
BitRAT Operator's Manual



UnknownProducts

unk@404.city

Table of Contents

1. Recommendations
2. Setting up **BitRAT's** SSL/TLS
3. Building your Server
4. UAC Exploit
5. Reverse SOCKS4
6. SOCKS5
7. XMR Miner
8. Downloader
9. Disabling Windows Defender
10. Remote Browser
11. hVNC
12. Blockchain (BTC) Payment Explained
13. FAQ - Troubleshooting

I - RECOMMENDATIONS FOR BITRAT

So: you've downloaded the client, made the purchase, opened up to your main window; what now? If you have any prior experience with Remote Administration Trojans/Tools and port-forwarding you can skip to section 2.

First off, there are three main recommendations we would recommend with **BitRAT** in order to maintain privacy, security and functionality.

- Dedicated IP(s) Capable of port forwarding
- OpenVPN software
- Dedicated RDP or VPS

These are basic, non negotiable standards that are designed to keep you, the end user, safe when spreading your Remote Tool. Good OPSEC practice is everything.

TOR Browser:

<https://www.torproject.org/download/>

Mullvad VPN:

<https://mullvad.net/en/> or

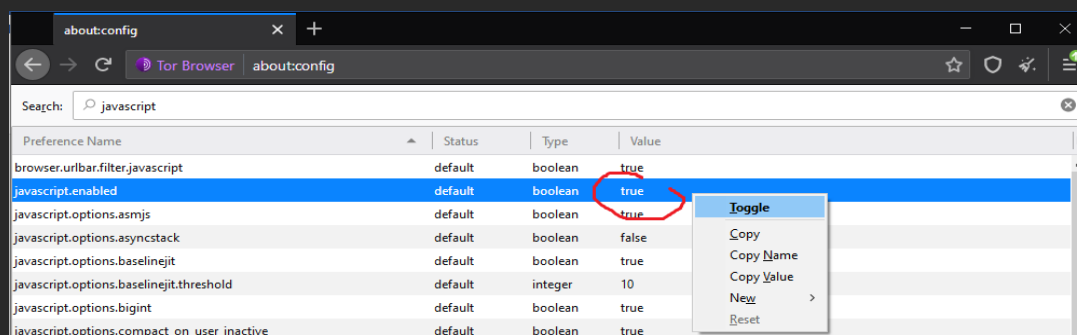
OpenVPN Client:

<https://openvpn.net/>

BitRAT Client:

<http://unknownposdhmyrm.onion/download/rel.rar>

When surfing with TOR;



Note: after booting TOR browser, type about:config into the URL browser and disable javascript.

1. When updating your client, extract the new contents of the file into your BitRAT folder. Do NOT delete the old directory.

Simply overwrite the old client with the new and boot BitRAT like normal.

2. Always make sure your clock is synced with your system's region time. Make sure TOR is not running before starting BitRAT for best results.

3. Back up your personal HWID into a notepad file, save it on your desktop or a USB drive. This is essentially your personal account number and cannot be recovered.

4. If you need to change systems simply download the client on the new system and click "update HWID" on the payment screen and enter your first HWID.

2 – SETTING UP BITRAT – PORT FORWARDING – ONLY FOR SSL

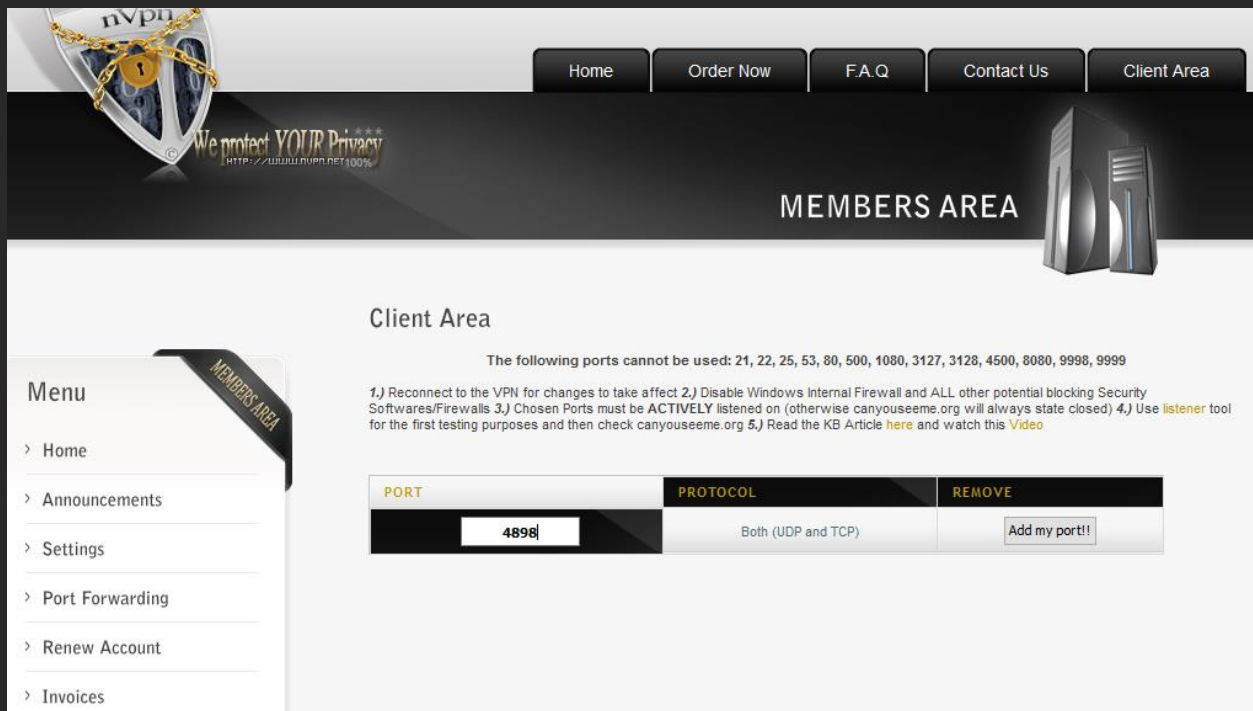
Warning: You **only** need to port forward your dedicated IP for SSL/TLS build.

TOR is recommended to only use PORT 80.

If you are only going to use **TOR** Hidden service, please skip this section.

Port forwarding with a Dedicated VPN IP is the easiest way to port forward your Remote tool. Doing this, you bypass Windows Firewall and don't have to submit any entries into permissions.

Using a dedicated IP from nVPN for an **example**:



The screenshot shows the nVPN Client Area. At the top, there's a navigation bar with links: Home, Order Now, F.A.Q, Contact Us, and Client Area. Below this is a banner for "MEMBERS AREA" with the text "We protect YOUR Privacy" and a URL "HTTP://WWW.NVPN.NET/100%". The main content area is titled "Client Area" and lists ports that cannot be used: 21, 22, 25, 53, 80, 500, 1080, 3127, 3128, 4500, 8080, 9998, 9999. Below this, there are instructions for reconnecting to the VPN, disabling Windows Firewall, and using the listener tool. A table shows the port forwarding configuration:

PORT	PROTOCOL	REMOVE
4898	Both (UDP and TCP)	<input type="button" value="Add my port!!"/>

Open the **Admin Panel** > **Port forwarding** > **Enter desired port**:

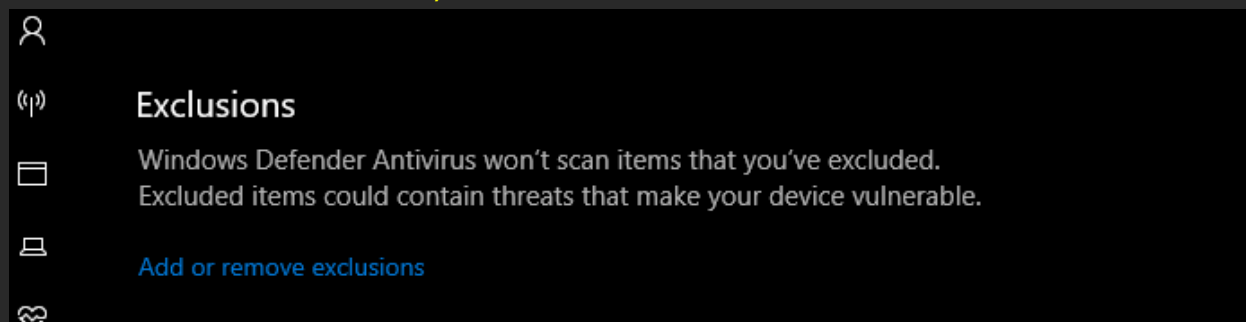
Your Remote Tool is now ready to receive incoming connections via SSL.

Port forwarding on a Windows Private Server, or directly from your **windows machine**, would require a manual port forward allowing TCP and UDP connections through your Windows Firewall. In our example we will be forwarding port 4898. This can be achieved by first **disabling your antivirus**, adding your BitRAT client folder to the list of exceptions by opening;

Windows Security > Virus and Threat Protection > Toggle “Real Time Protection” off



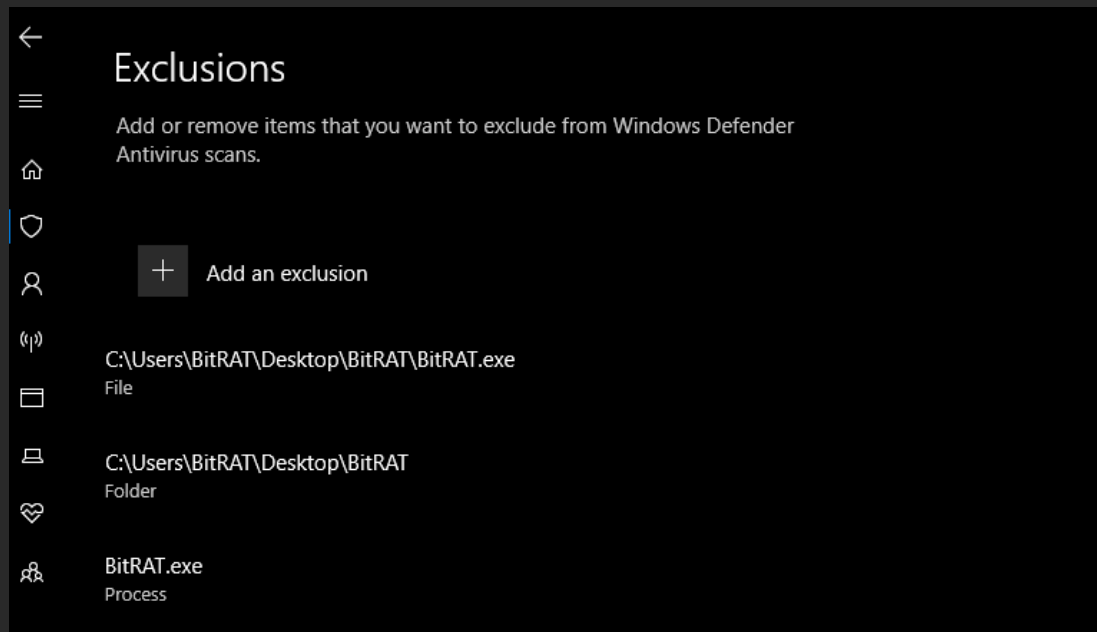
Exclusions > Folder > BitRAT Directory



Next, we will be adding a port-forwarding exclusion to Windows Firewall. **BitRAT** only uses TCP protocol in TLS/SSL mode.

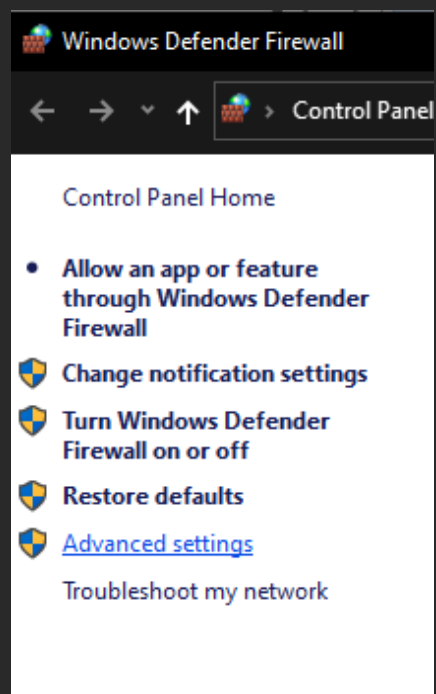
1.

Control Panel > Firewall and Network > Allow an App through Firewall > Select "BitRAT.exe"



2.

Control Panel > Windows Defender Firewall > Advanced Settings.



3.

Inbound Rules > New Rule > Port > TCP > Specific Port: 4898

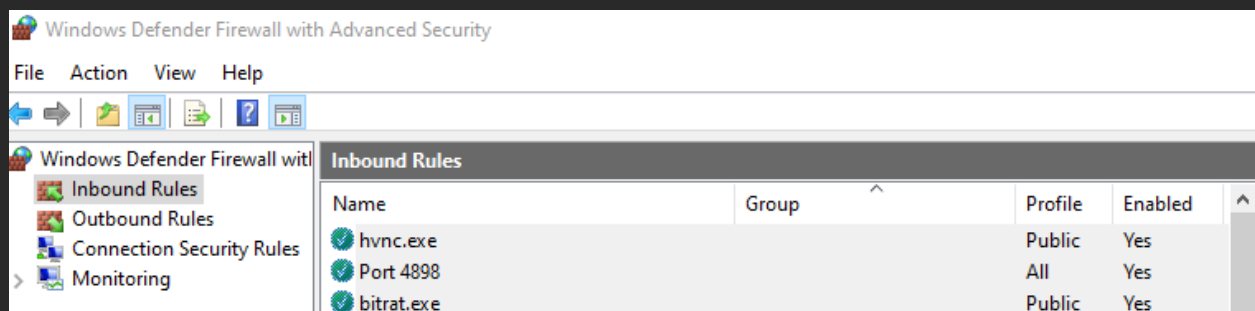
Inbound Rules > New Rule > Program > Specific Program > BitRAT.exe

Outbound Rules > New Rule > Port > TCP > Specific Port: 4898

Outbound Rules > New Rule > Program > Specific Program > BitRAT.exe

Note: If you are still using a home device, you will also need to port forward in your Router.

BitRAT should *automatically* forward this process for you.



3 – BUILDING YOUR SERVER - SSL

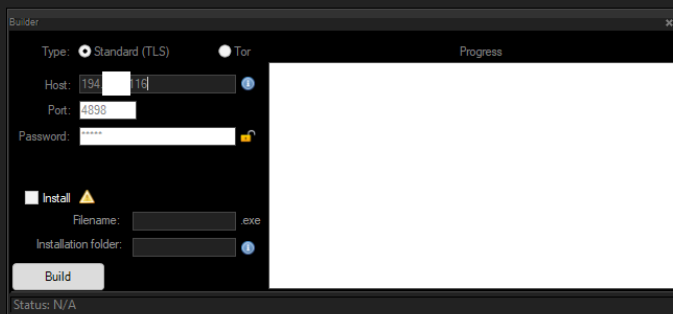
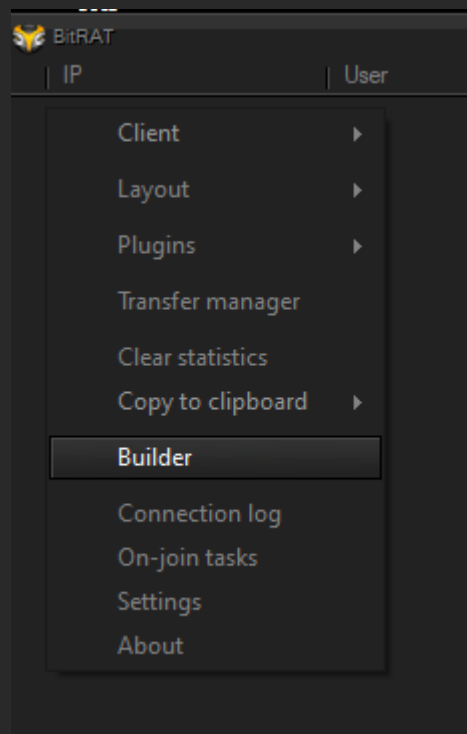
SSL/TLS is the most stable way to use any Remote Tool over TCP. Using TLS for the majority of your clients promotes stability, speed and general faster response times.

Right Click > Settings > “Start Socket” > Generate your SSL Certificate

Right Click > Builder > TLS > Enter Assigned IP > Enter Port > Assign Password > Build

ALWAYS SECURELY BACK UP YOUR DATA

Always back up your static IP and settings in case you lose your RDP/machine and need to reinstall BitRAT.



Note: Please use the 'Install' function on your crypter if you are crypting your server

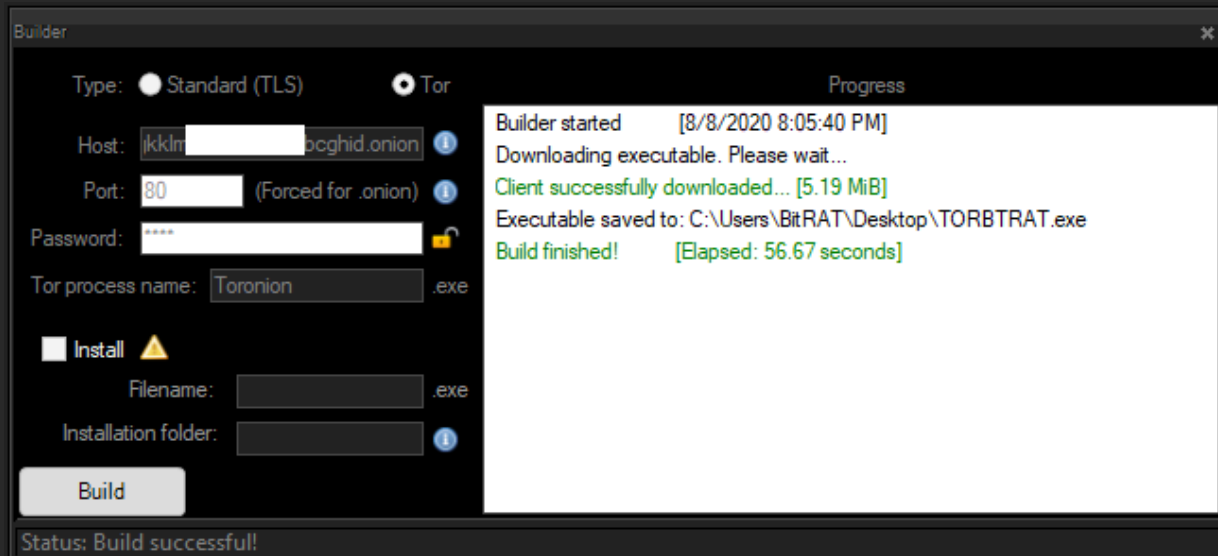
3 – BUILDING YOUR SERVER – TOR HIDDEN SERVICE

Right Click > Settings > Tor Hidden Service > Generate your .onion > Start

Note: **SAVE** your .onion link by exporting it via “Backup”

Always click “**Start**” on your TOR Hidden Service in the settings window or you will have issues connecting to TOR based clients.

Right Click > Builder > TOR > Post your .onion as “Host” > Port 80 > Name your TOR process > Build



TOR Hidden Service is very good for the initial infection of your client. Though less stable than TLS/SSL via slower response times, you are able to silently Download and Execute your TLS server while holding TOR as backup in case your client disconnects.

Do not port forward any **TOR** port, it is heavily recommended that you use the *default Port 80* and force when starting. If you port forward you may be vulnerable if this port is opened to the public.

*It is essential that you close the Socket (Click STOP) when you are not managing your **TOR** clients or your connection may not remain anonymous.*

4 – UAC ELEVATION EXPLOIT

UAC elevation is very straight-forward.

Right click on Client > Client > UAC Exploit

Your client will disconnect temporarily and reconnect if the Exploit was successful. A successful UAC elevation looks like;

BitRAT

IP

User

System

UAC Level

Operating System

Active Window

Idle

Bandwidth

In/Out

GR

Clients: 2

v Old limited client disconnecting

	87.101	i8@10...	DESKTOP-7D2...	ore(TM)7-	IQM, Microsoft ...	Limited	Win 10 (x64)	Task Manager	0d 0h 12m 12s	N/A	54.03 KiB/30...
	87.101	i7@10...	DESKTOP-7D2...	ore(TM)7-	IQM, Microsoft ...	Admin	Win 10 (x64)	Task Manager	0d 0h 0m 6s	N/A	255 B/65 B

^ Reconnected client with Admin

If your client does not reconnect, you will have to wait until they restart their device

Alternatively, you can utilize BitRAT's process protection function which will add the process to the protected Windows Process list in Task Manager as well as utilize the UAC Exploit. If the client force closes the process, they will get a BSOD and their system will crash, forcing a restart.

Right click on Client > Client > Process Protection

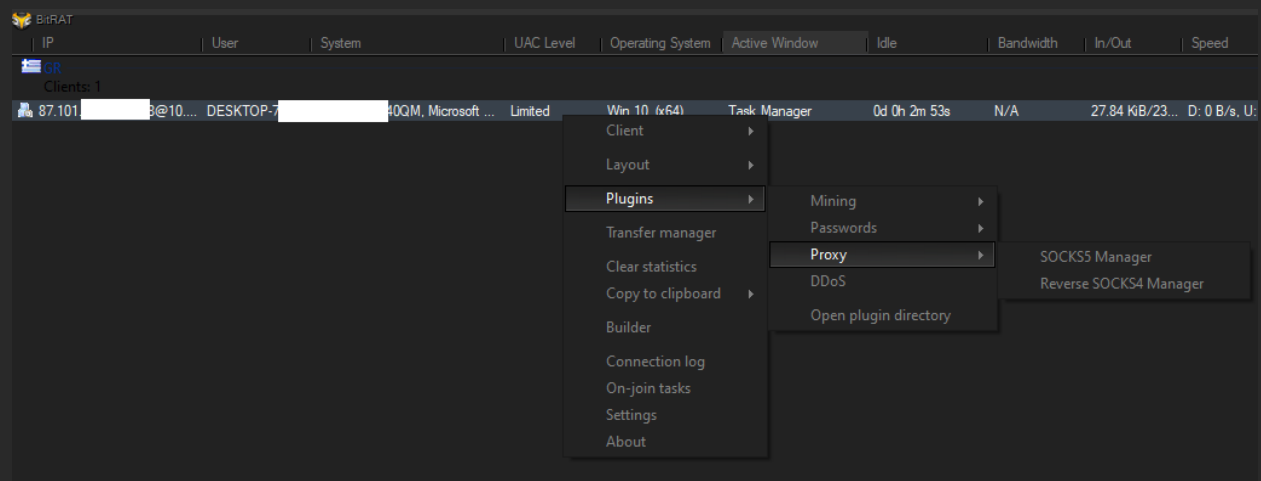
5 – REVERSE SOCKS4 PROXY

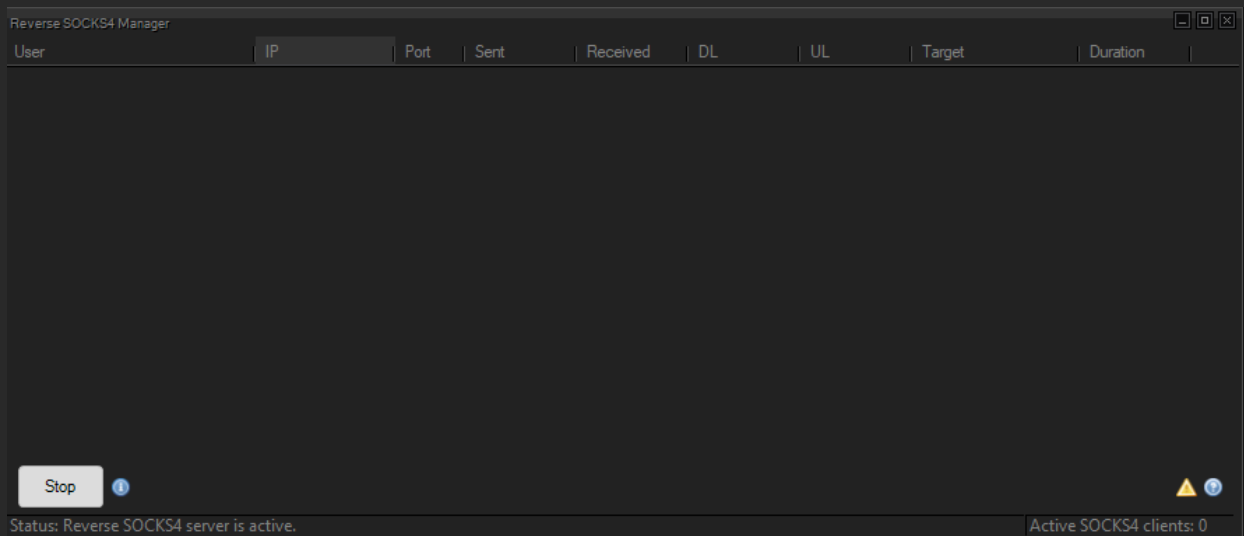
Ports 30000 – 65535 must be port forwarded on your static IP (SSL) in order for your SOCKS4 push to work. If you are connected via a TOR client, you must Download and Execute a TLS client with a dedicated static IP to reconnect. Most Dedicated IP providers will have this already forwarded for you. If not, submit a support ticket to have the range opened up.

You will require UAC elevation exploited to prevent issues with User Control.

Right Click > Plugins > Proxy > Reverse SOCKS4 Manager

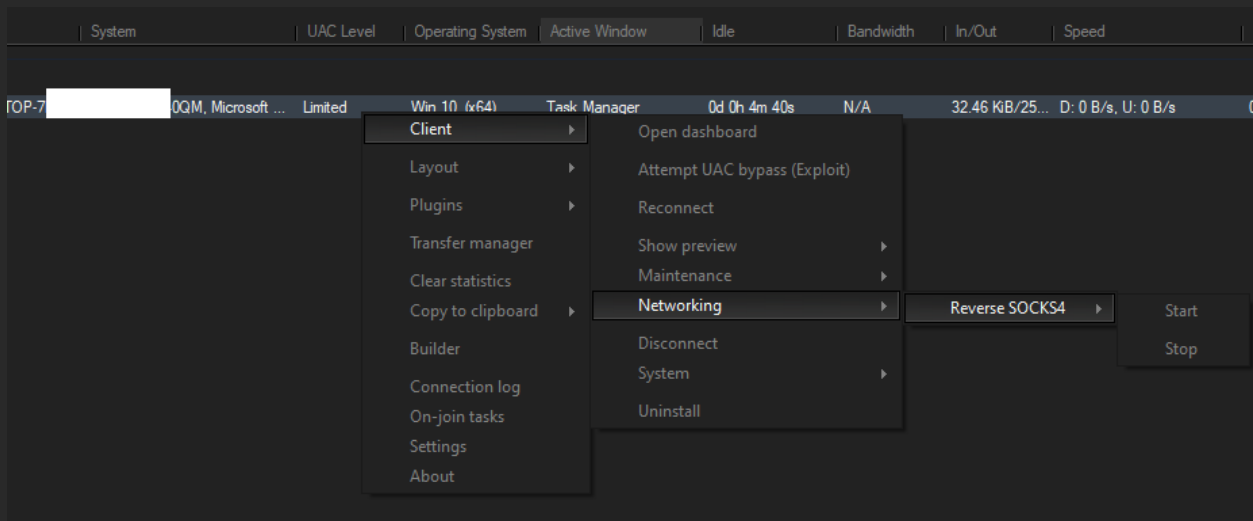
Click “Start” to enable your Reverse SOCKS4 Manager.





Right click on Client > Client > Networking > Reverse SOCKS4 > Start

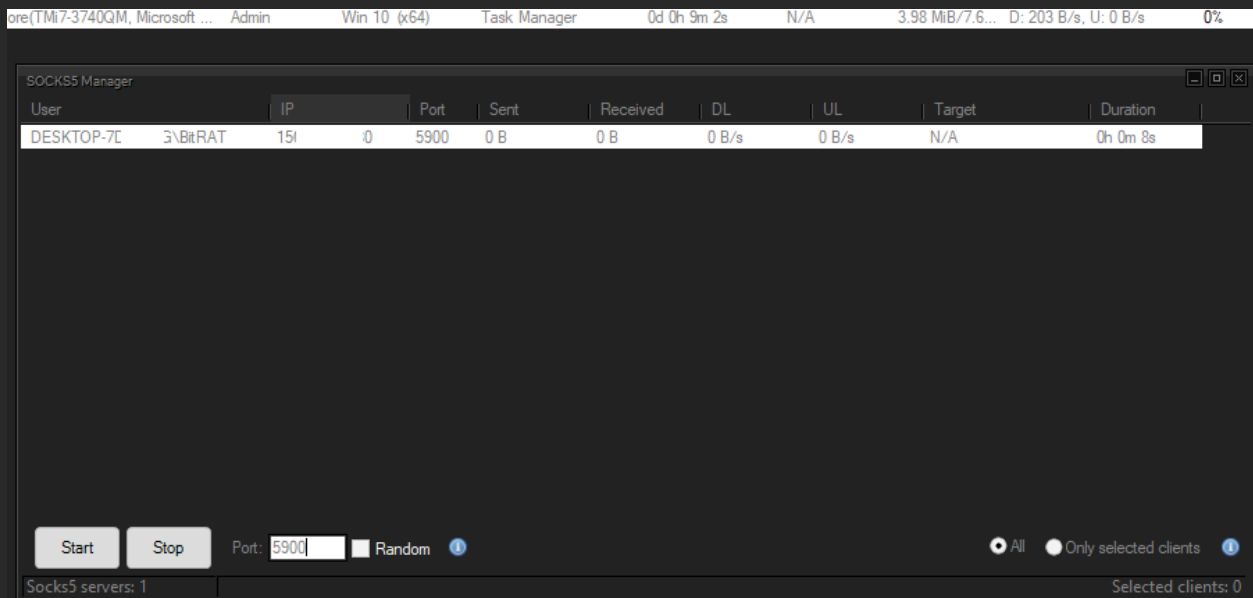
After which, your enslaved client will pop up on your Reverse SOCKS4.



6 – SOCKS5 MANAGEMENT

BitRAT will do all the work and automatically try to UPnP push a SOCKS5 proxy when enabling your Client. It makes the process incredibly easy; after a UAC exploit, simply open the SOCKS5 Manager and click “Start”. If successful, your client will pop up and you can monitor traffic.

Right Click > Plugins > Proxy > **SOCKS5 Manager**



If the above does not show a client, you will have to use hVNC or Remote Desktop to manually portforward from inside the device.

7 – XMR MINER

XMR Miner can be set up with a plethora of Pools; typically from a trusted source like <https://monero.org/services/mining-pools/> you will pay commission depending on the pool you use. **BitRAT** makes it incredibly easy to set up as follows:

XMR Mining

User	Threads	Pool	Algorithm	OpenCL	CPU	Shares	Donate	Speed	Duration
------	---------	------	-----------	--------	-----	--------	--------	-------	----------

Start

Stop

Pool:

Algorithm:

Process priority:

Rig ID:

Username:

Threads:

User-Agent:

Password:

Donate:

☒ Keepalive

☐ No huge pages

☐ Nicehash

☒ 64-bit

☒ All

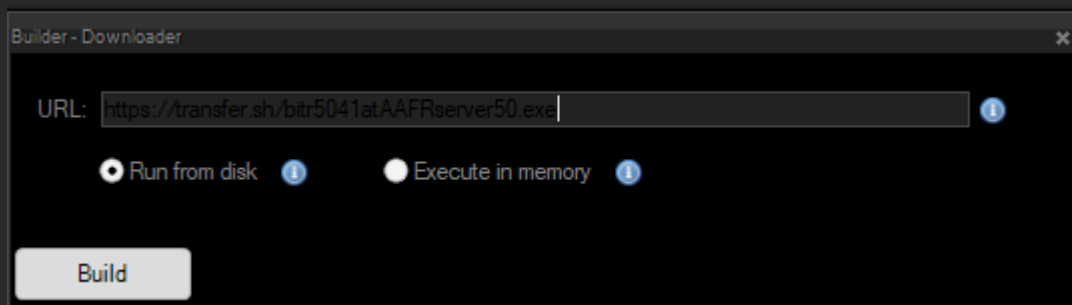
☐ Only selected clients

BitRAT recommends using 64-bit mining on 64-bit systems for the best results. The information bubbles on the XMR miner window show the most recent, up to date tips on how to get the most out of your clients. Only alter UserAgents and string information if you are absolutely sure what you want out of your clients. BitRAT will auto appropriate the best results.

You can select separate clients by holding the left CTRL and left clicking on each of the clients. When you are finished selecting, click “Start” on your XMR miner management window.

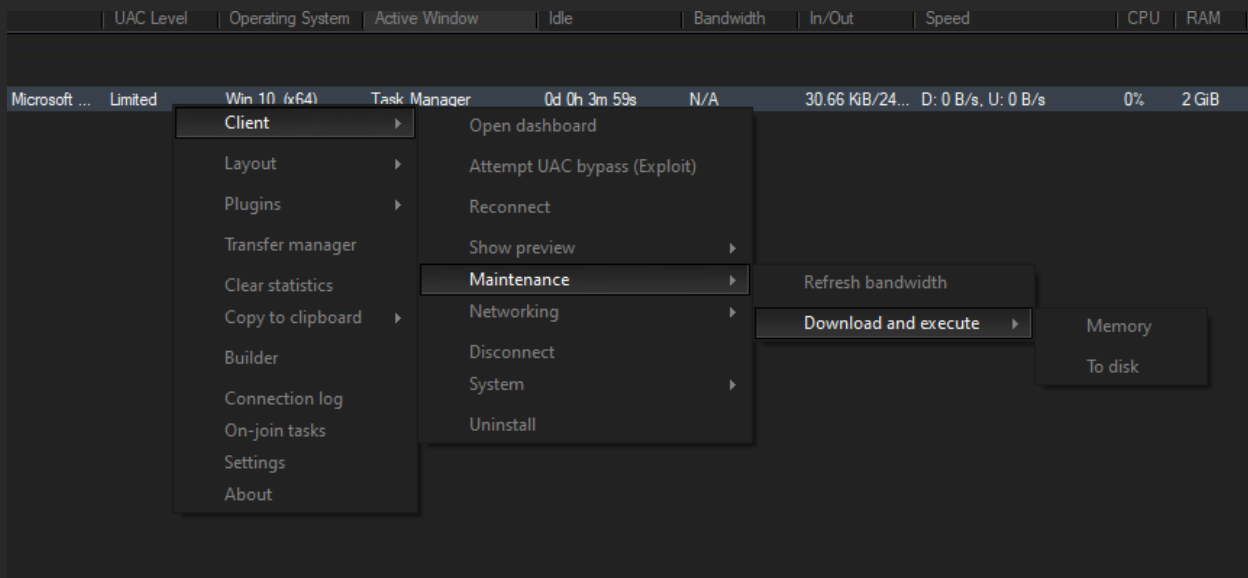
8 - DOWNLOADER

When you need a smaller stub size and to further avoid runtime detection; a silent downloader will do the job. Though “To Memory” typically produces the best results, some crypter services may not support this function due to the requirement of disk initialization. Definitely best to test any .exe before spreading.



You must submit an http or https direct link to your EXE that will download upon execution

A similar function is used to initiate the Download & Execute function on a connected client.



Right click on Client > Client > Maintenance > To Disk or Memory

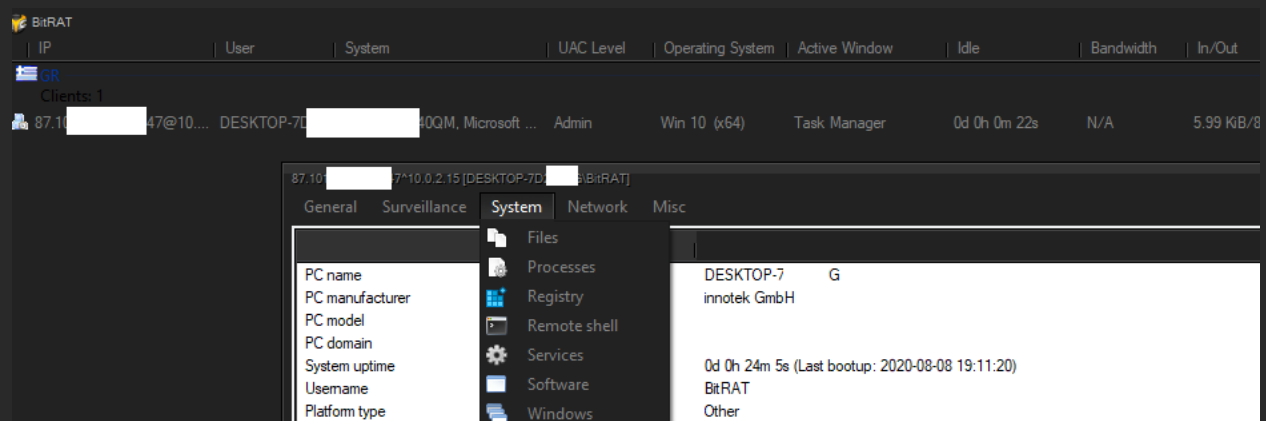
9 – DISABLING WINDOWS DEFENDER

Primarily, **BitRAT** showcases an **automatic** feature that will purge Windows Defender from the selected client.

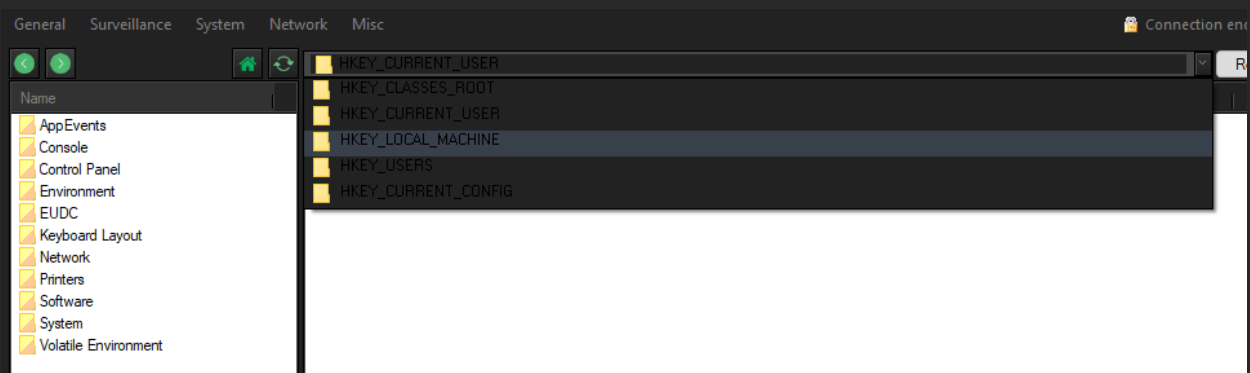
Right Click on Client > Client > Windows Defender Killer

Alternatively, If you need to revert this in the future, you must disable Windows Defender manually. Once you have admin privileges, (UAC Exploit) you can now edit the registry.

Right Click on Client > Open Dashboard > System > Registry > Drop down “HKEY_LOCAL_MACHINE”



Opening the registry, we're going to disable Windows Antivirus manually. On the list menu on the left;



SOFTWARE > Microsoft > Windows Defender Folder > Add new value “DisableAntiSpyware”

REG_DWORD - Change your Value from (0) to (1).

SOFTWARE > Microsoft > Windows Defender Folder > Add new value "DisableAntiVirus"

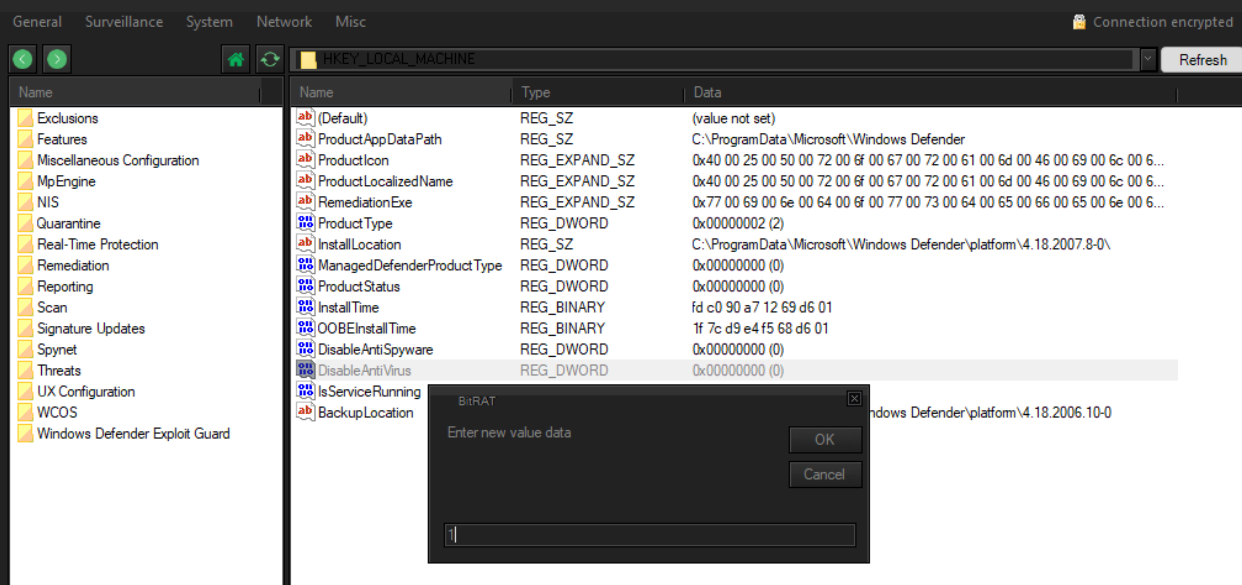
REG_DWORD - Change your Value from (0) to (1).

SOFTWARE > Microsoft > Windows Defender Folder > Real-Time Protection > Add new value "DisableBehaviorMonitoring"

REG_DWORD - Change your Value from (0) to (1).

SOFTWARE > Microsoft > Windows Defender Folder > Add new value "DisableAntiSpyware"

REG_DWORD - Change your Value from (0) to (1).



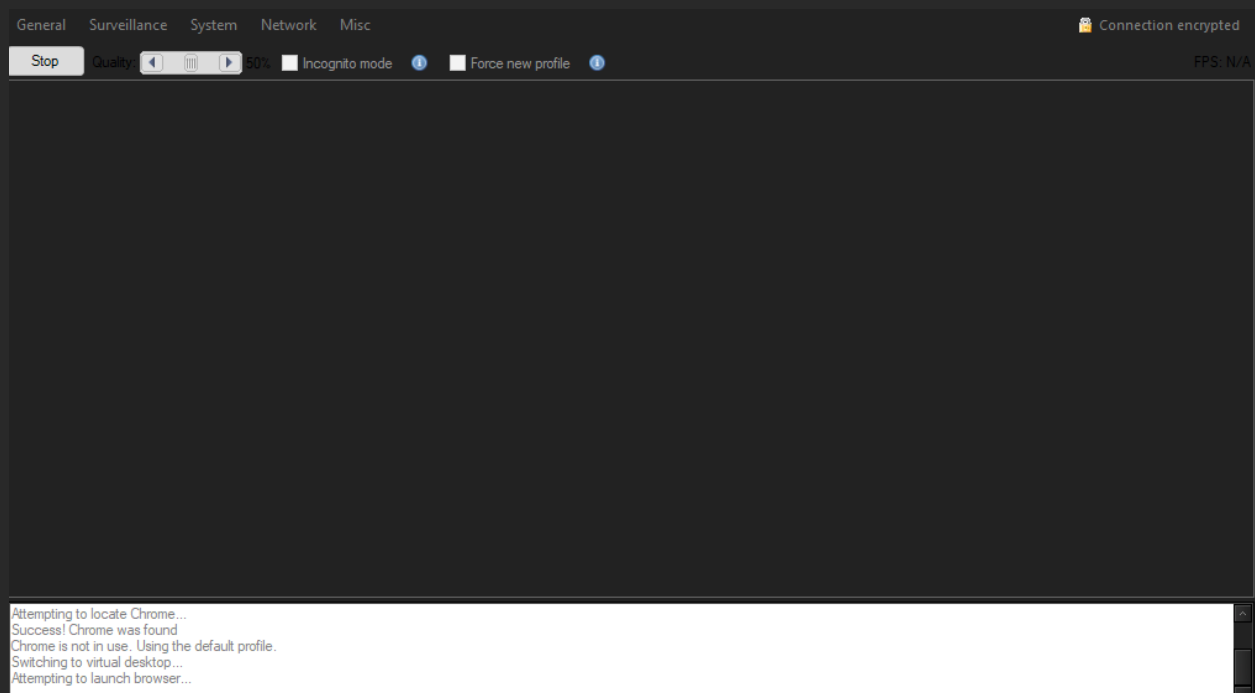
Should this fail, you can use **BitRAT**'s hVNC function for total control and initiate the steps manually to purge Windows Defender. Alternatively, again, you can use the Remote Shell.

I0 – REMOTE BROWSER - CHROME

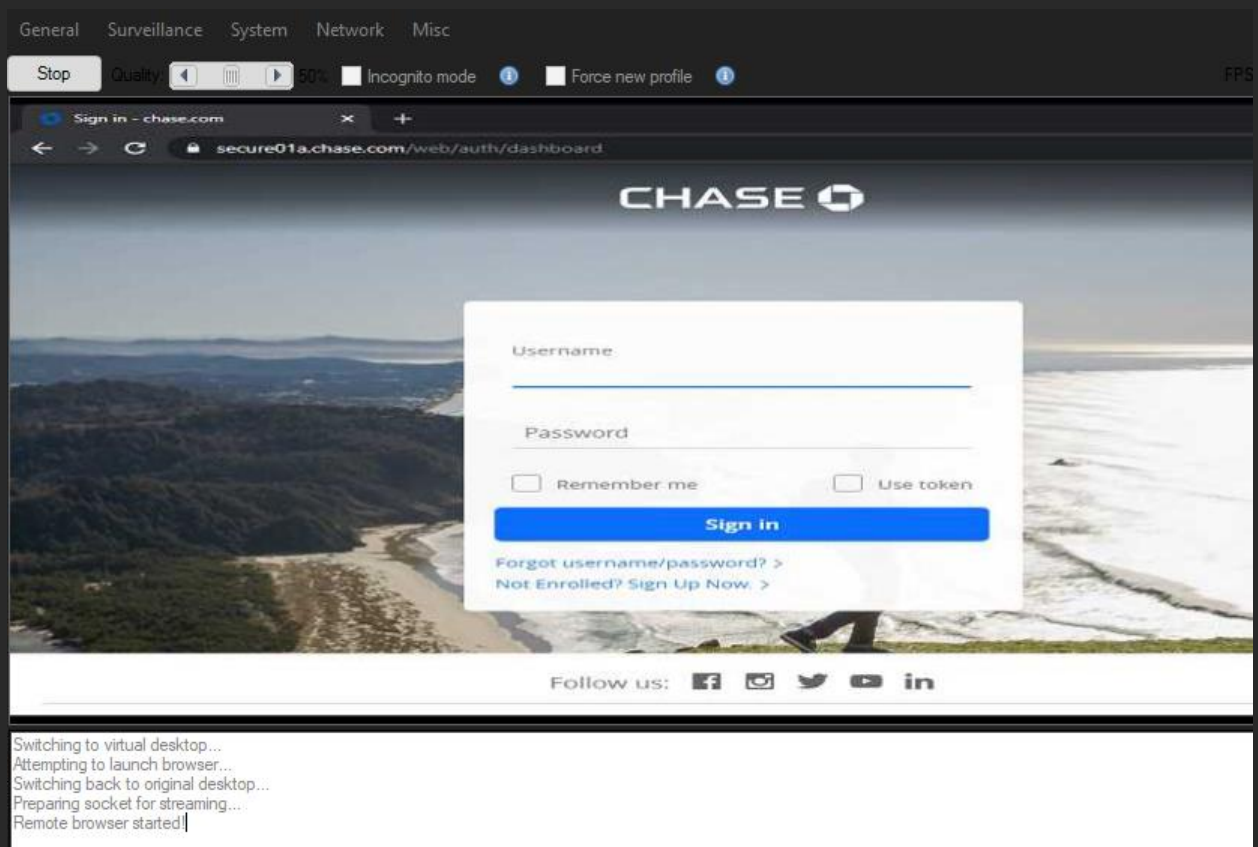
Remote Browser is one of the easiest functions to use with **BitRAT**. Just like many other functions, **BitRAT** does all of the work for you. Simply navigate;

Hidden Remote Browser will only work on Windows 8.1 – Windows 10. Windows 7 will leave a black screen.

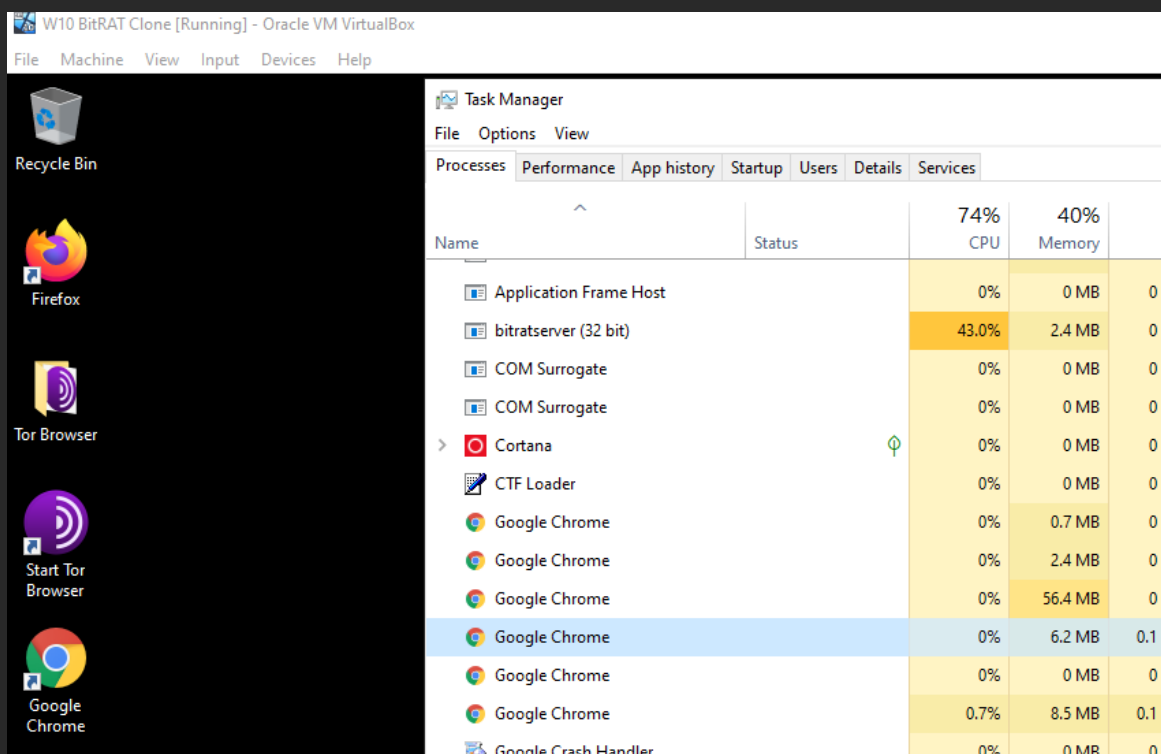
Right click on client > Open Dashboard > Misc > Remote Browser



After clicking start, the **BitRAT** will attempt to open a hidden socket and launch the users browser. Completely hidden from desktop view.

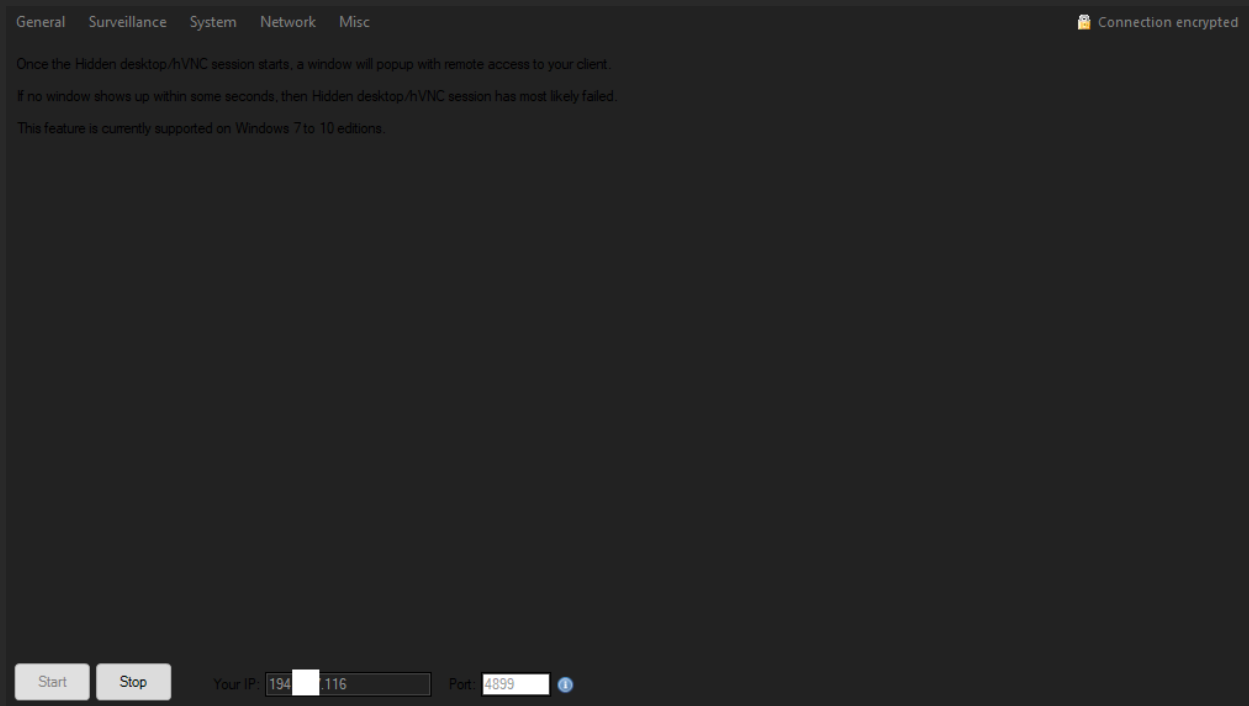


However, you will still see it in the task manager.

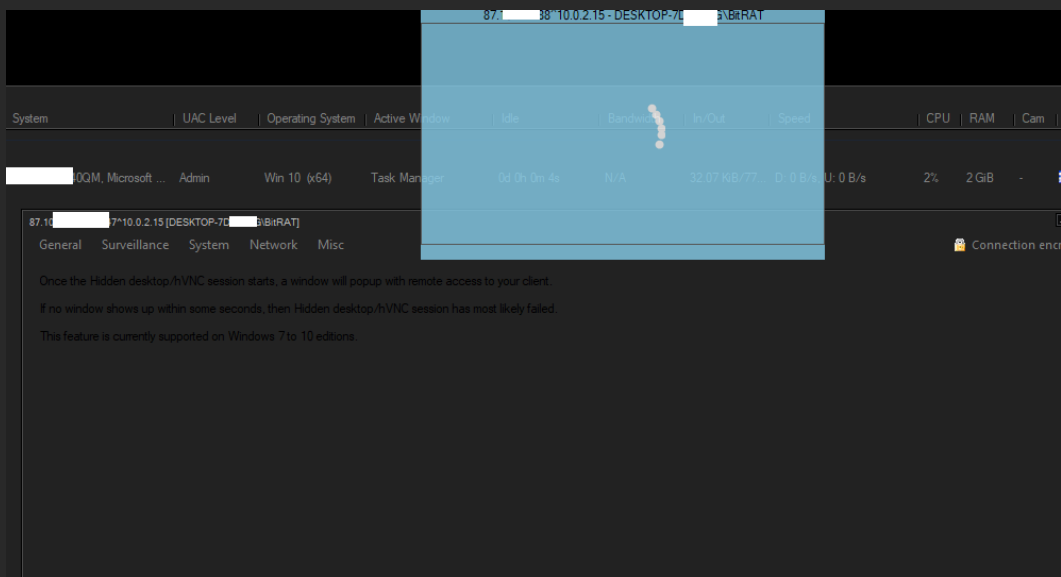


11 - hVNC

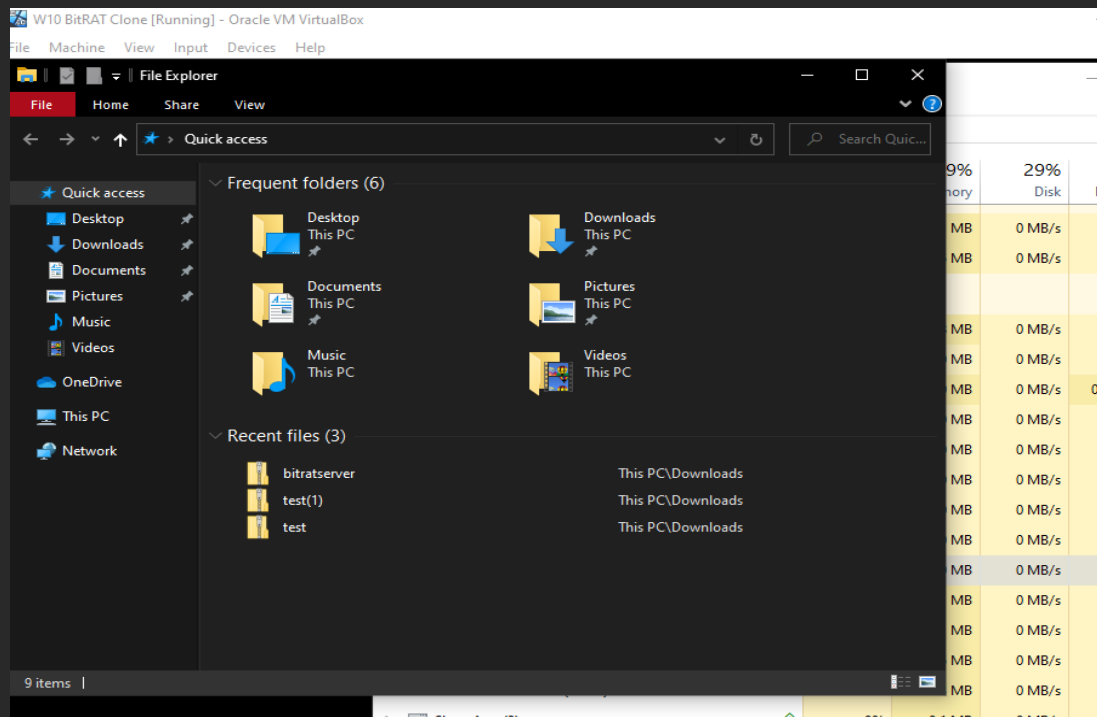
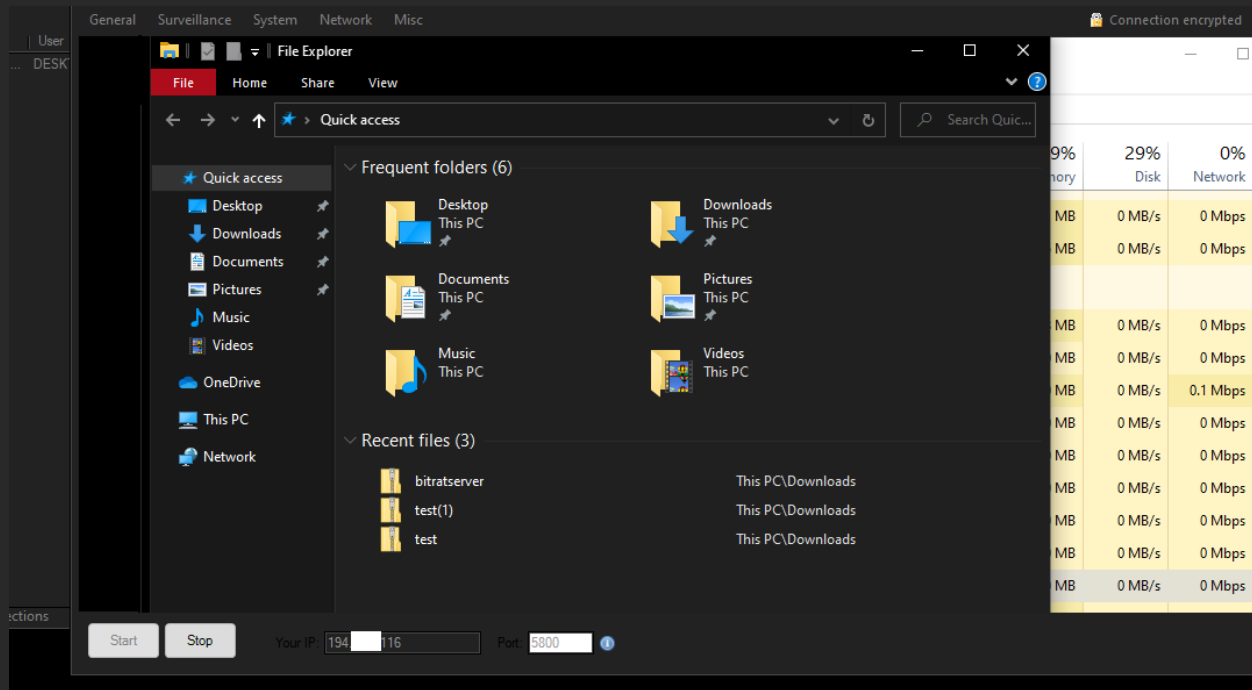
hVNC requires a static IP to be initiated with a dedicated port open for a constant stream of communication between the Client and host. Very straight-forward, the hVNC window will initiate automatically when you click Start after filling in the IP and port fields.



Right click on Client > Client > Open Dashboard > Misc > hVNC



If hVNC initialization fails, force reboot on the client from your main window screen. Initiate **without** Admin.



I2 – BTC PAYMENT EXPLAINED

A BTC payment is not like a Paypal payment or like swiping your debit card. You have to wait for miner confirmations before the payment will go through. This will entirely depend on your fee.

When you initiate a transaction it is uploaded to what's called the mempool. You can track your transaction hash at <http://mempool.space> and, if you've opted to pay the priority fee(usually a few cents above average) your payment for BitRAT will confirm within a few minutes. If you've opted to pay less than the minimal fee, you will have BitRAT once your payment confirms. Simple.

The payment process is automatic and has not made errors to this date. Only contact support with your blockchain hash ready, typically found in your wallet, after it has been marked confirmed by the mempool and you still do not have access to BitRAT.

The following is an excerpt from;

<https://www2.deloitte.com/ch/en/pages/strategy-operations/articles/blockchain-explained.html>

You (a "**node**") have a file of transactions on your computer (a "**ledger**"). Two government accountants (let's call them "**miners**") have the **same file** on theirs (so it's "**distributed**"). As you make a transaction, your computer sends an e-mail to each accountant to inform them.

Each accountant rushes to be the first to check whether you can afford it (and be paid their salary "**Bitcoins**"). The first to check and validate hits "REPLY ALL", attaching their logic for verifying the transaction ("**proof of work**"). If the other accountant agrees, everyone updates their file...

This concept is enabled by "**Blockchain**" technology.

13 – FREQUENTLY ASKED QUESTIONS - TROUBLESHOOTING

My Client doesn't have TOR Browser installed, will a TOR stub still work?

Yes. BitRAT will install TOR Libraries in the End user's background processes

Help! My RDP/VPS/Host crashed and my BitRAT Client is gone!

Simply download the BitRAT client on your new host machine and click "Update HWID". Enter your very **first** HWID. Please see Page 4.

TOR is stuck on an endless loop loading.

Sync your clock with your system's designated region and make sure It is up to date. TOR protocol depends on this in order to function.

BitRAT will not boot and gives me a "TOR Failure" error code.

Close BitRAT.exe, Open the task manager, End the TOR task and restart BitRAT.

How do I update BitRAT?

Download the new client from the main host link. Extract the contents to your BitRAT directory. Do **not** delete your old directory.

Where can I find my HWID after I have already paid for BitRAT?

You can find your HWID by right clicking > About.

Do I need to register a .onion link in order to use BitRAT's TOR Hidden service?

No, BitRAT will autoregister a unique .onion link for you simply by clicking "generate". This will be stored in BitRAT\data\tor\html

What is BitRAT's client capacity? Will thousands of clients make it unbearably slow?

Though I would recommend installing separate tags and sockets for different spreading campaigns, No. BitRAT utilizes FastObjectListview and pulls heavy data from clients once you initialize the connection.

What crypter can we use best with BitRAT?

Currently, BitRAT does not promote any crypter services, however, most crypters will work with BitRAT.

How can I check to see if my port is opened?

Use a free port scanning service like canyouseeme.org. You can verify the port was scanned by checking the connection log located inside the RAT.

I would like to move BitRAT to an RDP/PC/VPS. How do I change my HWID license?

From the payment screen, at the bottom of the window you can update your HWID by inputting your old, **FIRST** one.

How do I back up my TOR clients?

Simply copy your TOR directory. BitRAT\data\Tor\html

Do you have a monthly package available?

No. BitRAT is currently only a Lifetime license.

My hVNC is connecting but only showing a black screen.

You must force restart your client. Try **without** Admin privileges, connecting with a limited user, then UAC Exploit.

BitRAT isn't editing the Windows Defender registry.

Some CPUs have an extra layer of protection like those with ESET installed. You must disable ESET from the remote shell, as well as edit the registry. A quick tutorial can be found here <https://www.windowcentral.com/how-edit-registry-using-command-prompt-windows-10>

Alternatively, you can utilize BitRAT's Windows Defender Killer function and let BitRAT do the work.

Warning: this is irreversible.

Download and execute isn't installing my drop programs.

Keep in mind, same as the downloader, it must be a direct link to your .exe. No .zip, no download button.

What CPU specs are best for BitRAT?

BitRAT can run on basically modern device running Windows. Recommended specs are an i7-6650 or newer with at least 8gb of RAM and you can **comfortably** manage up to 10,000 clients; though capable of more.