

Forum:[Hack Forums](#)

Thread: [\[Preview\] Minecraft 1.7.9 - Man In The Middle Attack](#)

DragonHunter - February 8, 2014, 12:15 pm

Hey folks whats up,

As you might know or not from time to time I'm now looking at how good network security is being done

And for right now it's not looking so good ?

Well so I was thinking... I play minecraft... why not have a bit of fun in there and see what's up?
I never knew minecraft had their connection encrypted which was fun to know it was

So I went ahead and did a few days of research and having fun with different servers and surprisingly I noticed a few things

At the very end when I had everything decrypted I was at the point of the login HOORAY... or not... apparently minecraft was hashing their ServerId+AES+Public RSA Key...

So yeah... there was where the fun ended for me ?

What I was able todo:

Change the AES and RSA Key to anything I wanted it to be

Dumping the login information

Dumping the AES/RSA (Modulus + Exponent)

Getting the server protocol version (game version)

Getting the IP Address / Port of where minecraft wants to connect to

Spoofing RSA-1024bit and Spoofing AES-128bit

Re-building the packets

Verifying if spoofs were successfull

Decrypting and processing the data/packets

Cloning myself into a different server (look at image below)

Decrypt and Encrypt again

The connection is encrypted with AES 128bit and RSA 1024bit

I'm having the AES-128bit stealthy spoofed but that did not fix my problem for the RSA-1024bit which I really needed for gathering everything else

I had to spoof the RSA-1024bit otherwise I wouldn't get the AES-128bit key

So in short I'm currently stuck at a small problem... getting a bypass for the RSA-1024bit spoof

If I'm able to get the private key of the public key only thing I would be able to get ingame

Cloning a server example

The MITM and Game which shows "Not authenticated with Minecraft.net"

Minecraft server in Offline-Mode

Modifying encrypted data is possible ?

Only in Offline-Mode I would be able to be being ingame, Hopefully I will fix the Hash issue soon for the login ?
Enjoy ?

LethalNET - February 8, 2014, 12:22 pm

Vouch for DH, He is a HQ & Legit programmer.
Good luck with this project mate looks pretty neat :)

SIM-1456245 - February 8, 2014, 12:26 pm

Dude that is some deep haxor shit man. You are really ep1c ub3r l33t pr0 with this. Amazing. I was looking in this kind of things, but from the other side, making a safe connection, not hacking it.

DragonHunter - February 8, 2014, 1:06 pm

(Feb 8, 2014 01:26 PM)Electroalek Wrote: [\[CITE\]](#) Dude that is some deep haxor shit man. You are really ep1c ub3r l33t pr0 with this. Amazing. I was looking in this kind of things, but from the other side, making a safe connection, not hacking it.Thanks :)

You can look into my other project if you feel like you want to look at some security stuff
<https://hackforums.net/showthread.php?tid=4004452>

SIM-1456245 - February 8, 2014, 1:30 pm

(Feb 8, 2014 02:06 PM)DragonHunter Wrote: [\[CITE\]](#) Thanks :)

You can look into my other project if you feel like you want to look at some security stuff
<https://hackforums.net/showthread.php?tid=4004452>

Cool, but I haven't really followed that one, and that thread is 2.0 of some project, I indeed have seen that thread, but I quickly understood that it is an update of another thread.

Temploit - February 8, 2014, 1:49 pm

To sum it up, this is just fucking amazing ._ . Astonishing job as always!

NETExplorer - February 8, 2014, 2:28 pm

(Feb 8, 2014 01:22 PM)LethalNET Wrote: [\[CITE\]](#) Vouch for DH, He is a HQ & Legit programmer.
Good luck with this project mate looks pretty neat :)
How can you vouch on this thread?

????

Bonfire - February 8, 2014, 5:36 pm

I've seen your other works and they never seem to disappoint. Although I barely understand whats going on here, very nice job man!

0xBB - February 8, 2014, 7:07 pm

So that's what you were doin on twitch filthy hax0r. Good job as always Dergun. ?

DragonHunter - February 9, 2014, 1:52 am

Right now I'm streaming what I can do with this pretty much :P

iVision - February 9, 2014, 2:08 am

Are you using hooks or use your SOCKS5 local proxy attack thingy you showed a while ago? Looks good;)

MaxX0r - February 9, 2014, 5:33 am

Nice one dragon, as always. ;) good job

FacetheBass - February 9, 2014, 6:29 am

This is brilliant. I wish I had the drive to learn something like this. Excellent job man.

LethalNET - February 9, 2014, 6:57 am

(Feb 8, 2014 03:28 PM) PatPositron Wrote: [\[CITE\]](#) How can you vouch on this thread?

????

Well simply because.... I can ?

Justice. - February 9, 2014, 8:59 am

Wow, fucking amazing, astonishing work, wtf. :D

DragonHunter - February 9, 2014, 11:35 am

Streaming right now again, come take a look to see some stuff ;)

<http://www.twitch.tv/anguiscapt0r>

DragonHunter - March 6, 2014, 10:28 am

I Sended a e-mail to the MineCraft team at tuesday about those MITM Attacks, waiting for their response now ;)

DragonHunter - June 22, 2014, 10:40 am

Ok so they responded some time back and they wanted to see the source code... ok... lol.. not gonna happen

So I updated it now to 1.7.9

If anyone wants to kick in and play here, xxx.xxx.xxx.xxx [Offline]

I'm also streaming currently at, <http://www.twitch.tv/AnguisCapt0r>