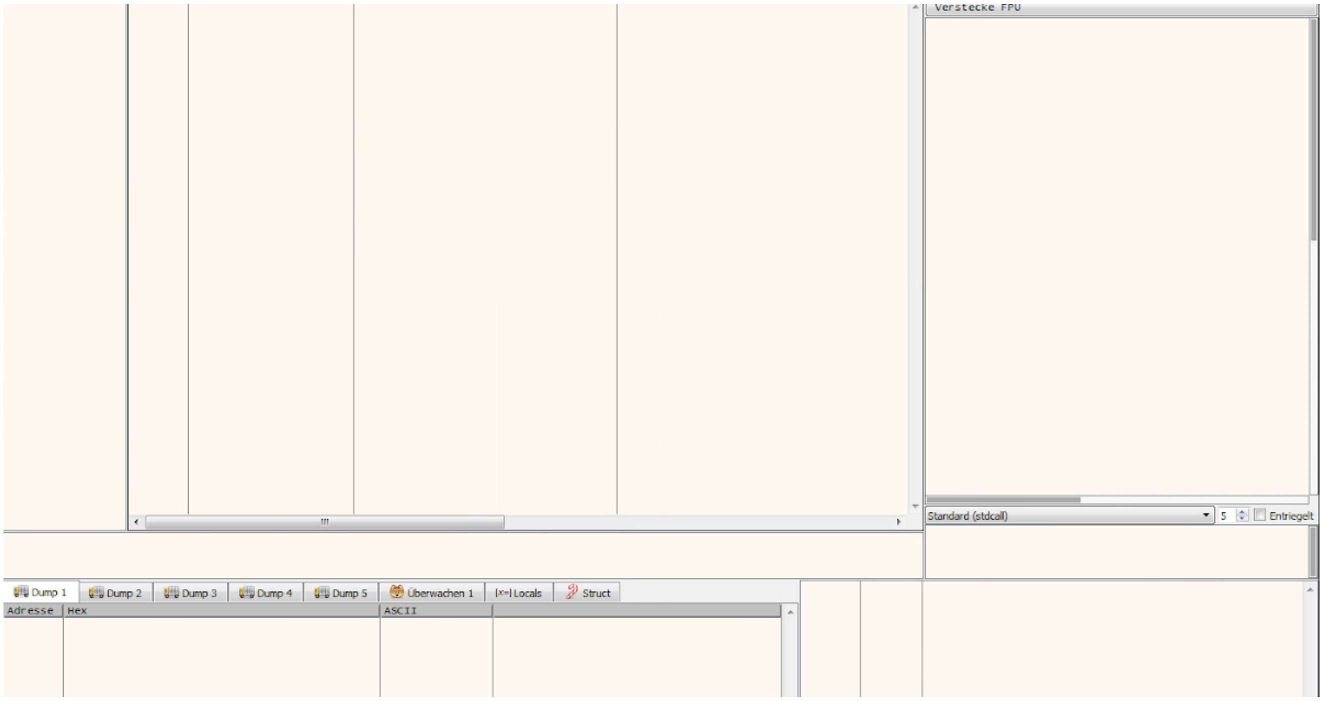
Export JRAT/Adwind Config with x32dbg

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

MlwrDssctng

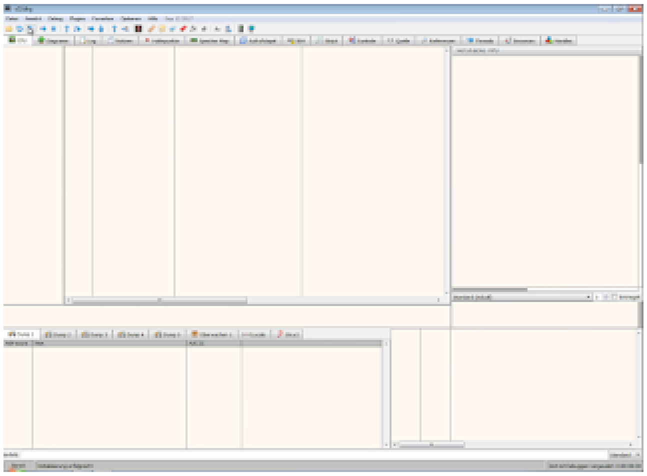


In this blog post I'll explain how you can export the config of JRAT/Adwind to gather further insight into this kind of malware. The trick is, that you must be aware that JRAT/Adwind creates a fake JAR and config at the beginning to confuse analysts.

Afterwards, the real config and JAR are run.

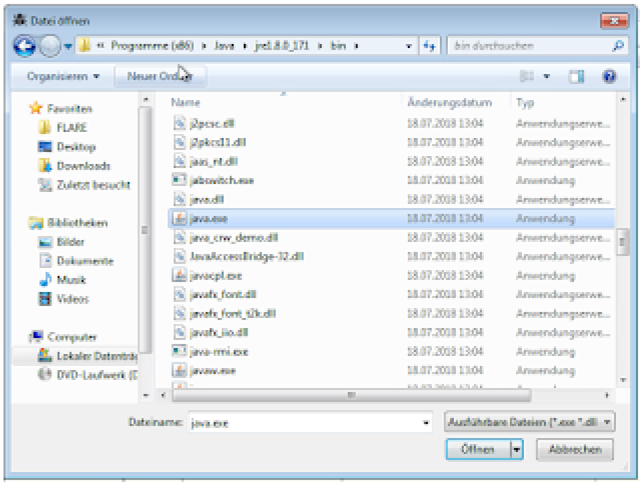
Step 1:

Start x32dbg



Step 2:

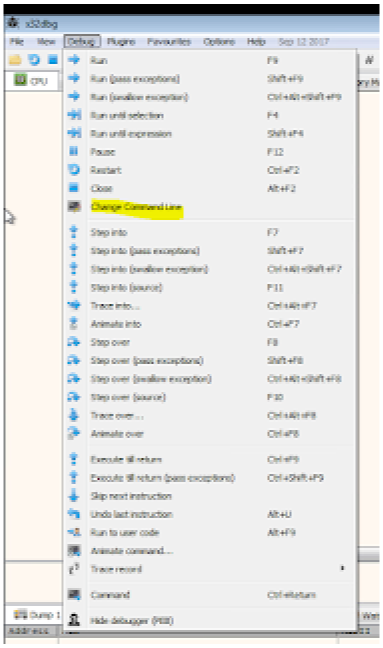
Open java.exe



Dateiname: java.exe

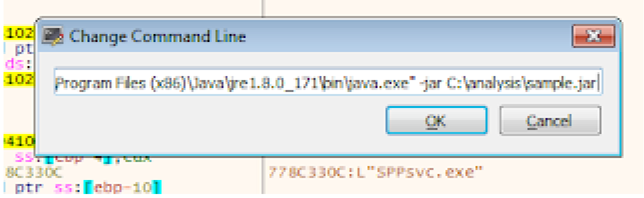
Step 3:

Under Debug, choose "Change Command Line"


x32dbg
File
View
Debug
Plugins
Favourites
Options
Help
Sep 12 2017
CPU
Run F9
Run (pass exceptions) Shift+F9
Run (swallow exception) Ctrl+Alt+Shift+F9
Run until selection F4
Run until expression Shift+F4
Pause F12
Restart Ctrl+F2
Close Alt+F2
Change Command Line
Step into F7
Step into (pass exceptions) Shift+F7
Step into (swallow exception) Ctrl+Alt+Shift+F7
Step into (source) F11
Trace into... Ctrl+Alt+F7
Animate into Ctrl+F7
Step over F8
Step over (pass exceptions) Shift+F8
Step over (swallow exception) Ctrl+Alt+Shift+F8
Step over (source) F10
Trace over... Ctrl+Alt+F8
Animate over Ctrl+F8
Execute till return Ctrl+F9
Execute till return (pass exceptions) Ctrl+Shift+F9
Skip next instruction
Undo last instruction Alt+U
Run to user code Alt+F9
Animate command...
Trace record
Command Ctrl+Return
Hide debugger (PEB)
Dump 1
Address

Step 4:

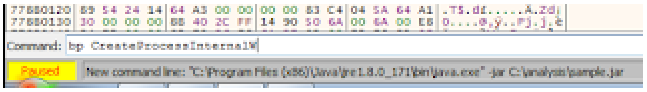
Point it to your suspected JRAT/Adwind JAR file



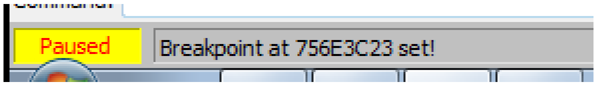
```
Program Files (x86)\Java\jre1.8.0_171\bin\java.exe" -jar C:\analysis\sample.jar
```

Step 5:

Create a Breakpoint on "CreateProcessInternalW"



```
77BB0120  89 54 24 14  64 A3 00 00  00 00 83 C4  04 5A 64 A1  .T$.d£.....Ä.Zd¡
77BB0130  30 00 00 00  8B 40 2C FF  14 90 50 6A  00 6A 00 E8  0....@,ÿ..Pj.j.è
Command: bp CreateProcessInternalW
Paused  New command line: "C:\Program Files (x86)\Java\jre1.8.0_171\bin\java.exe" -jar C:\analysis\sample.jar
```



```
Paused  Breakpoint at 756E3C23 set!
```

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.

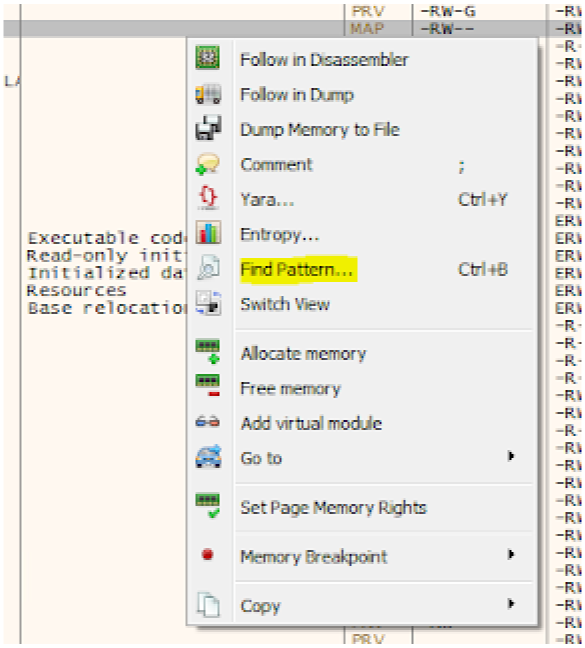
Step 6:

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.

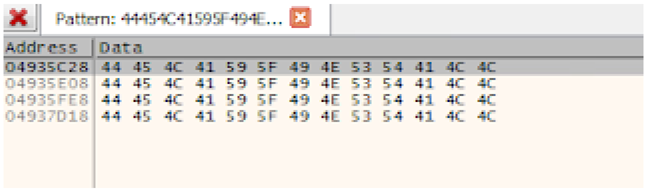
Step 7:

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:



Pattern: 44454C41595F494E...

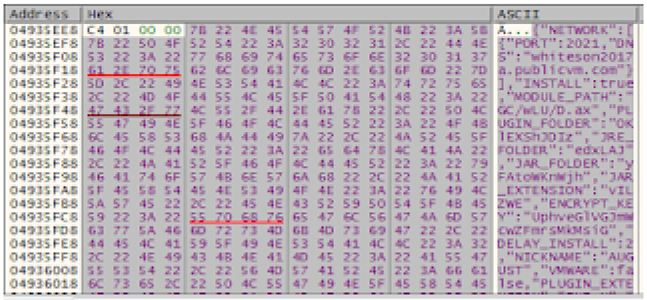
```
Address   Data
04935C28  44 45 4C 41 59 5F 49 4E 53 54 41 4C 4C
04935E08  44 45 4C 41 59 5F 49 4E 53 54 41 4C 4C
04935FE8  44 45 4C 41 59 5F 49 4E 53 54 41 4C 4C
04937D18  44 45 4C 41 59 5F 49 4E 53 54 41 4C 4C
```

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.

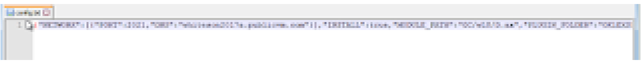
Step 10:

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



```
Address   Hex                                              ASCII
04935EE8  C4 01 00 00 7B 22 4E 45 54 57 4F 52 4B 22 3A 5B  A...{"NETWORK":[
04935EF8  7B 22 50 4F 52 54 22 3A 32 30 32 31 2C 22 44 4E  {"PORT":2021,"DN
04935F08  53 22 3A 22 77 68 69 74 65 73 6F 6E 32 30 31 37  S":"whiteson2017
04935F18  61 2E 70 75 62 6C 69 63 76 6D 2E 63 6F 6D 22 7D  a.publicvm.com"}
04935F28  5D 2C 22 49 4E 53 54 41 4C 4C 22 3A 74 72 75 65  ],"INSTALL":true
04935F38  2C 22 4D 4F 44 55 4C 45 5F 50 41 54 48 22 3A 22  ,"MODULE_PATH":"
04935F48  47 43 2F 77 4C 55 2F 44 2E 61 78 22 2C 22 50 4C  GC/wLU/D.ax","PL
04935F58  55 47 49 4E 5F 46 4F 4C 44 45 52 22 3A 22 4F 4B  UGIN_FOLDER":"OK
04935F68  6C 45 58 53 68 4A 44 49 7A 22 2C 22 4A 52 45 5F  lEXShJDIz","JRE_
04935F78  46 4F 4C 44 45 52 22 3A 22 65 64 78 4C 41 4A 22  FOLDER":"edxLAJ"
04935F88  2C 22 4A 41 52 5F 46 4F 4C 44 45 52 22 3A 22 79  ,"JAR_FOLDER":"y
04935F98  46 41 74 6F 57 4B 6E 57 6A 68 22 2C 22 4A 41 52  FAtoWKnWjh","JAR
04935FA8  5F 45 58 54 45 4E 53 49 4F 4E 22 3A 22 76 49 4C  _EXTENSION":"vIL
04935FB8  5A 57 45 22 2C 22 45 4E 43 52 59 50 54 5F 4B 45  ZWE","ENCRYPT_KE
04935FC8  59 22 3A 22 55 70 68 76 65 47 6C 56 47 4A 6D 57  Y":"UphveGlVGJmW
04935FD8  63 77 5A 46 6D 72 73 4D 6B 4D 73 69 47 22 2C 22  cwZFmrsMkMsiG","
04935FE8  44 45 4C 41 59 5F 49 4E 53 54 41 4C 4C 22 3A 32  DELAY_INSTALL":2
04935FF8  2C 22 4E 49 43 4B 4E 41 4D 45 22 3A 22 41 55 47  ,"NICKNAME":"AUG
04936008  55 53 54 22 2C 22 56 4D 57 41 52 45 22 3A 66 61  UST","VMWARE":fa
04936018  6C 73 65 2C 22 50 4C 55 47 49 4E 5F 45 58 54 45  lse,"PLUGIN_EXTE
```

Congratulations! You exported your first Adwind/JRAT config!



config.txt

```
1 {"NETWORK":[{"PORT":2021,"DNS":"whiteson2017a.publicvm.com"}],"INSTALL":true,"MODULE_PATH":"GC/wLU/D.ax","PLUGIN_FOLDER":"OKlEX
```

Installing Rudra to analyze PCAPs and PE files