

Forum:[Hack Forums](#)

Thread: [\[Remote Administration\] Kief's first line of aid.](#)

Purple Kief - October 6, 2016, 9:23 am

This thread was created as a first line of aid for the people that kept adding me on Skype. I currently do not offer any helping service please refrain from commenting on this thread.

This holds a very minimal amount of information but should be good enough to get you going. Now let's start off by asking, what are you looking for? I'll try to split this into 5 categories: Port forwarding, DNS, recommendations, crypting and testing your stub.

Port Forwarding

Spoiler [\(Click to View\)](#)

I KNOW ALRIGHT! Your damn port refuses to open no matter what you do. Aren't you lucky ports can't say no to me.

Check out the following: <https://hackforums.net/showthread.php?tid=5327327>

You're looking for: The 'port forwarding' section followed by the 'testing your port' section.

Keep in mind:LISTEN TO THE DAMN PORT!!

For every RAT you use you MUST use a different port!

Use a 5 digit port!

Don't use a port that was already open! (ex. 80)

Your firewall MUST be disabled when testing!

Done everything? Nothing working?: Feel free to contact me again. NOTE: If your issue is clearly described in my guide I will INSTANTLY block you from my skype. It's also important to mention it to me if my guide is not clear, it's not your fault if you can't understand a part of my guide but are trying your best.

DNS

Spoiler [\(Click to View\)](#)

Probably wondering what DNS to use and how to set it up.

Check out the following: <https://hackforums.net/showthread.php?tid=5327327>

You're looking for: The 'setting up a DNS' section followed by the 'testing your DNS' section.

Keep in mind:fagdns.su is no longer operational. (shoutout to lapanthere for keeping it going all this time)

Done everything? Nothing working?: Feel free to contact me again. NOTE: If your issue is clearly described in my guide I will INSTANTLY block you from my skype. It's also important to mention it to me if my guide is not clear, it's not your fault if you can't understand a part of my guide but are trying

your best.

Crypting

Spoiler ([Click to View](#))

What crypter should I buy? What settings should I use? IT'S GIVING ME 11/35!!!!

Check out the following: <https://hackforums.net/showthread.php?tid=5327327>

You're looking for: The 'setting up a RAT' section followed by one of the crypters all the way in the bottom of my guide.

Keep in mind: Crypting isn't always easy!

When using startup in: Orcus, Imminent Monitor, ONLY use self injection!

Make sure you have a HQ icon ready: <https://hackforums.net/showthread.php?tid=5182868>

For assembly use a popular program that's not overused.

Scan your files ONLY on: <http://pscan.xyz> or <http://scan.majyx.net>

Done everything? Nothing working?: Feel free to contact me again. NOTE: If your issue is clearly described in my guide I will INSTANTLY block you from my skype. It's also important to mention it to me if my guide is not clear, it's not your fault if you can't understand a part of my guide but are trying your best.

Testing your stub

Spoiler ([Click to View](#))

NOTE: This was taken from my massive guide.

<https://hackforums.net/showthread.php?tid=5327327>

So you've set up your RAT according to my guide and are ready to test your stub.

Only a matter of understanding what IP you need to use inside of your builder for different situations.

Using the wrong IP inside of your builder usually leads to no connection. As most of you might think there's multiple IP's to use in multiple situations. You can find them down below.

BUILD YOUR STUB ACCORDING THE 'SETTING UP YOUR RAT' SECTION!

Alot of you are testing your stubs the wrong way, making you think things are broken while that might actually not be the case. Here's how you test your stub properly. (All of this assumes you are running your RAT on your actual pc and not somewhere else)

Where am I testing my stub?

- 1) On the same computer you're running your RAT on.
- 2) On a VM on the same computer that you're running your RAT.
- 3) A different computer in the same network.
- 4) An outside computer outside of your network.

What IP do I need for that?

- 1) SAME COMPUTER = localhost or 127.0.0.1
- 2) VM SAME COMPUTER = Your IPv4 or when using a VPN your public IP (found at

canyouseeme.org)

3) Different computer same network = Your IPv4 or when using a VPN your public IP (found at canyouseeme.org)

4) Computer outside of your network = Your public IP found at canyouseeme.org or your DNS.

Couple of examples.

1) Testing on my own computer --> <https://gyazo.com/26352d88a01457884aa949c5a32949e6>

2) Testing on my own VM (no VPN) --> <https://gyazo.com/6b9590b953c96285083efb9894c1aea2>

3) Testing outside of network --> <https://gyazo.com/2f3586ac057ed84882e55c3e2681d07c>

HELP NO CONNECTION!!

Calm down, don't panic. This guide WILL have the fix you're looking for but start by checking the following:

- Is my stub crypted? Always test connections uncrypted! This way you'll know if it was your crypter that broke the stub or not.

- Did my AV remove it? It might not look like it, but this is the case 95% of the time. Go check if the process is actually running.

- Am I being a dumbo? Did you misread a portion of my guide? It's very possible, go read over it again.

Done everything? Nothing working?: Feel free to contact me again. NOTE: If your issue is clearly described in my guide I will INSTANTLY block you from my skype. It's also important to mention it to me if my guide is not clear, it's not your fault if you can't understand a part of my guide but are trying your best.

Recommendations 01/03/2018

Spoiler ([Click to View](#))

NOTE: I will update this as my personal preferences change so you guys will always have the most optimal equipment.

KIEF PLZ WHAT RAT DO I BUY? WHAT VPN? DNSS??!!

RAT: Imminent Monitor 5.0

Explanation: I'll be the first to say it alright, Imminent is currently dominating the market. (not to mention it's only 25\$) It has the fastest remote destkop, pretty much all features every other RAT has (yes even the UAC bypass) and I know for a fact Shockwave is actively developing more features. Stability is great, support is great, overall a TOP tool right now.

Crypter: Data protector v4

Explanation: No matter which way you look at it, data's runtime is currently unmatched on HF. Not only that, it does support all major RATs fully. Downpart being the crypter is .net reliable meaning that if you've got a native RAT (ex: babylon, #) you're adding .NET dependencies that wouldn't be there otherwise.

DNS: Armada's DNS

Explanation: Been using it for a while. Armada is professional when need be, the DNS's work as intended and with free replacements if they go down it's really all you could ask for.

If you're interested in buying this I suggest you tell me personally. Deal times will decrease by 100% and I might even be able to cut you a deal.

VPN: Crypticvpn -- Crypticvpn.com

Explanation: Has the most servers you can PF on, cleanest website and client interface. Support is great too.

Don't do ANY of this. I WILL slap you.

Spoiler ([Click to View](#))

RAT Related

- Do not use Darkcomet for the reason that it has serious security flaws. (I will deny you help if you insist on using this RAT)
- Do not use Blackshades for the reason the police took over the product.
- Do not use NO-IP for the reason that it is monitored by Microsoft.
- Do not use duckDNS for the reason that they'll give you honeypots.
- Never use the same port for 2 RATs. (or program in general)
- Participate in banking fraud.
- Participate in carding.

Crypter Related

- Use startup in both crypter and RAT.
- Use any settings in both crypter and RAT.
- Never crypt a crypted file.
- Inject into a process when using startup on a .NET RAT. (Ex. Luminosity)
- Do not cry to crypter owners about a 10/35 detection rate, it's your own fault.
- Assume scantime and runtime is the same.
- Do not use the website <http://www.virustotal.com>

Rottapotta - October 6, 2016, 9:32 am

Oh a new update? Will check this out!

EDIT: I suggest you to add "Do not use No-IP, since Microsoft has it in their control!"

Purple Kief - October 6, 2016, 9:51 am

(Oct 6, 2016 09:32 AM)Rottapotta Wrote: [\[CITE\]](#) EDIT: I suggest you to add "Do not use No-IP, since Microsoft has it in their control!"

Whoops, looks like I forgot something. :)

Also forgot my recommended VPN in my recommendations.

Thanks bud.

\$lick - October 6, 2016, 9:57 am

Thanks for recommending NanoCore as the best RAT to use ??

Yolosmokecrack - October 6, 2016, 12:44 pm

this thread is HQ, hopefully this will stop the mass amount of repeated questions !

President Morty - October 6, 2016, 12:46 pm

(Oct 6, 2016 12:44 PM)Yolosmokecrack Wrote: [\[CITE\]](#) this thread is HQ, hopefully this will stop the mass amount of repeated questions !

It won't.

PhoenixBYTE - October 6, 2016, 1:50 pm

(Oct 6, 2016 12:46 PM)Xylos Wrote: [\[CITE\]](#) It won't.

Agreed, I don't understand how people are so dumb though, there are so many RAT helpdesks but they still ask the same old questions, this is getting so tiring, there should be a sticky of RAT Helpdesks so certain people can have it right in front of their faces .-.

#Skyline - October 6, 2016, 3:47 pm

(Oct 6, 2016 09:23 AM)Purple Kief Wrote: [\[CITE\]](#) From doing this for quite a while now I've realised that if you spoonfeed people they tend to not understand anything.

I've been here longer to tell you it won't change anything.

You can give them all the answers, but they'll still ask.

However threads like these do minimize the repetitive questions. ?

StaveArkle - October 6, 2016, 3:52 pm

Good thread. You should add the Freedom domain method to DNS.

Purple Kief - October 9, 2016, 2:29 pm

(Oct 6, 2016 03:47 PM)#Skyline? Wrote: [\[CITE\]](#) I've been here longer to tell you it won't change anything.

You can give them all the answers, but they'll still ask.

However threads like these do minimize the repetitive questions. ?You've not only been here longer, you're also way more experienced.

(Oct 6, 2016 03:52 PM)StaveArkle Wrote: [\[CITE\]](#) Good thread. You should add the Freedom domain method to DNS.Thanks, I guess?

Was gone for a bit, added everyone on skype will deal with the rest tomorrow. :)

VirtualMon3y - October 9, 2016, 2:58 pm

Keep up the hard graft Kief my man you are always trying to help out members. Peace... ?

HDThree - October 10, 2016, 5:32 am

Thanks for the guide. Keep up the HQ threads!

needhelp5 - October 13, 2016, 10:25 am

Thanks for the guide man !

BlueDarts - October 14, 2016, 6:37 am

thanks for all the suggestions man ?

NapoleonicCode - December 6, 2016, 10:28 am

Thanks for the help ?

aerohack - December 10, 2016, 11:48 am

Excellent thread and very detailed!

I have some questions:

Port Forwarding

- What is the difference between using a 4 and 5 digit port? Why 5 digits port is better?

DNS

- DynDNS is a good alternative to NO-IP?

Crypting

- Which Crypters do you recommend to use with Luminosity Link and Imminent Monitor?
- Do you know some Crypter that install the server on MBR sector? (Survive format OS)

Thanks!

olomosch - January 3, 2018, 4:58 am

I have a Question.

I tested the client an another pc outside of network and i can't get any connection. :(

ImSimplyNameless - January 3, 2018, 5:01 am

(Jan 3, 2018 05:58 AM)olomosch Wrote: [\[CITE\]](#) I have a Question.

I tested the client an another pc outside of network and i can't get any connection. :(

I've send you a pm about this, you most likely didn't open your ports properly

Armada - January 3, 2018, 5:15 am

Kief buddy, you gotta update this OP thread....

Purple Kief - January 3, 2018, 6:48 am

(Jan 3, 2018 05:58 AM)olomosch Wrote: [\[CITE\]](#) I have a Question.

I tested the client an another pc outside of network and i can't get any connection. :(

Please go here: <https://hackforums.net/showthread.php?tid=5327327> and read the testing your binary section. If that does not help you I currently do not offer any helping services, my apologies.

(Jan 3, 2018 06:15 AM)Armada Wrote: [\[CITE\]](#) Kief buddy, you gotta update this OP thread....

Done, sorta.