

Forum:[Hack Forums](#)

Thread: [How to detect a virus on a jar file \(to see which file it is in\)](#)

lasermat - February 4, 2022, 12:48 pm

Hi (I use Google Translate)

I would like to know how can you find a virus that is hidden in a file .jar because I searched for it but I did not find it can someone help me?

Thanks

GenericSkid - February 4, 2022, 10:51 pm

I'll be blunt, there is no viable automated "virus detection" system for Java applications at the moment. The Minecraft cheating "community" has made a few tool but to be honest they kinda suck, either because they are too specific to Minecraft or are glorified signature scanners. That being said, existing automated virus scanning tools are not designed with Java in mind. The closest thing you will find now are tools that offer signature scans. But even those are problematic. Most anti-malware products are designed to do two things:

Look at the file for known malicious signatures

Evaluate the file at runtime for suspicious behavior

Quote:Signatures?

This is skipping some details, but for the most part signatures are just looking for one or more series of bytes in a file. Lets say a signature looks for the string "malware.com". Any program with literal text containing that will be flagged as malware. However the problem here is obfuscation. If you were to break the text into two parts, "mal" and "ware.com" then the signature does not find what it is looking for. Native windows programs (EXE) have something called a String-Table in their files, which has information that the program needs to run. Stuff like text printed to the console, text shown in buttons and labels, and in our case, text to malicious urls.

Java programs have something extremely similar called a Constant-Pool which contains all the constant/unchanging information that a Java program needs to run. However just like their native counter-parts just simple obfuscation measures will break signatures. So if we have a piece of malware that gets flagged by a anti-malware program with signatures it is very easy to bypass that signature as a malware author/distributor.

Quote:So what can you do if signatures don't work?

You can try evaluating the program!

Running malware is a terrible idea, but that's where Virtual Machines come in. It would be incredibly hard to simulate a program running so instead we can let programs run naturally but keep an eye on them in this contained environment. Consider a EXE file utilizes these windows features,

"SetWindowsHookExA" and "GetWindowTextA". If we saw those two things happening one after another it would be reasonable to assume that this program is a keylogger and grabbing keystrokes and letting us know which application the keys are being put into.

So what about Java? Well, the JVM will eventually have to delegate Java functions to native ones. File IO for instance. So it should be a somewhat reliable practice here.

Quote:Ok so how do I tell if a Java program is a virus?

If you are unable to decompile the program and infer it for yourself, you can do what works in almost every case and drop it in a VM (VirtualBox / VMWare) and see what it does using tools like:
SysInternals suite

Procmon

Process Explorer

AutoRuns

Wireshark

0xC - April 19, 2022, 12:14 pm

If you still need help, send me the file and I can try to reverse it and find the rat.