

Forum:[Hack Forums](#)

Thread: [A RAT in a .Jar file](#)

Curiosity2602 - January 15, 2021, 3:11 pm

So, could I send a RAT per minecraft mod since the extension .Jar is? I mean more like, could i put the mod into a folder and let people download it with dropbox? Or do i have to send them the mod as a single download for the RAT to work

Curiosity2602 - January 16, 2021, 5:27 am

(Jan 16, 2021 12:07 AM)Snyke Wrote: [\[CITE\]](#) Dropbox scans and distributes everything.

I wouldnt use that as a direct host, but you can, yes.

Best if you have a Java RAT imo.

Sounds great, thanks!

(Jan 16, 2021 12:07 AM)Snyke Wrote: [\[CITE\]](#) Dropbox scans and distributes everything.

I wouldnt use that as a direct host, but you can, yes.

Best if you have a Java RAT imo.

But one question tho if you dont mind answering. If i am able to send someone an RAT, would it be possible to gain access to the WebCam and login details? Since i know that the person that i am aiming for an laptop uses.

Z4ACK - January 16, 2021, 9:59 am

(Jan 16, 2021 06:27 AM)Curiosity2602 Wrote: [\[CITE\]](#) Sounds great, thanks!

But one question tho if you dont mind answering. If i am able to send someone an RAT, would it be possible to gain access to the WebCam and login details? Since i know that the person that i am aiming for an laptop uses.

I mean it depends. usually RATS have keyloggers which would do that. Id recommend not ratting but just sending a token logger for discord.

Curiosity2602 - January 16, 2021, 3:38 pm

(Jan 16, 2021 12:16 PM)Snyke Wrote: [\[CITE\]](#) Yes.

If you have physical access you could, hypothetically, use a USB spread feature.

I dont have physical access to that laptop sadly.

KingVOID7777 - January 16, 2021, 5:43 pm

(Jan 16, 2021 04:51 PM)Snyke Wrote: [\[CITE\]](#) So, hypothetically, one would need a RAT, good runtime crypter and delivery method. Whether the RAT stub is bound to another, working .exe and social engineered into installing it ("hey, I have this assorted video game cheat." Please be more creative) or bound to an exploit delivery method like a .doc or a .xls file (there are two different types. Macros and Silent. Macros are cheaper, at about \$50-100 for a FUD one which act as a downloader or Silent at about \$900-2000 depending on the CVE, and are often a rip off to the point where I've only found one legitimate seller in the last 3 months).

Objectively, you can find other methods of delivery if you are creative enough.

Edit: if you need to bind it to a .jar file, you would need a Java binder for a Java RAT.

Wait doesn't the creator of Warzone RAT also sell a silent exploit? And what's the difference

between Macro/Silent?

But anyway, back to the .jar RAT:

I've seen this personally before in exploiting communities (Roblox ??) where someone would literally just use a RAT and rename it to (cheat's name.exe) ((Usually Synapse X.exe)

For now you can probably trick the more naive ones into running a .jar that's purely the RAT, otherwise yeah you can bind it with one of the options Snyke said.

Kabir - January 16, 2021, 11:08 pm

(Jan 16, 2021 07:30 PM)Snyke Wrote: [\[CITE\]](#) Macro requires the user to click "Enable Editing", and if the .doc has a zoneidentifier that designates it was downloaded from the internet, it will open the document in protected view which actively warns the user that it may contain a virus if it has an active macro table. Regardless if it does or not.

yes regardless n most of them enables it as you see there are many macro excel / word documents in circulation

assuming 20% executions may be more not bad

Curiosity2602 - January 17, 2021, 3:04 am

(Jan 16, 2021 04:51 PM)Snyke Wrote: [\[CITE\]](#) So, hypothetically, one would need a RAT, good runtime crypter and delivery method. Whether the RAT stub is bound to another, working .exe and social engineered into installing it ("hey, I have this assorted video game cheat." Please be more creative) or bound to an exploit delivery method like a .doc or a .xls file (there are two different types. Macros and Silent. Macros are cheaper, at about \$50-100 for a FUD one which act as a downloader or Silent at about \$900-2000 depending on the CVE, and are often a rip off to the point where I've only found one legitimate seller in the last 3 months).

Objectively, you can find other methods of delivery if you are creative enough.

Edit: if you need to bind it to a .jar file, you would need a Java binder for a Java RAT.

Well, my plan was actually to send the RAT as minecraft mod since all of the mods .Jar are. I have already an good idea on how to trick that person in installing that mod. If DropBox is not going to work, i will tell him that he has to install that 1 other mod aswell that isnt in the modpack yet but on the minecraft server. I have also picked his favourit mod and was planning on sending it to him via discord after crypting that whole thing so that its undetectable.

(Jan 17, 2021 04:04 AM)Curiosity2602 Wrote: [\[CITE\]](#) Well, my plan was actually to send the RAT as minecraft mod since all of the mods .Jar are. I have already an good idea on how to trick that person in installing that mod. If DropBox is not going to work, i will tell him that he has to install that 1 other mod aswell that isnt in the modpack yet but on the minecraft server. I have also picked his favourit mod and was planning on sending it to him via discord after crypting that whole thing so that its undetectable.

And i also know that, that person isnt playing with anyone atm, so the chance is high that he is gonna give it a try. All i want is the Discord account to mess a little around with that person.

ElectroRAT - January 17, 2021, 10:24 am

This RAT is include .jar binder electrorat.com

3xploit - January 17, 2021, 10:49 am

There's one problem if you want to spread it as Minecraft mod: They are not executed normally (i.e. through a double click) but by the mod loader like Forge. However, it's not hard to change the entry point for the jar and make a real backdoored MC mod (also works for plugins btw).

Curiosity2602 - January 17, 2021, 11:05 am

(Jan 17, 2021 11:49 AM)\$moke Wrote: [\[CITE\]](#) There's one problem if you want to spread it as Minecraft mod: They are not executed normally (i.e. through a double click) but by the mod loader like Forge. However, it's not hard to change the entry point for the jar and make a real backdoored MC mod (also works for plugins btw).

What exactly do you mean by that? So it would technically work, since its getting executed by forge or?

3xploit - January 17, 2021, 11:11 am

(Jan 17, 2021 12:05 PM)Curiosity2602 Wrote: [\[CITE\]](#) What exactly do you mean by that? So it would technically work, since its getting executed by forge or?

If it's a normal jar using the main method it's not going to work, forge requires a specific entry point.

Curiosity2602 - January 17, 2021, 11:14 am

(Jan 17, 2021 12:11 PM)\$moke Wrote: [\[CITE\]](#) If it's a normal jar using the main method it's not going to work, forge requires a specific entry point.

Hmm but its not hard to change the entry point like you said am i correct? So it can work if i am right.

Another person told me that if they open the .Jar, it's goint to download the rat from a link.

3xploit - January 17, 2021, 11:22 am

(Jan 17, 2021 12:14 PM)Curiosity2602 Wrote: [\[CITE\]](#) Hmm but its not hard to change the entry point like you said am i correct? So it can work if i am right.

Another person told me that if they open the .Jar, it's goint to download the rat from a link.

Simply look up "how to code minecraft forge mod" to create the mod base and instead of adding the contents of the mod (new blocks idk) you add the backdoor.

It depends on how the jar is openend. As I already said, there's a difference if Forge loads the mod or if someone double clicks the jar.

Curiosity2602 - January 17, 2021, 11:26 am

(Jan 17, 2021 12:22 PM)\$moke Wrote: [\[CITE\]](#) Simply look up "how to code minecraft forge mod" to create the mod base and instead of adding the contents of the mod (new blocks idk) you add the backdoor.

It depends on how the jar is openend. As I already said, there's a difference if Forge loads the mod or if someone double clicks the jar.

Shrug, alright. But do you know if its easier to send a RAT as a minecraft mod, or a keylogger with a texture pack? Or is there another way to get to the discord details somehow perhaps

j0rdan - January 17, 2021, 10:00 pm

Good luck, lol. Love ratting children.

Curiosity2602 - January 18, 2021, 5:13 am

(Jan 17, 2021 12:22 PM)\$moke Wrote: [\[CITE\]](#) Simply look up "how to code minecraft forge mod" to create the mod base and instead of adding the contents of the mod (new blocks idk) you add the backdoor.

It depends on how the jar is openend. As I already said, there's a difference if Forge loads the mod or if someone double clicks the jar.

I noticed that you can open Forge with a double click (to install it into minecraft) and its a .Jar file aswell. That should be easier and should also work instead of using a mod, is that correct? I would put the RAT into Forge then.

(Jan 17, 2021 11:00 PM)j0rdan Wrote: [\[CITE\]](#) Good luck, lol. Love ratting children.

Well, that person that I am aiming for is actually 18, but I have a good plan for it. ?

3xploit - January 18, 2021, 5:24 am

(Jan 17, 2021 12:26 PM)Curiosity2602 Wrote: [\[CITE\]](#) Shrug, alright. But do you know if its easier to send a RAT as a minecraft mod, or a keylogger with a texture pack? Or is there another way to get to the discord details somehow perhaps

I'm not sure if you can run code by loading a texture pack. I recommend using a Discord token logger instead of a normal keylogger as it will be more effective.

...actually I don't recommend anything because you need to remember that such actions are illegal and not worth it if this is some kind of kid stuff.

Curiosity2602 - January 18, 2021, 5:27 am

(Jan 18, 2021 06:24 AM)\$moke Wrote: [\[CITE\]](#) I'm not sure if you can run code by loading a texture pack. I recommend using a Discord token logger instead of a normal keylogger as it will be more effective.

...actually I don't recommend anything because you need to remember that such actions are illegal and not worth it if this is some kind of kid stuff.

Belive me, its not kid stuff. I just want to mess around with that person and i wasnt planning on doing something like that ever again after i am done