

Forum:[Hack Forums](#)

Thread: [Why so few Executable Jar File \(.jar\) Rats?](#)

latencyx - October 26, 2024, 4:46 am

Hello friends,

I recently came across a question, why are there so few RATS with .jar output? The few that exist have very few detections and with a few modifications you can get something close to 0/40 in most virus scanners and easily bypass Windows Defender, do you have any opinions on this?

Delfin - October 26, 2024, 5:08 am

(Oct 26, 2024 04:46 AM)latencyx Wrote: [\[CITE\]](#) Hello friends,

I recently came across a question, why are there so few RATS with .jar output? The few that exist have very few detections and with a few modifications you can get something close to 0/40 in most virus scanners and easily bypass Windows Defender, do you have any opinions on this?

The main reason is the fact that .JAR files won't run on every Windows system. They depend on the JRE, which isn't preinstalled on any Windows version (no version to my knowledge, at least). It's the same reason that people prefer native binaries over .NET - native binaries just provide more compatibility and therefore more opportunities to infect a client. Regarding detections, I'd assume that the only reason .JAR has lower detections is because there's fewer people using it for malware, which means that there's less samples, and therefore less detections and signatures. If JAR malware gained prominence, detections would rise to the level of regular executables relatively quickly.

latencyx - October 26, 2024, 5:19 am

(Oct 26, 2024 05:08 AM)Delfin Wrote: [\[CITE\]](#) The main reason is the fact that .JAR files won't run on every Windows system. They depend on the JRE, which isn't preinstalled on any Windows version (no version to my knowledge, at least). It's the same reason that people prefer native binaries over .NET - native binaries just provide more compatibility and therefore more opportunities to infect a client. Regarding detections, I'd assume that the only reason .JAR has lower detections is because there's fewer people using it for malware, which means that there's less samples, and therefore less detections and signatures. If JAR malware gained prominence, detections would rise to the level of regular executables relatively quickly.

I thought about this dependency factor too, but I believe that a simple dropper can get around this, and because of the low sample size it might be something worth thinking about

Delfin - October 26, 2024, 6:02 am

(Oct 26, 2024 05:19 AM)latencyx Wrote: [\[CITE\]](#) I thought about this dependency factor too, but I believe that a simple dropper can get around this, and because of the low sample size it might be something worth thinking about

A dropper that installs the JRE on the user's PC? Doesn't sound very viable, to me at least. As regarding small sample sizes, you can just directly use languages like C# for small binaries, or stripped C/C++ ones.