Beyond good ol' Run key, Part 112

hexacorn.com/blog/2019/08/16/beyond-good-ol-run-key-part-112

August 16, 2019 *in Autostart (Persistence)*

This is a pretty ancient persistence trick one can use on systems where IBM's Java Control Panel is still present.

On these systems you will find Registry Key:

> HKLM\SOFTWARE\IBM\Java2 Runtime Environment\
> <version>\

and a Value Name underneath called:

> JavaHome = <directory>

By changing this value, one can ensure that next time the Control Panel applet is called, the signed CPL file will launch a *bin\javacpl.exe* program from this path.

In other words, for the example old version 1.6.0 one could change the value name to this:

> HKLM\SOFTWARE\IBM\Java2 Runtime Environment\
> 1.6.0\JavaHome=c:\test

and then drop a malicious *c:\Test\bin\javacpl.exe* file.

I have not tested it, but I am pretty sure that changing the value of that variable will definitely affect the way Java works, so things will be probably broken, unless proper links to files are established for all the content residing in the actual JavaHome directory.

Yes, it's ancient, and probably dead by this time + not worth pursuing, but just documenting… because why not.

Comments are closed.