

Forum:[Hack Forums](#)

Thread: [How does reverse TCP work](#)

jordima - January 27, 2018, 2:46 pm

When trying to use Quasar, we've been told we need to open a port at the receiving end (which we cannot).

I heard that you should use something called reverse TCP. Anyone knows how this works?

When we now send our Quasar created virus, it deploys... but does not get back in touch with the laptop we want to use to control the "slave" laptop.

CyberStrike - January 27, 2018, 3:00 pm

Basically after execution of the file in question the target machine will connect back to your computer of course you have to use your IP and make sure that the port being used is open, so you may have to set portforwarding in your router. You may also have to double check and make sure that your Windows firewall doesn't interfere and open up that port as well.

jordima - January 27, 2018, 3:09 pm

(Jan 27, 2018 04:00 PM)sirru5h Wrote: [\[CITE\]](#) Basically after execution of the file in question the target machine will connect back to your computer of course you have to use your IP and make sure that the port being used is open, so you may have to set portforwarding in your router. You may also have to double check and make sure that your Windows firewall doesn't interfere and open up that port as well.

But that is a forwarding at our end we switch on and a port our end we open?

Armada - January 27, 2018, 3:24 pm

(Jan 27, 2018 04:09 PM)jordima Wrote: [\[CITE\]](#) But that is a forwarding at our end we switch on and a port our end we open?

You still have to open your ports dude... nothing else to cut about, ports not forwarded means no connectivity.

If I am not mistaken Quasar uses a secondary port for the Reverse proxy and connection settings, so that will need to likely be opened as well depending on your network configuration.

jordima - January 27, 2018, 5:52 pm

(Jan 27, 2018 04:24 PM)Armada Wrote: [\[CITE\]](#) You still have to open your ports dude... nothing else to cut about, ports not forwarded means no connectivity.

If I am not mistaken Quasar uses a secondary port for the Reverse proxy and connection settings, so that will need to likely be opened as well depending on your network configuration.

But it does mean we do not need to open anything at the receiver's end. Correct?

Armada - January 27, 2018, 10:39 pm

(Jan 27, 2018 06:52 PM)jordima Wrote: [\[CITE\]](#) But it does mean we do not need to open anything at the receiver's end. Correct?

What? No....

I seriously hope you guys are not hoping on careers in Network configurations if you are asking

these type of questions.

quasar, like MAJORITY of RATs have a 2 piece configuration.

The Controller (Administrative)

The Binary Client.

The controller, aka the Administrative portion will always need ports forwarded, otherwise it is impossible to receive incoming client requests.

The binary clients require no port forwarding, they just have to be able to communicate with the internet itself. (No DMZ, etc)

CyberStrike - January 28, 2018, 4:28 am

OP .. reverse connections are used because firewalls do not block outgoing traffic, but incoming, say as a bind shell, for example traffic would be heading towards the target hence why the firewall would be more likely to block that. Easiest way to think of it is if it is going out the user is doing it, so the firewall is fine with it, someone trying to connect is bad unless the firewall is configured for that. (I dunno if this makes sense think of this out going is good incoming is bad) So to your router's firewall you will have a connection coming in so you have to open that port and forward the traffic to the right computer that will be listening.

jordima - January 28, 2018, 5:09 am

(Jan 28, 2018 05:28 AM)sirru5h Wrote: [\[CITE\]](#) OP .. reverse connections are used because firewalls do not block outgoing traffic, but incoming, say as a bind shell, for example traffic would be heading towards the target hence why the firewall would be more likely to block that. Easiest way to think of it is if it is going out the user is doing it, so the firewall is fine with it, someone trying to connect is bad unless the firewall is configured for that. (I dunno if this makes sense think of this out going is good incoming is bad) So to your router's firewall you will have a connection coming in so you have to open that port and forward the traffic to the right computer that will be listening.

Thank you, Sirru5h ? Most kind as explanation.

(Jan 27, 2018 11:39 PM)Armada Wrote: [\[CITE\]](#) What? No....

I seriously hope you guys are not hoping on careers in Network configurations if you are asking these type of questions.

quasar, like MAJORITY of RATs have a 2 piece configuration.

The Controller (Administrative)

The Binary Client.

The controller, aka the Administrative portion will always need ports forwarded, otherwise it is impossible to receive incoming client requests.

The binary clients require no port forwarding, they just have to be able to communicate with the internet itself. (No DMZ, etc)

? No, you're right. I would not fit well in network configuration or IT (my anecdote of what happened at my programming exam at Uni in my intro to this forum is telling ?).

Now we seem to probably struggle with this portforwarding.

It is explained everywhere how you configure Quasar, how you create the virus, but not how you set up the portforwarding well. :(

Armada - January 28, 2018, 4:11 pm

(Jan 28, 2018 06:09 AM)jordima Wrote: [\[CITE\]](#) Thank you, Sirru5h ? Most kind as explanation.

? No, you're right. I would not fit well in network configuration or IT (my anecdote of what happened at my programming exam at Uni in my intro to this forum is telling ?).

Now we seem to probably struggle with this portforwarding.
It is explained everywhere how you configure Quasar, how you create the virus, but not how you set up the portforwarding well. :(
SO tempted to whip open Visio up and make a diagram but I have done this way too many times already.

Basically your own network is firewalling your ass off from connections.

So, you have not opened your communication channels likely on your controllers router firewall.
Simply open the port and forward it to the correct internal IP#, and you are set to go.

jordima - January 28, 2018, 5:24 pm

(Jan 28, 2018 05:11 PM)Armada Wrote: [\[CITE\]](#) SO tempted to whip open Visio up and make a diagram but I have done this way too many times already.

Basically your own network is firewalling your ass off from connections.

So, you have not opened your communication channels likely on your controllers router firewall.
Simply open the port and forward it to the correct internal IP#, and you are set to go.

Thanks. Will need to show this to my IT friend who's helping as I am lost meanwhile ?

CyberStrike - January 28, 2018, 5:26 pm

Well glad that the explanation helped that said learning a bit about networking won't hurt.

jordima - January 28, 2018, 5:35 pm

(Jan 28, 2018 06:26 PM)sirru5h Wrote: [\[CITE\]](#) Well glad that the explanation helped that said learning a bit about networking won't hurt.
Drinking from the firehose ?

Or how in adversity, you can have a positive side.

CyberStrike - January 28, 2018, 7:09 pm

lol at first it seems like that but stick with it, simple networking don't worry about the hacking stuff yet. Hacking and math are pretty much the same if you can't add/subtract/multiply/divide how will you do fractions or anything more.

http://www.tcpipguide.com/free/t_NetworkingFundamentals.htm
<https://www.gns3.com/>

Armada - January 28, 2018, 7:41 pm

(Jan 28, 2018 08:09 PM)sirru5h Wrote: [\[CITE\]](#) lol at first it seems like that but stick with it, simple networking don't worry about the hacking stuff yet. Hacking and math are pretty much the same if you can't add/subtract/multiply/divide how will you do fractions or anything more.

http://www.tcpipguide.com/free/t_NetworkingFundamentals.htm
<https://www.gns3.com/>

The more I see you post this stuff the more I am starting to like you.

He is right guys, if you cant do math, fucking forget about subnetting.. Its all math, and its a pain in the ass, and I am GOOD at math, and it still annoys me. ?

CyberStrike - January 28, 2018, 9:52 pm

(Jan 28, 2018 08:41 PM)Armada Wrote: [\[CITE\]](#) The more I see you post this stuff the more I am starting to like you.

He is right guys, if you cant do math, fucking forget about subnetting.. Its all math, and its a pain in the ass, and I am GOOD at math, and it still annoys me. ?

Thank you Armada and great example about how subnetting you need to have a bit of math. Guys don't forget IPv6 (which is going to be the standard) is hexadecimal and programs those ascii characters are converted to ASM again hex comes into the picture then to binary so the machine can understand, it sounds really dumb but math is literally how computers work at the end of the day it's binary, like look when you do a simple printf it is making kernel calls (when we reverse it in radare2 we will see it) we may look at something like this

```
Code #include <stdio.h>
int main()
{
    // printf() displays the string inside quotation
    printf("Hello, World!");
    return 0;
}
```

Code ./hello
Hello, World!

So after we compiled it we get our "Hello World!" statement but it goes from something people can understand "Hello, World!" to hex looks like this now "48 65 6c 6c 6f 2c 57 6f 72 6c 64 21" if we run it in a debugger we will find this value

Code 0x7fff7a51d90 -> Name: __printf(format=0x5555555546f4 "Hello, World!")
x/30wx \$rdi
0x5555555546f4: 0x6c6c6548 0x57202c6f 0x646c726f 0x00000021
Note it is backwards due to endianness.

That is a small example, if you are wondering "Why the hell do I need to know this shit?!" Simple this is part of the process to develop your own exploits and even simpler reason it's how a computer interprets what we do when issuing a command, even if you use someone elses exploit learning how it works is quite important. If I was to dump(print) the value or that register in binary I will get a series of 0 & 1's but that is binary, what the computer understands.

No one is saying go get a minor in math, but at some point you will want to advance, be it in knowledge or career. If you apply yourself to networking/coding anything fucking dog training you will fail that is fine, but get back up and analyse what went wrong and try again. It's important to look objectively at what skills are needed and go get familiar with these skills, in the case of computers a bit of math is required (probably no more than college algebra for most tasks). You will find that if say you suck at whatever and you do it day in day out even for 15 minutes that "I suck at ..." will resolve itself.

Edit: Added screen shot from radare2 showing visually "Hello,World!"
[https://imgur\[.\]com/a/PTeOV](https://imgur[.]com/a/PTeOV)

jordima - January 29, 2018, 5:22 am

Thanks :)

The thing that doesn't compute yet with me is why I've always been considered reasonably good at math's and building (mathematical) architecture for software packages... but I understand bugger all about coding ?

jordima - February 2, 2018, 4:10 am

Many thanks to the helpers here.

We figured out that our ISP did not allow opening a port in the router. It had to be done on the login page of the ISP.

This is now solved and all works.

Thanks

CyberStrike - February 2, 2018, 9:55 am

Excellent best of luck I am sure that you guys will get this all resolved. ;)

jordima - February 2, 2018, 10:13 am

(Feb 2, 2018 10:55 AM)sirru5h Wrote: [\[CITE\]](#) Excellent best of luck I am sure that you guys will get this all resolved. ;)

Well, even if don't, at least I learned a lot ?