Beyond good ol' Run key, Part 133

hexacorn.com/blog/2021/03/05/beyond-good-ol-run-key-part-133

March 5, 2021 *in Anti-Forensics, Autostart (Persistence)*

Java programs compiled into executable form using launch4j have a few interesting features that make them a good target for both persistence and LOLBIN-ish activities.

When the executable starts it checks the environment for a presence of Java Runtime Environment (JRE) and while doing so it is checking a number of locations:

- 64-bit search: HKLM\SOFTWARE\JavaSoft\Java Runtime Environment
- 32-bit search: HKLM\SOFTWARE\JavaSoft\Java Runtime Environment
- 64-bit search: HKLM\SOFTWARE\JavaSoft\Java Development Kit
- 32-bit search: HKLM\SOFTWARE\JavaSoft\Java Development Kit
- 64-bit search: HKLM\SOFTWARE\JavaSoft\JRE
- 32-bit search: HKLM\SOFTWARE\JavaSoft\JRE
- 64-bit search: HKLM\SOFTWARE\JavaSoft\JDK
- 32-bit search: HKLM\SOFTWARE\JavaSoft\JDK
- 64-bit search: HKLM\SOFTWARE\IBM\Java Runtime Environment
- 32-bit search: HKLM\SOFTWARE\IBM\Java Runtime Environment
- 64-bit search: HKLM\SOFTWARE\IBM\Java2 Runtime Environment
- 32-bit search: HKLM\SOFTWARE\IBM\Java2 Runtime Environment
- 64-bit search: HKLM\SOFTWARE\IBM\Java Development Kit
- 32-bit search: HKLM\SOFTWARE\IBM\Java Development Kit

The JAVA_HOME environment variable is not being used.

Placing malicious entry under any of these branches e.g.:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\JavaSoft\Java Development Kit\1.8]
"JavaHome"="c:\test"
```

and then dropping malicious *c:\test\jre\bin\javaw.exe* will cause the original program compiled with launch4j 9when launched) to spawn that malicious *javaw.exe*.

And as a little bonus, the stub of launch4j accepts these debug command line arguments (or uses equivalent values of environment variables shown in parenthesis):

- *–l4j-debug* (or *Launch4j=*debug**)
- *–l4j-debug-all* (or *Launch4j=*debug-all**)

When any of these two are present a *launch4j.log* log file will be created with all the information needed for troubleshooting (the second option generating more verbose version of the log file).