

Forum:[Hack Forums](#)

Thread: [\[Preview\] Lineage2 Man-In-The-Middle \[Spoofing RSA-1024, Blowfish and more\]](#)

DragonHunter - January 10, 2013, 3:59 pm

just a beta preview of my new program L2MITM
Lineage2 - Man In The Middle

This program is able to dump the username and password of the person who is going to login
The program decrypts the RSA-1024bit, Blowfish, Xor encryption of the game

Just a early stage of the project,
It's also having a simple plugin system so you're able to do a lot and have fun with scripting different stuff
For now I made a plugin that will dump the username and password to a file
And a other plugin that would attack the next monster when you killed it (bot)

You could make a lot outta this :)

Haven't been doing some gamehacks for such time so why not
I thought I'd be also funny to break to spoof the RSA Key so I was able to decrypt the username and password hehe ^_^
Haven't seen anyone so far breaking the RSA for this game so maybe I'm the first 1 ?
Breaking the RSA 1024bit costed me 2 full days messing around with spoofing it and setting all the offsets correct etc
Note: No game hooks are being used, the program is written 100% in C#

[Video: <http://www.youtube.com/watch?v=ezW41ADAZVI&feature=youtu.be>]

tweety - January 10, 2013, 4:07 pm

Seen some of this stop. This newb know's what his doing. Did you manage to write the bot to auto target people yet?

DragonHunter - January 10, 2013, 4:14 pm

(Jan 10, 2013 05:07 PM)Tweety. Wrote: [\[CITE\]](#) Seen some of this stop. This newb know's what his doing. Did you manage to write the bot to auto target people yet?Ye could do that ye but it's just a very basic bot plugin more like a POC ?

xSilent - January 10, 2013, 7:53 pm

Well, this proves even if you use encryption; Nothing is secure.

Nice job, Dragon. ?

marvinn - January 11, 2013, 5:04 am

Nice one, were you thinking about an opensource framework for capturing the packets so people can customize it to an other game?

tweety - January 11, 2013, 5:13 am

(Jan 11, 2013 06:04 AM)marvinn Wrote: [\[CITE\]](#) Nice one, were you thinking about an opensource

framework for capturing the packets so people can customize it to an other game?
I believe that's what the plugin system is made for.

Meerkat.? - January 11, 2013, 9:04 am

Holy shit Anguis, you're the fucking boss.

CyNecx - January 11, 2013, 3:04 pm

Hey Dragon !

Could you please tell us whats new in your cool new ssp 2 proto ?

Anyways this looks very nice !

facebookdoom - January 11, 2013, 3:39 pm

Excellent work! I myself have written packet bots years ago for the MMORPG "Silkroad Online". You can bank hard if you come up with the first bot for a up-coming MMORPG.

pr3fix - January 11, 2013, 5:33 pm

Pretty cool and unique project.

Always interesting stuff from you Dragon :D

The-One - January 12, 2013, 2:53 am

I keep wondering how you are everytime able to amaze me... :)

Callum. - January 12, 2013, 4:03 am

Can you explain exactly what you're doing?

I'm quite confused, are you logging everyone who joins the servers, password?

Can you give an explanation to someone who hasnt played the game and doesnt understand what you did(minus the auto attack bot)

Coiner - January 12, 2013, 5:00 am

(Jan 12, 2013 05:03 AM)Callum. Wrote: [\[CITE\]](#) Can you explain exactly what you're doing?

I'm quite confused, are you logging everyone who joins the servers, password?

Can you give an explanation to someone who hasnt played the game and doesnt understand what you did(minus the auto attack bot)

He setted up in other words a proxy. Normal way of packets transfer: Client -> Server; Server -> Client. With his app: Client -> App -> Server; Server -> App -> Client. Thus he can control the packets, sniff the packets and so on. This has been already done in Mu-Online for ages, but first time seeing this for L2. Good job DragonHunter.

iVision - January 12, 2013, 5:07 am

Cool Dragon, will you ever release something that doesn't amaze us all?

Goodjob DragonHunter.

ps: tbh I like DragonHunter more then your new name.

DragonHunter - January 12, 2013, 9:53 am

Thanks for the nice comments guys ^_^

Just wanted to post this also because I think it's funny

CockWave challenged me to do this also for world of warcraft but appearently... 1 picture sais a thousand wurd

U notice anything ? no encryption... lol so boring doing wow ____.

xSilent - January 12, 2013, 12:28 pm

(Jan 12, 2013 10:53 AM)AnguisCaptor Wrote: [\[CITE\]](#) Thanks for the nice comments guys ^_^
Just wanted to post this also because I think it's funny
CockWave challenged me to do this also for world of warcraft but appearently... 1 picture sais a thousand wurds

U notice anything ? no encryption... lol so boring doing wow ____.
Spoiler [\(Click to View\)](#)

No encryption? I thought that game sucked. ?

phinal - January 12, 2013, 3:47 pm

(Jan 12, 2013 10:53 AM)AnguisCaptor Wrote: [\[CITE\]](#) Thanks for the nice comments guys ^_^
Just wanted to post this also because I think it's funny
CockWave challenged me to do this also for world of warcraft but appearently... 1 picture sais a thousand wurds

U notice anything ? no encryption... lol so boring doing wow ____.

I'm curious as to what theme you're using, looks nice.

Good work by the way, never seen this done before...

facebookdoom - January 12, 2013, 5:16 pm

(Jan 12, 2013 10:53 AM)AnguisCaptor Wrote: [\[CITE\]](#) Thanks for the nice comments guys ^_^
Just wanted to post this also because I think it's funny
CockWave challenged me to do this also for world of warcraft but appearently... 1 picture sais a thousand wurds

U notice anything ? no encryption... lol so boring doing wow ____.

WoW has a super awesome anti cheat system which is called Warden.

TrackPro+ - January 12, 2013, 5:41 pm

Wow, awesome man. Shows mostly every move LOL

Exit - January 14, 2013, 5:15 am

Old pop's high on codes.

;]

- kris.

DragonHunter - January 14, 2013, 5:57 am

(Jan 14, 2013 06:15 AM)Exit Wrote: [\[CITE\]](#) Old pop's high on codes.

;]

- kris.Yo daughter. Daddy is not hacking ?

Go back do your backtrack homework, I wanna hear something about that nice java zeroday ?

mastermarre - January 16, 2013, 10:24 pm

Wow, this is an amazing application.

Just one question:

What technique do you use to route the packets through your local proxy if you do not hook anything?

DragonHunter - January 17, 2013, 4:36 am

(Jan 16, 2013 11:24 PM)mastermarre Wrote: [\[CITE\]](#) Wow, this is an amazing application.

Just one question:

What technique do you use to route the packets through your local proxy if you do not hook anything? People need to go to their 'System' folder which is located in the lineage2 folder where u installed it

And then u need to edit the l2.ini which contains the ip/port, u edit it to your MITM server and u can start having fun :)

So ye if you would give the l2.ini to a few guys like hey join my server to play... well they'll connect first to you and then play ?

So the funny thing is that while they're playing u could basically enable a bot and turn their player into a bot and they'll have no idea wtf is happening ?

Superior1 - January 22, 2013, 12:34 pm

Nice theme, did you make it, or find it?