

Forum: [Hack Forums](#)

Thread: [\[Uregnt\] Encrypt communication between server and client {msfvenom}?](#)

IrisOP - October 26, 2020, 7:01 am

I am controlling an android phone with msfvenom payload.apk. But the data transfer is not encrypted. I mean if I setup a different computer with linux and msfvenom in the same network, I can control the android phone. Is there any way to end-to-end encrypt all server-client communications? I need to make sure no one else can control the device and I'm not talking about only LAN connections, I am mainly focused on WAN connection.

EDIT;

I'm not willing to trust third parties on this. So, vpn is not the solution.

IrisOP - October 27, 2020, 8:07 pm

I need some information on this. Can someone help me please?

Noodlez_ - October 27, 2020, 10:51 pm

Well it seems like your confused about what a VPN does. It creates that encrypted tunnel between you and the client. Hints the name Virtual Private Network. However if your referencing a VPN as PIA, [censored], ect. You would be correct not to trust your traffic to route through it. However you can set up your own VPN through an open source self hosted server/client such as OpenVPN.

IrisOP - October 28, 2020, 2:17 am

(Oct 27, 2020 10:51 PM)Noodlez_ Wrote: [\[CITE\]](#) Well it seems like your confused about what a VPN does. It creates that encrypted tunnel between you and the client. Hints the name Virtual Private Network. However if your referencing a VPN as PIA, [censored], ect. You would be correct not to trust your traffic to route through it. However you can set up your own VPN through an open source self hosted server/client such as OpenVPN.

Actually I am not. Any VPN setup requires trusting a third party. There is no way for me to setup a VPN on victims' android phone. So, if the payload.apk is not encrypting the traffic before sending it out of the phone, anyone can spy on it until it reaches VPN servers. And no matter if I am using [censored] or my own VPN setup, I will still have to trust the VPS provider. Key note here is It's not about my traffic. It's about victims' traffic.

The traffic needs to be encrypted by payload.apk and decrypted only on my computer.

So far I have found <https://github.com/letsencrypt/letsencrypt>

But I don't know how exactly do I set it up. And I don't even know if this will work in my case or not.