcrypt is unfortunately down... what else ?
The new domain for scrubcrypt is <https://scrubcrypt.su>

Added runtime scan to thread

Runtime:

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

3/21 (Bypass Defender)

Refil - April 19, 2024, 3:20 pm

Great tutorial thank you so much

Scrubspooof - April 24, 2024, 7:12 pm

(Apr 19, 2024 03:20 PM)Refil Wrote: [\[CITE\]](#) Great tutorial thank you so much
No problem

Lucid - April 25, 2024, 12:23 pm

This was a very detailed post with great instructions - cheers for sharing with us!