Export JRAT/Adwind Config with x32dbg

By MlwrDssctng

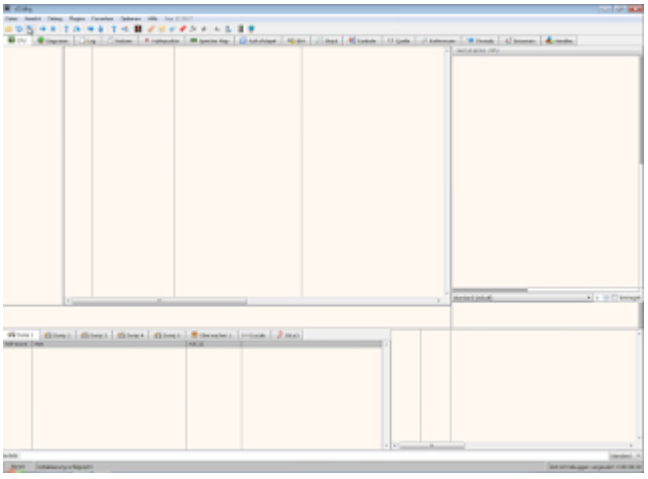
Published: 2018-08-08 · Archived: 2026-04-05 18:09:09 UTC

In this blog post I'll explain how you can export the config of JRAT/Adwind to gather further insight into this kind of malware. The trick is, that you must be aware that JRAT/Adwind creates a fake JAR and config at the beginning to confuse analysts.

Afterwards, the real config and JAR are run.

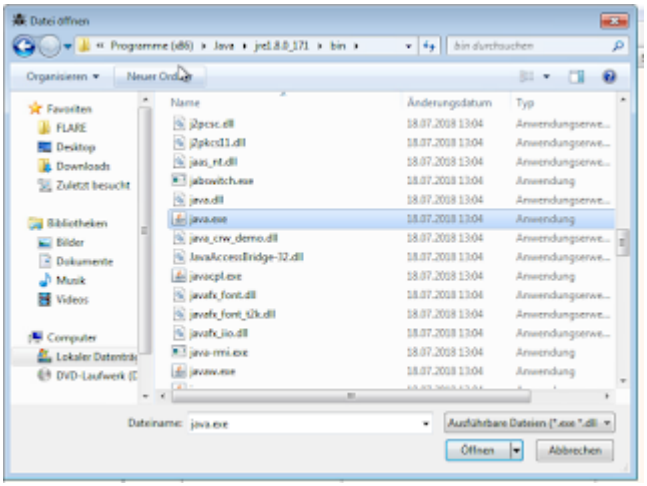
Step 1:

Start x32dbg



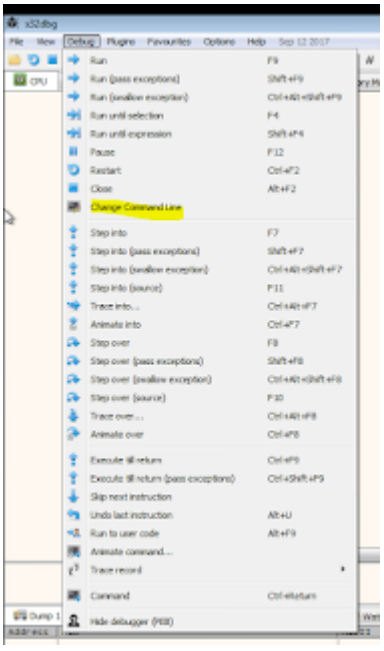
Step 2:

Open java.exe



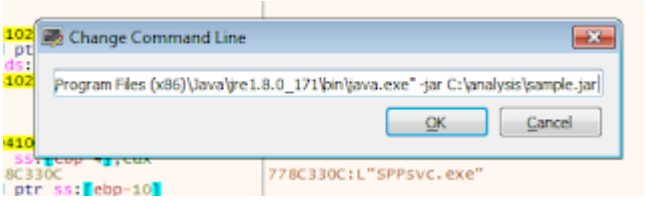
Step 3:

Under Debug, choose "Change Command Line"



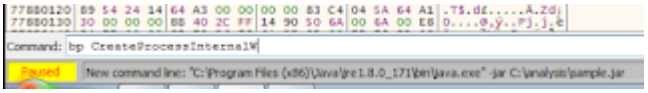
Step 4:

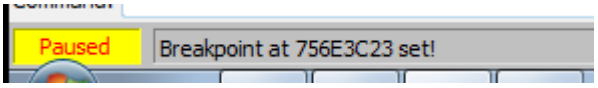
Point it to your suspected JRAT/Adwind JAR file



Step 5:

Create a Breakpoint on "CreateProcessInternalW"

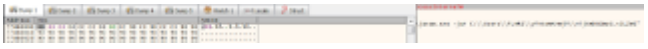




Hint: As mentioned earlier this Breakpoint will be hit multiple times since JRAT starts multiple processes (for example to detect AV solutions with the help of WMI etc.) so you should watch the Stack Windows of x32dbg to find the "real" call.

Step 6:

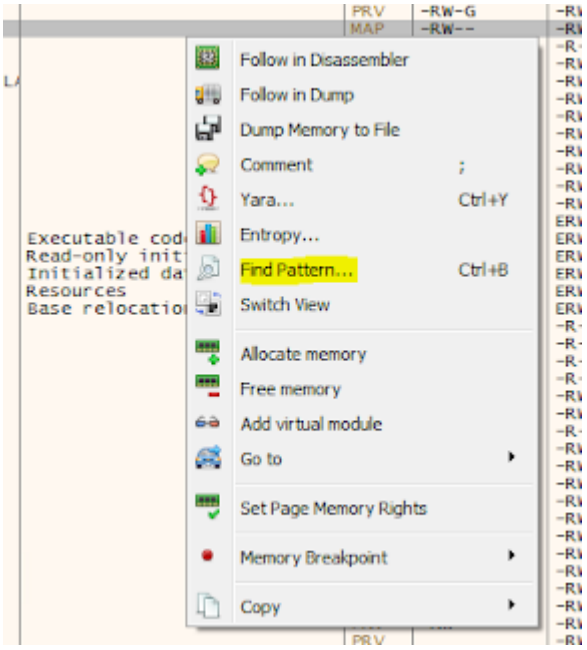
So after hitting the breakpoint multiple times you should see something like this:



Adwind is about to start the real JAR and thus we can be sure that the real config must be somewhere in memory.

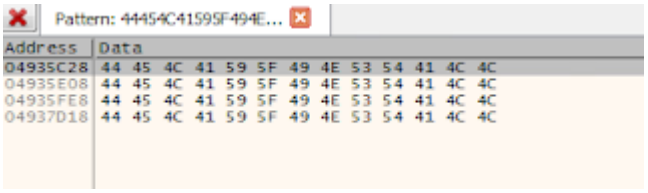
Step 7:

Switch to Memory Map and rightclick and click "Find pattern"



Step 8:

Since I've seen Adwind/JRAT configs multiple times, I know that the word "DELAY_INSTALL" is found somewhere in the config so let's search for this string since it's pretty unique. You will find multiple matches:

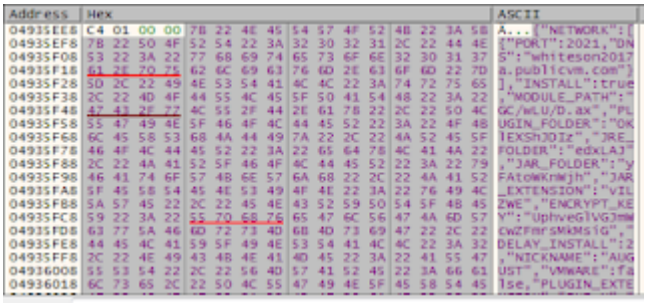


Step 9:

Double click on them to open the CPU View and look if it is the right config. Hint: If the DNS_SERVER in the config is pointing to 127.0.0.1 you are looking at the dummy config which is not what you are looking for so repeat step 8 until you catch the right one.

Step 10:

Once you found the right config mark the text, right click on it, choose "Binary" and "Save to file"



Congratulations! You exported your first Adwind/JRAT config!

Source: https://dissectingmalware.blogspot.com/2018/08/export-jratadwind-config-with-x32dbg.html