

Forum:[Hack Forums](#)

Thread: [Curious about rat packet encrypt and non-encrypt](#)

cristlol - December 1, 2017, 10:59 am

Any expert please explain why should rats encrypt packets when it makes the data bigger

If not encrypt packets will it make rat faster? ?

Armada - December 1, 2017, 10:27 pm

(Dec 1, 2017 11:59 AM)cristlol Wrote: [\[CITE\]](#) Any expert please explain why should rats encrypt packets when it makes the data bigger

If not encrypt packets will it make rat faster? ?

So the data can not be read?

Why encrypt ANYTHING unless you want it kept private?

cristlol - December 2, 2017, 1:07 am

(Dec 1, 2017 11:27 PM)Armada Wrote: [\[CITE\]](#) So the data can not be read?

Why encrypt ANYTHING unless you want it kept private?

Oh, Encrypt for avoiding antiviruses it is?

Thanks

QU?CKSILVER - December 2, 2017, 9:42 am

Data encryption can also fool firewalls into thinking it's not botnet related traffic. If a Firewall can't inspect those packets due to data encryption, it can either decide to let such connection NOT to be established or simply let it talk to server. Firewalls usually block botnet connections by inspecting and learning from the methods they use to communicate (handshake process, negotiation, TCP window size, specific characteristics of data packets, etc...)

Yes, this can also help bypass antiviruses with built-in firewall solutions. Same concept explained above.

It's a pain in the ass for a firewall to make conclusions with encrypted traffic because it can either think you're trying to use a VPN tunnel to bypass it, or simply browsing SSL enabled sites, connecting to server that requires end to end encryption, etc... tl;dr The data needs to be deeply analyzed to decide whether to consider it suspicious or to simply allow it.

Armada - December 2, 2017, 10:17 am

(Dec 2, 2017 10:42 AM)QU?CKSILVER Wrote: [\[CITE\]](#) Data encryption can also fool firewalls into thinking it's not botnet related traffic. If a Firewall can't inspect those packets due to data encryption, it can either decide to let such connection NOT to be established or simply let it talk to server. Firewalls usually block botnet connections by inspecting and learning from the methods they use to communicate (handshake process, negotiation, TCP window size, specific characteristics of data packets, etc...)

Yes, this can also help bypass antiviruses with built-in firewall solutions. Same concept explained

above.

It's a pain in the ass for a firewall to make conclusions with encrypted traffic because it can either think you're trying to use a VPN tunnel to bypass it, or simply browsing SSL enabled sites, connecting to server that requires end to end encryption, etc... tl;dr The data needs to be deeply analyzed to decide whether to consider it suspicious or to simply allow it.

..... ?

Or you know to stop Packet interception and MITM attacks.
Has absolutely nothing to do with firewalls and anti viruses. lol

Packet encryption is pretty much to ensure only the designated target gets the information and is only readable by the intended host. Firewalls, Antiviruses? Nope.

Read up on [IPSec](#)

Quote:Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection.

cristolol - December 2, 2017, 1:19 pm

(Dec 2, 2017 11:17 AM)Armada Wrote: [\[CITE\]](#) ?

Or you know to stop Packet interception and MITM attacks.
Has absolutely nothing to do with firewalls and anti viruses. lol

Packet encryption is pretty much to ensure only the designated target gets the information and is only readable by the intended host. Firewalls, Antiviruses? Nope.

Read up on [IPSec](#)

Oh, now I get the point of encrypting packets.

Thanks

Armada - December 2, 2017, 1:31 pm

(Dec 2, 2017 02:19 PM)cristolol Wrote: [\[CITE\]](#) Oh, now I get the point of encrypting packets.

Thanks

Also, just to be clear, encryption of packets, does not increase the size of the packet, it just makes more of them.

When a packet is encrypted, if you refer to the diagram in the wiki article, you will see the packets are "Padded" at the start and end of each, thus reducing the size of the data in the packet, because the padding takes up bytes in the packet size, so the system breaks the data down in to more packets, instead of larger packet sizes.

IPSec is much more complicated than what I have explained here, but it should give a good general idea of how and why packet encryption is utilized.

QU?CKSILVER - December 3, 2017, 3:37 pm

(Dec 2, 2017 11:17 AM)Armada Wrote: [\[CITE\]](#) ?

Or you know to stop Packet interception and MITM attacks.
Has absolutely nothing to do with firewalls and anti viruses. lol

Packet encryption is pretty much to ensure only the designated target gets the information and is only readable by the intended host. Firewalls, Antiviruses? Nope.

Read up on [IPSec](#)

Well, I know what the whole purpose of data encryption is. Plus, I never said data encryption was directly related to antiviruses and firewalls. I wanted to say that packet encryption can help bypass firewalls and antiviruses and I have seen this myself being effective against hardware level firewalls such as Sonicwall and Fortinet and antivirus software such as Norton Security.

I mean, you know most physical firewalls have an intrusion prevention system/stateful packet inspection system that will basically inspect anything going in and outside the network to decide whether to allow certain things or not. They have a big ass database of signatures from popular C&Cs, VPN tunnels, and many applications that it is capable of blocking, right? Well, if the firewall learned about network behavior of a certain application because of its' traffic, if you manage to manipulate the way THAT application communicates by modifying packet data, or using different encryption methods you can possibly evade it.

BrBi - December 3, 2017, 3:44 pm

(Dec 3, 2017 04:37 PM)QU?CKSILVER Wrote: [\[CITE\]](#) Well, I know what the whole purpose of data encryption is. Plus, I never said data encryption was directly related to antiviruses and firewalls. I wanted to say that packet encryption can help bypass firewalls and antiviruses and I have seen this myself being effective against hardware level firewalls such as Sonicwall and Fortinet and antivirus software such as Norton Security.

I mean, you know most physical firewalls have an intrusion prevention system/stateful packet inspection system that will basically inspect anything going in and outside the network to decide whether to allow certain things or not. They have a big ass database of signatures from popular C&Cs, VPN tunnels, and many applications that it is capable of blocking, right? Well, if the firewall learned about network behavior of a certain application because of its' traffic, if you manage to manipulate the way THAT application communicates by modifying packet data, or using different encryption methods you can possibly evade it.

exactly if they have packets strings/signature in their database the encryption is a good way to bypass them

Armada - December 3, 2017, 4:50 pm

(Dec 3, 2017 04:37 PM)QU?CKSILVER Wrote: [\[CITE\]](#) I never said data encryption was directly related to antiviruses and firewalls.

(Dec 2, 2017 10:42 AM)QU?CKSILVER Wrote: [\[CITE\]](#) Data encryption can also fool firewalls into thinking it's not botnet related traffic. If a Firewall can't inspect those packets due to data encryption, it can either decide to let such connection NOT to be established or simply let it talk to server. Firewalls usually block botnet connections by inspecting and learning from the methods they use to communicate (handshake process, negotiation, TCP window size, specific characteristics of data packets, etc...)

Yes, this can also help bypass antiviruses with built-in firewall solutions. Same concept explained above.

It's a pain in the ass for a firewall to make conclusions with encrypted traffic because it can either think you're trying to use a VPN tunnel to bypass it, or simply browsing SSL enabled sites, connecting to server that requires end to end encryption, etc... tl;dr The data needs to be deeply analyzed to decide whether to consider it suspicious or to simply allow it.

Anti viruses run off of Definitions and Heuristic Analysis.
Firewalls run off of RULE SETS.

MASSIVE Difference dude.....

FURTHER!

Neither have anything to do with Packet Encryption!. Holy shit I am actually getting worked up over how stupid this conversation is.

QU?CKSILVER - December 3, 2017, 5:10 pm

Lmao, Armada quit playing dumb please. I can't believe you want to argue with me, not gonna happen.

Armada - December 3, 2017, 5:12 pm

(Dec 3, 2017 06:10 PM)QU?CKSILVER Wrote: [\[CITE\]](#) Lmao, Armada quit playing dumb please. I can't believe you want to argue with me, not gonna happen.

There is no argument, you are flat out wrong.

Otherwise simply prove me wrong. ?

Post the technicals proving otherwise, I have already posted the core of ALL of it.

QU?CKSILVER - December 3, 2017, 5:39 pm

(Dec 3, 2017 06:12 PM)Armada Wrote: [\[CITE\]](#) There is no argument, you are flat out wrong.

Otherwise simply prove me wrong. ?

Post the technicals proving otherwise, I have already posted the core of ALL of it.

I ain't talking nonsense here, NOR am I going to waste my time posting shit I know you're not even going to bother to read. This is what it looks like when somebody wants to be right all the time.

It looks like you've got yourself some homework.

Research about antiviruses with firewall solutions and how do they detect suspicious outgoing traffic.

Research about how firewalls learn about new network threats and what the whole SPI feature does.

Research about how packet manipulation and/or data encryption can help BYPASS hardware firewalls/software level firewalls.

Research about what application signature databases are and how firewalls take advantage of these.

I mean, why would I even bother to prove my point, if you will always have a fucking comeback and just make this discussion endless? Nah, bro like I said, not going to happen. Maybe just show somebody with expertise in this field what I just posted and maybe you will understand. I think you didn't read my very first post right, you rushed it, hence the fact you're saying I'm wrong. SMFH.

Armada - December 3, 2017, 5:44 pm

(Dec 3, 2017 06:39 PM)QU?CKSILVER Wrote: [\[CITE\]](#) I ain't talking nonsense here, NOR am I going to waste my time posting shit I know you're not even going to bother to read. This is what it looks like when somebody wants to be right all the time.

It looks like you've got yourself some homework.

Research about antiviruses with firewall solutions and how do they detect suspicious outgoing traffic.

Research about how firewalls learn about new network threats and what the whole SPI feature does.

Research about how packet manipulation and/or data encryption can help BYPASS hardware firewalls/software level firewalls.

Research about what application signature databases are and how firewalls take advantage of these.

I mean, why would I even bother to prove my point, if you will always have a fucking comeback and just make this discussion endless? Nah, bro like I said, not going to happen. Maybe just show somebody with expertise in this field what I just posted and maybe you will understand. I think you didn't read my very first post right, you rushed it, hence the fact you're saying I'm wrong. SMFH.

I do not see any technical's here, I see a bunch of more gibberish from someone who can not admit they do not know what in the flying fuck they are talking about.

Just admit it bro, I know WTF I am talking about and your spewing BS out yo mouth, your lips are fucking turning brown.

QU?CKSILVER - December 3, 2017, 5:47 pm

(Dec 3, 2017 06:44 PM)Armada Wrote: [\[CITE\]](#) I do not see any technical's here, I see a bunch of more gibberish from someone who can not admit they do not know what in the flying fuck they are talking about.

Just admit it bro, I know WTF I am talking about and your spewing BS out yo mouth, your lips are fucking turning brown.? Go elsewhere, really. Disrespectful crackhead.

Armada - December 3, 2017, 5:52 pm

(Dec 3, 2017 06:47 PM)QU?CKSILVER Wrote: [\[CITE\]](#) ? Go elsewhere, really. Disrespectful crackhead.

Says the dude who thinks Packet encryption has anything to do with firewalls and AV;s despite being provided a wiki article explaining the EXACT CONCEPT.

You just wasted 30 seconds of my life which I will never get back, fuck you I am putting you on my ignore list now. Fucking retard, learn networking and then maybe you can email me or something asking to be unblocked. Maybe by then you will understand networking well enough to do so. ?

QU?CKSILVER - December 3, 2017, 6:00 pm

(Dec 3, 2017 06:52 PM)Armada Wrote: [\[CITE\]](#) Says the dude who thinks Packet encryption has anything to do with firewalls and AV;s despite being provided a wiki article explaining the EXACT CONCEPT.

You just wasted 30 seconds of my life which I will never get back, fuck you I am putting you on my ignore list now. Fucking retard, learn networking and then maybe you can email me or something asking to be unblocked. Maybe by then you will understand networking well enough. If you think I am a time waster, why do you still bother to reply? Fuck logic.

I am done with you, don't forget your homework.

Armada - December 3, 2017, 6:27 pm

(Dec 3, 2017 07:00 PM)QU?CKSILVER Wrote: [\[CITE\]](#) If you think I am a time waster, why do you still bother to reply? Fuck logic.

I am done with you, don't forget your homework.

I assign my own homework at this point, Son.

I am well over 15 years out of the educational system, and in the working force already, so while you worry about what Mrs CrabApple or whoever your rotten crotched teachers your dealing with, I again repeat, thats a YOU problem.

BunnyBot - July 28, 2018, 5:15 am

I think this is to make sure that in no way can the data be decrypted and transmitted and to bypass antiviruses with built-in firewall solutions. Firewalls usually block botnet connections.

int - July 28, 2018, 6:31 am

(Dec 3, 2017 07:27 PM)Armada Wrote: [\[CITE\]](#) I assign my own homework at this point, Son.

I am well over 15 years out of the educational system, and in the working force already, so while you worry about what Mrs CrabApple or whoever your rotten crotched teachers your dealing with, I again repeat, thats a YOU problem.

Who are we going to trust, a homeless hacker or another member on hf trying to help?

Stop being a fucking retard, he was trying to help and you keep trying to flex, which you can't do when you are literally homeless

PlugWalkJoe - July 28, 2018, 6:35 am

(Dec 3, 2017 07:27 PM)Armada Wrote: [\[CITE\]](#) I assign my own homework at this point, Son.

I am well over 15 years out of the educational system, and in the working force already, so while you worry about what Mrs CrabApple or whoever your rotten crotched teachers your dealing with, I again repeat, thats a YOU problem.

None of you are wrong, you both agree on one point, 'Encrypting the packet so only the destination provided can actually read it'.

On the packet layer, firewalls do actually analyse packets. For example UTM devices with built in firewalls have been analyzing packets since 2008 (to my knowledge).

https://en.wikipedia.org/wiki/Deep_packet_inspection, a more specific article would be

https://en.wikipedia.org/wiki/Stateful_firewall. I'm disappointed in both of you. Mostly in Armada's ignorance.