

Forum:[Hack Forums](#)

Thread: [Official Samaritans RAT Help Desk | Ask Questions | Troubleshooting | Free](#)

Business - November 14, 2018, 7:12 am

Samaritans RAT Help Desk

This thread will be comprised of Samaritans:

Answering RAT questions
Troubleshooting problems
Suggesting tools (RAT, DNS, VPN, etc)
Giving free advice

So that we can offer our best assistance, please be detailed when describing your issue or question. The more we know, the more we can help!

#Skyline - November 14, 2018, 7:33 am

Please feel free to let know if you require any of the above. As we are happy too help.

FallenCancer - November 14, 2018, 4:18 pm

Is there any sort of vpn that you recommend because I don't know which to get

Business - November 14, 2018, 4:20 pm

(Nov 14, 2018 05:18 PM)FallenCancer Wrote: [\[CITE\]](#) Is there any sort of vpn that you recommend because I don't know which to getFor most RAT usages, you'll want a VPN that allows for port forwarding. There are many options, but any with port forwarding capabilities would work fine.

crazy_command3r - November 15, 2018, 8:55 am

Crypting methods, differences between native and managed, icons (do they really make the virus detectable?), compression and file pumping. Could you explain these things? (Just a fast explanation, not a full in-depth)

Business - November 15, 2018, 6:16 pm

(Nov 15, 2018 09:55 AM)crazy_command3r Wrote: [\[CITE\]](#) Crypting methods, differences between native and managed, icons (do they really make the virus detectable?), compression and file pumping. Could you explain these things? (Just a fast explanation, not a full in-depth)A lot of things can cause your file to be detected. We won't be covering many crypting questions here, as many people use them for illegal purposes. You would probably get better answers in the cryptography section. ?

ETH - November 16, 2018, 2:30 am

I need help on port forwarding anyone in samartians can help me

Business - November 16, 2018, 2:31 am

(Nov 16, 2018 03:30 AM)Hollow Wrote: [\[CITE\]](#) I need help on port forwarding anyone in samartians

can help me! got you, PM me.

Jacque Fresco - November 16, 2018, 6:44 am

(Nov 15, 2018 09:55 AM)crazy_command3r Wrote: [\[CITE\]](#) Crypting methods, differences between native and managed, icons (do they really make the virus detectable?), compression and file pumping. Could you explain these things? (Just a fast explanation, not a full in-depth)

Even if Business is not interested in Helping out, because he thinks his answers can be used to help you or others fulfilling/completing blackhat activities, i will answer your question because as a real life samaritan i learned to be completely neutral to every person and group without making any prejudices.

Both compression and file pumping are mostly only being used in the malware "industry" to make a binary less detected.

As my knowledge reaches compression is just a form of Algorithm that can be used to make the size of the data smaller without having to fear that data gets extinct. (of course there are compressors for for example images (jpeg) that is compressing with the loss of data:

<https://www.labnol.org/software/tutorials/jpeg-vs-png-image-quality-or-bandwidth/5385/>)

But you dont want this to have in binarys. I can't tell you exactly how compression works, since i for myself was never interested in really understanding it. Im sure you will find some more info if you search around for the names of such programs like upx or mpress (

<https://dzone.com/articles/packers-how-they-work-featuring-upx>). Since you then have a smaller binary as the outcome that does not look like the original one, AV's will not recognize it that fast as malware (since the signature is now changed). Common compressors/packers like upx or mpress are so much overused/public that all kind of Anti Viruses have decompressors/unpackers so compressing a executable is no longer a nice option as long as you are not using a self coded or unknown packer.

File pumping is the cheap way to change the signature of a executable and pretty often being used in the past, but its not longer worth a thing since modern AV's have heuristics. What a file pumper does is that its adding some random bytes to the end of the file. Thats really simple.

I hope it basically answered your questions. Have a nice day (:

sh4moon - November 16, 2018, 7:53 am

(Nov 15, 2018 09:55 AM)crazy_command3r Wrote: [\[CITE\]](#) Crypting methods, differences between native and managed, icons (do they really make the virus detectable?), compression and file pumping. Could you explain these things? (Just a fast explanation, not a full in-depth)

crypting just encrypts specific parts of the exe (I think you can also do all of it).

to my knowledge icons don't help with av detection, but they definitely make the file more convincing to the user.

compression is a legit technique to make nonmalware more portable. in files, there's a lot of repeating of small parts of code. compression just makes it more efficient. av works by making signatures for malware. compression tends to change the signature.

file pumping just puts random data in the file to change the signature.

UndefeatedHades - November 16, 2018, 8:06 am

Any assistance with finding a good DNS for ratting?

crazy_command3r - November 16, 2018, 9:39 am

Thank you guys, I'm not interested in using this information in malicious actions, just letting you know.

I want to learn more about cryptography and things like that, so i can understand more how viruses and encrypted/obfuscated programs work.

Business - November 16, 2018, 1:09 pm

(Nov 16, 2018 09:06 AM)UndeateHades Wrote: [\[CITE\]](#) Any assistance with finding a good DNS for radding?I usually suggest Freenom as a free DNS service. That'll be perfect for starting out!

wraxu - November 16, 2018, 1:23 pm

Is there a way I can bind my rat file with another exe.

careswho - November 16, 2018, 2:15 pm

Thanks for this thread!

My main question is about VPN. Is there really any way to get to use a software based RAT with a VPN which doesn't have port forwarding?

The reason I ask this is because I am looking for a VPN which is good in terms of privacy, jurisdiction and obviously price as well. So most of the VPNs which have port-forwarding are either in the 5, 9, 14 eye countries or don't have a well documented no-logging policy. My research was mainly using That One Privacy Guy's guide and I think N-o-r-d has it when it comes user privacy but unfortunately it doesn't have port-forwarding.

So is there anyway around for a software based RAT with a VPN which doesn't have port-forwarding?

Thanks,

Business - November 16, 2018, 2:16 pm

(Nov 16, 2018 02:23 PM)wraxu Wrote: [\[CITE\]](#) Is there a way I can bind my rat file with another exe. The easiest and most common method to bind is by using the binding feature within a crypter. If you're a beginner, this is the easiest method.

(Nov 16, 2018 03:15 PM)careswho Wrote: [\[CITE\]](#) Thanks for this thread!

My main question is about VPN. Is there really any way to get to use a software based RAT with a VPN which doesn't have port forwarding?

The reason I ask this is because I am looking for a VPN which is good in terms of privacy, jurisdiction and obviously price as well. So most of the VPNs which have port-forwarding are either in the 5, 9, 14 eye countries or don't have a well documented no-logging policy. My research was mainly using That One Privacy Guy's guide and I think N-o-r-d has it when it comes user privacy but unfortunately it doesn't have port-forwarding.

So is there anyway around for a software based RAT with a VPN which doesn't have port-forwarding?

Thanks,I want more Samaritans to help here, so I'll leave this question for Skyline. :)

Pronouncer - November 16, 2018, 2:30 pm

(Nov 16, 2018 03:15 PM)careswho Wrote: [\[CITE\]](#) Thanks for this thread!

My main question is about VPN. Is there really any way to get to use a software based RAT with a VPN which doesn't have port forwarding?

The reason I ask this is because I am looking for a VPN which is good in terms of privacy, jurisdiction and obviously price as well. So most of the VPNs which have port-forwarding are either in the 5, 9, 14 eye countries or don't have a well documented no-logging policy. My research was mainly using That One Privacy Guy's guide and I think N-o-r-d has it when it comes user privacy but unfortunately it doesn't have port-forwarding.

So is there anyway around for a software based RAT with a VPN which doesn't have port-forwarding?

Thanks,

1. Use laundered bitcoin
2. Purchase from a offshore location, or a bulletproof hosting (Prepare to spend a lot)
3. Setup VPN
4. Profit?

You have to remember, no VPN can promise 0 logging. Unless they own their own ISP provider. Even russia has logging laws now.11

sh4moon - November 16, 2018, 2:32 pm

(Nov 16, 2018 03:15 PM)careswho Wrote: [\[CITE\]](#) Thanks for this thread!

My main question is about VPN. Is there really any way to get to use a software based RAT with a VPN which doesn't have port forwarding?

The reason I ask this is because I am looking for a VPN which is good in terms of privacy, jurisdiction and obviously price as well. So most of the VPNs which have port-forwarding are either in the 5, 9, 14 eye countries or don't have a well documented no-logging policy. My research was mainly using That One Privacy Guy's guide and I think N-o-r-d has it when it comes user privacy but unfortunately it doesn't have port-forwarding.

So is there anyway around for a software based RAT with a VPN which doesn't have port-forwarding?

Thanks,

it depends. if you can make the RAT a bind instead of reverse connection you could (doubt it). or you could buy/rent a separate server.

Pronouncer - November 16, 2018, 2:35 pm

(Nov 16, 2018 03:32 PM)sh4moon Wrote: [\[CITE\]](#) it depends. if you can make the RAT a bind instead of reverse connection you could (doubt it). or you could buy/rent a separate server.

Depends on the usage of the rat tbh. Like if you're not an idiot you can even use it on a normal VPN no problem. HTTP botnets are a bit safer in my opinion, or remote rats, on a OFFSHORE RDP paid with mixed Bitcoin

sh4moon - November 16, 2018, 2:39 pm

(Nov 16, 2018 03:35 PM)Pronouncer Wrote: [\[CITE\]](#) Depends on the usage of the rat tbh. Like if you're not an idiot you can even use it on a normal VPN no problem. HTTP botnets are a bit safer in my opinion, or remote rats, on a OFFSHORE RDP paid with mixed Bitcoin

personally I would use a vpn in combination with some things. I also wouldn't host anything on my home network. just buy a server, set it up on that, connect to the server over vpn and tor on public

WiFi.

careswho - November 16, 2018, 3:00 pm

Thanks for the reply guys. I was looking at WebMonitor but I'd like to reverse proxy which they don't support.

I'll have a look at \$\$ viability of the options you guys suggested and move from there.

wraxu - November 16, 2018, 3:04 pm

Literally all the VPNs I buy are trash. What is a decent VPN that supports port forwarding and what's a decent crypter for the higher end price range.

Business - November 16, 2018, 8:36 pm

(Nov 16, 2018 04:04 PM)wraxu Wrote: [\[CITE\]](#) Literally all the VPNs I buy are trash. What is a decent VPN that supports port forwarding and what's a decent crypter for the higher end price range. The other day I was giving a lesson and this guy bought PureVPN. I don't remember how much it was, but if it's cheap it was really nice quality. Might be worth checking out!

#Skyline just released a VPN, but port forwarding is not currently available for it.

Mustophia - November 17, 2018, 2:22 am

Hi, whats the samaritans official Weblink, thank you

Business - November 17, 2018, 2:28 am

(Nov 17, 2018 03:22 AM)Mustophia Wrote: [\[CITE\]](#) Hi, whats the samaritans official Weblink, thank you <https://hackforums.net/showthread.php?tid=5896628&highlight=Samaritans>

Armada - November 17, 2018, 2:47 am

Pfft what can I say?

I'm also part of this group, I support Business on ALL his shit cause well, he just legit AF.

Sign me up for Secondary assistance on this thread. ?

Business - November 18, 2018, 5:34 pm

(Nov 17, 2018 03:47 AM)Armada Wrote: [\[CITE\]](#) Pfft what can I say?

I'm also part of this group, I support Business on ALL his shit cause well, he just legit AF.

Sign me up for Secondary assistance on this thread. ? This is probably the most stacked RAT help desk roster I've ever seen. Glad to see you back man! ?

Thanks for the kind words!

UndeateHades - November 20, 2018, 9:32 am

(Nov 16, 2018 02:09 PM)?usiness Wrote: [\[CITE\]](#) I usually suggest Freenom as a free DNS service. That'll be perfect for starting out! Do they distribute my info?

Armada - November 20, 2018, 10:37 am

(Nov 20, 2018 10:32 AM)UndeateHades Wrote: [\[CITE\]](#) Do they distribute my info?
No, but they will ban on malicious reports.

Its a good starter though to learn.

UndeclaredHades - November 20, 2018, 4:43 pm

(Nov 20, 2018 11:37 AM)Armada Wrote: [\[CITE\]](#) No, but they will ban on malicious reports.

Its a good starter though to learn.
Works for me, TY

Business - November 22, 2018, 1:17 pm

(Nov 20, 2018 05:43 PM)UndeclaredHades Wrote: [\[CITE\]](#) Works for me, TYFeel free to request assistance here if needed.

ThanksgivingTurkey - November 22, 2018, 3:45 pm

Hi everyone, I'm having omnirat issues with persistence; I recently installed omnirat on my Xiaomi Redmi 5; got it to connect to my server and after about 5 minutes it's completely gone, should I try to reinstall? Has anyone ever had this issue, I was looking through other threads and some people were saying chinese phones have issues with persistence. On the other hand I have a samsung phone I've installed it on and it's having no issues, able to reboot/uninstall the app with it still being on. And my last question is, what would be the best way to uninstall omnirat as it has no such feature, would it just be to wipe the phone completely?

Pseudonym_96 - November 23, 2018, 9:33 am

Hello,

I set up a DNS with freenom, I set up a port forwarding rule on my router, but whenever I try to view my open port on canyouseeme, it is never seen. I am not sure where I am going wrong haha.

NYANxCAT - November 23, 2018, 9:52 am

(Nov 23, 2018 10:33 AM)Pseudonym_96 Wrote: [\[CITE\]](#) Hello,

I set up a DNS with freenom, I set up a port forwarding rule on my router, but whenever I try to view my open port on canyouseeme, it is never seen. I am not sure where I am going wrong haha.
Did you try to use the port "open the RAT" and check on canyouseeme?

Pseudonym_96 - November 23, 2018, 9:54 am

(Nov 23, 2018 10:52 AM)??` NYAN CAT ?? Wrote: [\[CITE\]](#) Did you try to use the port "open the RAT" and check on canyouseeme?

I did try to use the port on the rat and canyouseeme is not seeing the port

UPDATE: The port is open but when the stub is clicked, the RAT doesn't pick it up.

Business - November 23, 2018, 2:44 pm

(Nov 23, 2018 10:54 AM)Pseudonym_96 Wrote: [\[CITE\]](#) I did try to use the port on the rat and canyouseeme is not seeing the port

UPDATE: The port is open but when the stub is clicked, the RAT doesn't pick it up.I'll help you tonight after work man! I'd be glad to fix it for you. I won't be done at work for about 6 hours though...

Pseudonym_96 - November 23, 2018, 2:51 pm

(Nov 23, 2018 03:44 PM)?usiness Wrote: [\[CITE\]](#) I'll help you tonight after work man! I'd be glad to fix it for you. I won't be done at work for about 6 hours though...

That is roughly 11 or 12pm my time, I should still be up haha, thanks so much!

UPDATE: I bit the bullet and got a VPN with a DNS and I managed to get everything port

forwarded. Initial connection tests work, now it's time to learn about crypting stubs haha

no\$fer7u - November 24, 2018, 8:59 pm

What java RAT can I use right now? can you recommend me any please and thank you

anubis_fr - November 25, 2018, 8:57 am

Hello Sir,

What is the best cheap way to be 24h/24h available by a client please ? I cannot find a RDP seller who allows portforwarding + disabling Windows Defender. Admin RDP are pretty more expensive.

Maybe something with a VPS ?

Thanks

Business - November 25, 2018, 9:45 am

(Nov 25, 2018 09:57 AM)anubis_fr Wrote: [\[CITE\]](#) Hello Sir,

What is the best cheap way to be 24h/24h available by a client please ? I cannot find a RDP seller who allows portforwarding + disabling Windows Defender. Admin RDP are pretty more expensive.

Maybe something with a VPS ?

ThanksNot sure what you mean? Do you just want to have access to your RAT from any PC?

anubis_fr - November 25, 2018, 11:42 am

(Nov 25, 2018 10:45 AM)?usiness Wrote: [\[CITE\]](#) Not sure what you mean? Do you just want to have access to your RAT from any PC?

Thanks for answering

Not exactly, in fact I just would like to have my server running 24h/24h.

For example if the server is running while I'm not on my PC, my clients should be able to be updated with a scheduled task as soon as they connect, right ?

Sorry if it's hard to understand, I'm not a native english speaker.

Business - November 25, 2018, 4:16 pm

(Nov 25, 2018 12:42 PM)anubis_fr Wrote: [\[CITE\]](#) Thanks for answering

Not exactly, in fact I just would like to have my server running 24h/24h.

For example if the server is running while I'm not on my PC, my clients should be able to be updated with a scheduled task as soon as they connect, right ?

Sorry if it's hard to understand, I'm not a native english speaker.Why do they need to be updated if they're connected fine?

I have some time on my hands now guys! PM me for assistance.

UndeatedHades - November 25, 2018, 5:34 pm

(Nov 22, 2018 02:17 PM)?usiness Wrote: [\[CITE\]](#) Feel free to request assistance here if needed.

I could really use some help setting up freenom right about now

Business - November 25, 2018, 5:36 pm

(Nov 25, 2018 06:34 PM)UndeateadHades Wrote: [\[CITE\]](#) I could really use some help setting up freenom right about nowOk, register a domain and create an account, then I will set it up for you!

UndeateadHades - November 25, 2018, 5:36 pm

(Nov 23, 2018 03:51 PM)Pseudonym_96 Wrote: [\[CITE\]](#) That is roughly 11 or 12pm my time, I should still be up haha, thanks so much!

UPDATE: I bit the bullet and got a VPN with a DNS and I managed to get everything port forwarded. Initial connection tests work, now it's time to learn about crypting stubs haha
What VPN did you get.

(Nov 25, 2018 06:36 PM)?usiness Wrote: [\[CITE\]](#) Ok, register a domain and create an account, then I will set it up for you!

Doing it now, mind adding me on discord?

Business - November 25, 2018, 5:42 pm

(Nov 25, 2018 06:36 PM)UndeateadHades Wrote: [\[CITE\]](#) What VPN did you get.

Doing it now, mind adding me on discord?Just reply here once you have it and I'll PM you.

UndeateadHades - November 25, 2018, 5:42 pm

(Nov 25, 2018 06:42 PM)?usiness Wrote: [\[CITE\]](#) Just reply here once you have it and I'll PM you.
I've made my account and claimed my domain.

(Nov 25, 2018 06:42 PM)?usiness Wrote: [\[CITE\]](#) Just reply here once you have it and I'll PM you.
Messaged you too

Fixed my DNS for me in under 10 minutes this guy is where it's at big vouch!

Pseudonym_96 - November 25, 2018, 6:57 pm

(Nov 25, 2018 06:36 PM)UndeateadHades Wrote: [\[CITE\]](#) What VPN did you get.

Doing it now, mind adding me on discord?

I got a year package with PhyberVPN. They are having a Black Friday/week sale. it is \$10 for the year currently.