

Forum:[Hack Forums](#)

Thread: [Technical Misconceptions of R.A.Ts Explained](#)

Armada - June 23, 2015, 9:16 pm

So, I got some time on my hands tonight, and have decided to write something up for clarification and general informational uses to all members involved in the RAT community.

This document is not meant to "Break your understanding" of Remote Administrative Tools. But to correct some typical misconceptions associated to this type of software.

Lets dive right in

Firstly, the history.

- Remote Administrative Tools (Legit or otherwise) are as the description states, software designed to remotely administrate another machine across the network (internet).

- Origins of this type of technology go back to some of the earlist of computer networking. There was a need to access and issue commands and code to servers and services without the administrator having to get off their fat ass to actually physically go input the command line. Thus the advent of remote admin concept.

Trojan/Backdoor/RAT Basics:

R.A.Ts or Trojan viruses are nothing more than a client/server application suite.

Its pretty basic in technical standards really.

Lets take a look at figure 1 here.

Figure 1 demonstrates the most simplistic form of client/server communication.

The Client will connect to the server for its services.

Now, this same theory "Back in my day" (Damn I feel older and older everytime I say this one) We distributed "Servers"

- And I say "Servers" in the sense the Hackers terminal HAD to remotely establish a connection the the infected machine as per Figure 1.

Lets go more complex a little more, and assume Hacker has more than a single infected machine.
Figure 2

In figure 2 we clearly see the Hacker has access to numerous infected terminals, However the Hackers terminal MUST connect to the infected slaves.

Armada, your talking gibberish, it doesn't work that way!

- Absolutely correct. NOW.

That last part was a History lesson for the new comers.

NOW

- Here is where the technical misconception stands.

Where Figure 1 and 2 the Hacker connected to the infected machines. This is clearly no longer the case. With the advent of Firewall technology and anti viral/internet protective suites, hackers had to find another method to success.

Fire walls block incomming connections be default, hindering the "Old style" trojan/RAT software obsolete. If the end Admin(Hacker) can not connect to the machine, whats the use, right?

Thus later revisions of the software started to instead of broadcasting the host IP# of the infected terminal, now "Calls home" - IE checks in to what is commonly called the "Client"

The TECHNICAL MISCONCEPTION.

Looking at figure 1 and 2 it should be apparent to anyone with a bit of networking knowledge. In this new scenario of Infected host calling home to the Hacker, the roles have now been reversed.

Figure 3 - Todays RAT networking topology

In this scenario, the infected machines(slaves) check in to the Command and Control Console (Hackers terminal).

This effectively by ALL NETWORKING DEFINITION makes the Hackers terminal now the server, and the infected slaves the clients.

Clients connect to servers for the associated services. NEVER the other way around.

Confused yet? ?

I dont blame you one bit. This is a technical aspect to backdoor administration that has long gone uncorrected, but has been incorrect since the day our infected terminals started calling home to us instead of us connecting to them.

And frankly, it bothers the hell out of me to see new users being taught improper networking under the guise of "Its easier to understand"

- Easier to understand is NOT technically correct and should under NO CIRCUMSTANCE be encouraged or enforced. (IMO)

So to recap or tl;dr

Binaries considered "Clients" are in fact the management servers

and the "servers" are technically the clients of the management server in question.

I tried to simplify as much as possible for the new users. ?

- Further note, I dont have any hope on this changing a damn thing, but the technical incorrectness has always bothered me on this one.

Cheers everyone. ?

Cheese - June 23, 2015, 9:23 pm

Nice explanation, I'm sure this will give a lot of users an idea how this works.

Thanks for this ?

KFC Watermelon - June 23, 2015, 9:39 pm

The builder in Luminosity is called "Client Binary Builder". It clearly says client builder numerous times. People still save it as "Server.exe".

Armada - June 24, 2015, 12:11 am

(Jun 23, 2015 09:39 PM)KFC Watermelon Wrote: [\[CITE\]](#) The builder in Luminosity is called "Client Binary Builder". It clearly says client builder numerous times. People still save it as "Server.exe". The exact technical misconception I am attempting to address here!

Nice to see a actual software developer of these applications confirm my statements on this. Respect ?

21st Century Schizoid Man - June 24, 2015, 12:15 am

Nice thread my friend! ?, It is really interesting to me how rats work.

Mr. Dr. Prof. Patrick - June 24, 2015, 1:47 am

There is no misconception, and a reverse connection can be argued anyway a person see fit, though the Infected PCs connect to the the Hacker PC, Never Once does the Infected PCs make a request

the Binary accepts requests and answers accordingly - the exact definition of a server, it hardly matters who initiates the connection whether the server or the client.

So by definition calling the Stub/Binary/Infected PC a server is absolutely correct

Armada - June 24, 2015, 1:50 am

(Jun 24, 2015 01:47 AM)Mr. Dr. Prof. Patrick Wrote: [\[CITE\]](#) There is no misconception, and a reverse connection can be argued anyway a person see fit, though the Infected PCs connect to the the Hacker PC, Never Once does the Infected PCs make a request

the Binary accepts requests and answers accordingly - the exact definition of a server, it hardly matters who initiates the connection whether the server or the client.

So by definition calling the Stub/Binary a server is absolutely correct

Absolutely Incorrect.

Client/Server communication is SIMPLISTIC

The fact the roles have been reversed changes nothing.

Infected terminal (CLIENTS) connect to the Master (Server) and await commands.

This is the literal definition of client/server communication.

The Programmer of one of the most popular R.A.T.s on the HF market confirms this exact principal in his OWN software.

Bo Burnham - June 24, 2015, 1:51 am

This is great!

Hopefully this should clear it up for some people ^^

Thanks Armada :D

Armada - June 24, 2015, 1:54 am

(Jun 24, 2015 01:51 AM)H?tman™ Wrote: [\[CITE\]](#) This is great!

Hopefully this should clear it up for some people ^^

Thanks Armada :D
Once in a while i try lolz :)

Mr. Dr. Prof. Patrick - June 24, 2015, 2:00 am

server : [https://en.wikipedia.org/?title=Server_\(computing\)](https://en.wikipedia.org/?title=Server_(computing))

client-server: https://en.wikipedia.org/wiki/Client%E2%80%93server_model

see this: "A client does not share any of its resources, but requests a server's content or service function."

NOWHERE does it say it matters who connects to who. funny how your argument is based on that

Rikanono - June 24, 2015, 5:58 am

You are both right. you are just talking about 2 different things.

in OSI layer 4 the Server is the one that opens the port (hacker)
so if u talk about a "connection" hacker =Server slave=client

in OSI layer 7 the Server is the one that Servers you with data\information (slave)
so if you talk about an "application" hacker=client slave=Server

Mr. Dr. Prof. Patrick - June 24, 2015, 6:42 am

(Jun 24, 2015 05:58 AM)Rikanono Wrote: [\[CITE\]](#) You are both right. you are just talking about 2 different things.

in OSI layer 4 the Server is the one that opens the port (hacker)
so if u talk about a "connection" hacker =Server slave=client

in OSI layer 7 the Server is the one that Servers you with data\information (slave)
so if you talk about an "application" hacker=client slave=Server

The type of connection a R.A.T uses has already been classified as a reverse connection you can read more about it here:

<https://help.gnome.org/users/vinagre/stable/connect-reverse.html.en>

the OP refuses to accept this and decided to bask in his own ignorance

Vuln - June 24, 2015, 9:29 am

There are no misconceptions about how reverse connections work, only about the "official" client/server terminology. There are a lot of different yet widely accepted definitions floating around, so I would like to know what your source is.

There's no point in arguing if you don't provide proof to back up your claims.

Armada - June 24, 2015, 10:53 am

(Jun 24, 2015 05:58 AM)Rikanono Wrote: [\[CITE\]](#) You are both right. you are just talking about 2 different things.

in OSI layer 4 the Server is the one that opens the port (hacker)
so if u talk about a "connection" hacker =Server slave=client

in OSI layer 7 the Server is the one that Servers you with data\information (slave)
so if you talk about an "application" hacker=client slave=Server Facepalms

Honestly, What in the hell do the OSI layers have to do with people wrongly classifying Clients and servers?

And secondly, your incorrect.

The Infected machine does not serve the information to the Master host.(Hacker terminal) It connects and WAITS FOR COMMANDS.

Thus by literal network definition making it a Client machine.

This stuff is not rocket science, but simplistic networking.

Rikanono - June 24, 2015, 11:43 am

(Jun 24, 2015 10:53 AM)A?mªĐa Wrote: [\[CITE\]](#) *Facepalms*

Honestly, What in the hell do the OSI layers have to do with people wrongly classifying Clients and servers?

And secondly, your incorrect.

The Infected machine does not serve the information to the Master host.(Hacker terminal) It connects and WAITS FOR COMMANDS.

Thus by literal network definition making it a Client machine.

This stuff is not rocket science, but simplistic networking.i am not incorrect.

http Webserver:

client connects to Server. Server Waits for Command. clients asks for a webpage. server servs this information.

RAT reverse connection:

slave connects to hacker. slave waits for command. hacker sends command (regeest screenshot). slave serves this information and sends the screenshot.

osi layer 4 the hacker is the server and serves the open port and waits for the connection

osi layer 7 the slaves is the server waits 4 commands and serves the requested information.

hope this clears things up now.

and i am sorry if you feel attackd by me, but i did not read your threads or posts. i just saw this thread here. so i just dont understand your reaction and why you are so pissed.

Armada - June 24, 2015, 11:48 am

(Jun 24, 2015 11:43 AM)Rikanono Wrote: [\[CITE\]](#) i am not incorrect.

http Webserver:

client connects to Server. Server Waits for Command. clients asks for a webpage. server servs this information.

RAT reverse connection:

slave connects to hacker. slave waits for command. hacker sends command (request screenshot). slave serves this information and sends the screenshot.

osi layer 4 the hacker is the server and serves the open port and waits for the connection

osi layer 7 the slaves is the server waits 4 commands and serves the requested information.

hope this clears things up now.

and i am sorry if you feel attackd by me, but i did not read your threads or posts. i just saw this thread here. so i just dont understand your reaction and why you are so pissed.

- THIS IS NOW A WEB SERVER THREAD -

But seriously.

When it comes to HTTP botnets, your correct, I openly admit this.

This thread was written with the "Typical" Client/server process in mind however. Im not threatened, but this is going off topic from the initial post, HTTP protocol bots really do deserve their own thread, maybe you can write something up for it? ?

Niko - June 24, 2015, 12:04 pm

This was very in depth. Nice explanation A?m^aĐa

Vuln - June 24, 2015, 12:50 pm

(Jun 23, 2015 09:16 PM)A?m^aĐa Wrote: [\[CITE\]](#) This effectively by ALL NETWORKING DEFINITION makes the Hackers terminal now the server, and the infected slaves the clients.

The bold part is plain wrong, whether you like it or not. Which is exactly why there are so many "misconceptions"...

(Jun 24, 2015 11:05 AM)A?m^aĐa Wrote: [\[CITE\]](#) No more free info from me, idiots ruined it for everyone else who might have found use in this stuff.

Maybe you should consider backing up your claims next time.

Coton Pker - June 24, 2015, 1:39 pm

I thought it was common knowledge that the server(slaves) sent to the client(admin) routinely. that's the reason it's not an incoming connection that'll make a firewall go nuts.

?Syria - June 24, 2015, 1:57 pm

(Jun 23, 2015 09:39 PM)KFC Watermelon Wrote: [\[CITE\]](#) The builder in Luminosity is called "Client Binary Builder". It clearly says client builder numerous times. People still save it as "Server.exe". its not "Client Binary Builder" its "Server Builder" :P

KFC Watermelon - June 24, 2015, 2:04 pm

(Jun 24, 2015 01:57 PM)?Syriamanal Wrote: [\[CITE\]](#) its not "Client Binary Builder" its "Server Builder" :P

The terminology I use in Luminosity is that the client initiates the connection to the server. Just as

your web browser would to google. Rikanono and others can be technically correct as well, since the server is "serving" you data and information. Fun fact: In Reverse Proxy - On Luminosity - your proxies are referred to as servers. Your clients start a reverse proxy server for you to connect to. However, port forwarding is not required on your clients, so it completely bypasses firewalls.

NanoCore/IM/Luminosity/Babylon all use the same terminology - "client" are your remote computers. And it makes sense, too. In my mind, there is one server, and numerous clients. That's how I've always seen it.

?Syria - June 24, 2015, 2:11 pm

(Jun 24, 2015 02:04 PM)KFC Watermelon Wrote: [\[CITE\]](#)

The terminology I use in Luminosity is that the client initiates the connection to the server. Just as your web browser would to google. Rikanono and others can be technically correct as well, since the server is "serving" you data and information. Fun fact: In Reverse Proxy - On Luminosity - your proxies are referred to as servers. Your clients start a reverse proxy server for you to connect to. However, port forwarding is not required on your clients, so it completely bypasses firewalls.

NanoCore/IM/Luminosity/Babylon all use the same terminology - "client" are your remote computers.

you sure?

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

QU?CKSILVER - June 24, 2015, 4:05 pm

Stop arguing, there's some sort of confusion here that needs to be solved...

Believe it or not, the infected client is literally a "server" because it serves data to the attacker, just as a server would do to a client requesting something out of it. In a reverse connection scenario, both (the client and the attacker) are both "servers", but mainly the "attacker", which is the one that actually HANDLES incoming connections and SHARES resources with clients. The client itself answers to calls (commands) from the server it is connected to (the attacker's terminal). PLAIN AND SIMPLE.

To make a long argument short, it is acceptable to call a binary a "server", but not totally CORRECT.

GoodByeGoodGuys - June 24, 2015, 4:56 pm

(Jun 24, 2015 04:05 PM)DJPunisher Wrote: [\[CITE\]](#) Stop arguing, there's some sort of confusion here that needs to be solved...

Believe it or not, the infected client is literally a "server" because it serves data to the attacker, just as a server would do to a client requesting something out of it. In a reverse connection scenario, both (the client and the attacker) are both "servers", but mainly the "attacker", which is the one that actually HANDLES incoming connections and SHARES resources with clients. The client itself answers to calls (commands) from the server it is connected to (the attacker's terminal). PLAIN AND SIMPLE.

To make a long argument short, it is acceptable to call a binary a "server", but not totally CORRECT.

Sure go ahead tell everyone to stop arguing then put your point across and finish it with "Plain and simple" as if everyone knows this.

You can call it whatever you want but when Armada, KFC try to show you something give you information that indeed is correct and you all jump in here trying to disprove it because someone

many years ago made a mistake in there thought process and you try to shit on them for correcting what was drilled into your minds.

Look at it like this

In this case the server is LuminosityLink hooked up via No-IP

The client is a home connection.

Server <----- Client

In this scenario Google is Google and You is your internet connection

Google <----- You

As you can see KFC and Armada is wrong because Google is not a server Google is a client and everyone who proved Armada and KFC is wrong are gods of HF and deserve gold statues built of them.

Now I have solved this can you all stop shitting on people for disproving something that was mistaken years ago and was never corrected?

EDIT:For all you retards out there I was being sarcastic KFC and Armada are right and you all need to listen because you are all wrong.

QU?CKSILVER - June 24, 2015, 5:04 pm

(Jun 24, 2015 04:56 PM)Wako Wrote: [CITE](#) Sure go ahead tell everyone to stop arguing then put your point across and finish it with "Plain and simple" as if everyone knows this.

EDIT:For all you retards out there I was being sarcastic KFC and Armada are right and you all need to listen because you are all wrong.

What are you NOT understanding here?

The fact that people call a binary a server is not questionable, It's because the roles are FUCKING REVERSED. You'd better think of it like this:

In a RAT connection, who is the one that asks for information? The attacker and who is the one that returns with the information? The infected client.

See how the roles are interchanged now? The client literally becomes a server and the actual server becomes a "client".

In a typical client/server connection, who is the one supposed to serve the data? The server. And who is the one supposed to gather the information? The client.

Now you can sit and think about it before proving anyone wrong.

In conclusion, the roles in a reversed connection are fucking reversed but yet it is STILL a typical client and server communication. No more arguments.

KFC Watermelon - June 24, 2015, 5:06 pm

This thread has turned out for the worst. To be completely honest, I really do not care. Call it a client, call it a server. Whatever floats your boat.

I see both points of the perspective clearly. Please do not involve me in this.

Vuln - June 25, 2015, 4:54 am

This discussion comes up every now and then. Consistency is key, let's leave it at that.

GoodByeGoodGuys - *June 25, 2015, 5:10 am*

I'm done with this. I'm out.

MaxX0r - *June 25, 2015, 1:15 pm*

I'm using this for [my RAT](#) on github. Some people were confused... thanks for this thread! :)