Unpacking Pyrogenic/Qealler using Java agent -Part 0x2

By Ayush Anand

Published: 2020-01-17 · Archived: 2026-04-05 21:43:39 UTC

January 17, 2020

We will learn how and when we can use **Java agent** to quickly unpack the Pyrogenic Infostealer. In the earlier post Pyrogenic Infostealer static analysis – Part 0x1 we statically analysed the Pyrogenic/Qealler Infostealer but this requires more time and effort. We will be using the same sample PaymAdviceVend_LLCRep.jar from ANY.RUN (MD5: **F0E21C7789CD57EEBF8ECDB9FADAB26B**) used in Part 0x1. Let's start with a basic introduction to Java agent.

CONTENTS

Introduction to Java agent

A Java agent is used to instrument programs running on the JVM and it can modify the Java bytecode at runtime without source code. In this post we will be using a Java agent to dump the classes during runtime without any bytecode modification but for more details please check this Java Agents Tutorial [1]. These are the minimum requirement for Java agent to work:

1. Java agent class file should have a **premain** method which acts as the entry-point.This method is executed before the real java application main method, premain method it's like TLS callback.
2. MANIFEST.MF should be defined with the **Premain-Class** attribute, which will point to class name with premain method. Another important point is there **must be a new line at the end of the MANIFEST file**. Otherwise, the last header is ignored.
3. javaagent parameter should be specified to load java agent jar file with premain method e.g . `java -javaagent:dumper.jar -jar malware.jar`

Unpacking using Java agent

dumper.java & **MANIFEST.mf** are used to build Java agent dumper.jar. **dumper.java** code is copied from Reversing an obfuscated java malware pdf [2] and I will highly recommend to go through the pdf[2] to understand

the different methods which can be used to analyse Java malware.

grade

Note: All java, MANIFEST and jar files are uploaded to GitHub repo[3].

dumper.java

```
 import java.io.*;
import java.lang.instrument.*;
import java.security.*;

// This code is copied from "Reversing an obfuscated java malware by Extreme Coders"
public class dumper {
    //A java agent must have a premain method which acts as the entry-point
    public static void premain(String agentArgs, Instrumentation inst) {
        System.out.println("agent loaded");
        // Register out trasnformer
        inst.addTransformer(new transformer());
    }
}

class transformer implements ClassFileTransformer {
    // The transform method is called for each non-system class as they are being loaded
    public byte[] transform(ClassLoader loader, String className,
        Class < ? > classBeingRedefined, ProtectionDomain protectionDomain,
        byte[] classfileBuffer) throws IllegalClassFormatException {
        if (className != null) {
            // Skip all system classes
            if (!className.startsWith("java") &&
                !className.startsWith("sun") && !className.startsWith("javax") && !className.startsWith("com") &
                System.out.println("Dumping: " + className);
                // Replace all separator characters with _
                String newName = className.replaceAll("/", "_") + ".class";
                try {
                    FileOutputStream fos = new FileOutputStream(newName);
                    fos.write(classfileBuffer);
                    fos.close();
                } catch (Exception ex) {
                    System.out.println("Exception while writing: " + newName);
                }
            }
        }
        // We are not modifying the bytecode in anyway, so return it as-is
        return classfileBuffer;
```

```
    }
}
```

MANIFEST.mf

```
Manifest-Version: 1.0
Premain-Class: dumper
```

grade

Note: If you know the basic of Java or any other object oriented programming language then it will be much easier to understand this dumped unpacked code.

1. Uploaded the jar file in GitHub repo[3] which is generated using following command: `javac dumper.java` `jar cmf MANIFEST.MF dumper.jar dumper.class transformer.class`
2. Execute this command `java -javaagent:dumper.jar -jar BankPaymAdviceVend_LLCRep.jar` to run the malware with java agent and it will dump all the accessed classes at runtime to the current working directory.
3. Please decompile all the dumped class files which start with q0b4 and j/t/e package name files using ByteCodeViewer FernFlower Java decompiler. One of the easiest way is to zip all classes and then use BCV. Then, import decompiled java source files from BCV into any Java IDE, this will help you in code navigation.
4. Start from the bottom and go up in the above pic then you will find the first proper package name q0b4/bootstrap/templates/Header which can be our starting point for unpacked code. We are Reverse engineers, we always start in reverse order :).
5. Below pic shows all the unpacked classes dumped using Java agent dumper.jar. It starts from ***Header.java*** which uses a decrypt function to AES decrypt the classes at runtime and invoke the main method. It invokes j.t.e.Main package main method.

grade

Other approach is to dump all the classes present in obfuscatedEntryList using for loop and continue analysis

Dumped class file analysis

Malware authors divided the source code in multiple sensible packages. They have made our job easier by giving proper names to functions, variables and classes. We will go through some of the classes ***Main***, ***Server***, ***MainEx*** and one util ***IPAddress*** class, as it will take too much time to go through each one of them.

Main & Server class

- - ***Main*** class invokes the loadLibrary method which sends the cmd to CC using ***sendCmd*** method.
  - ***Server*** class contains function ***loadLibrary*** which is used above and ***pushCredentials*** which is used to send the stolen credential to CC.

- ***Server*** class contain the following list of available library and cmds:

```
public static final int PYTHON = 162144;
public static final int SQLITE = 4353152;
public static final int JNA = 224288;
public static final int JNA_PLATFORM = 3048576;
public static final int JNA_4 = 307200;
public static final int JNA_PLATFORM_4 = 308224;
public static final int BCPROV = 310272;
public static final int INI4J = 311296;
public static final int XML = 312320;
public static final int JSON = 313344;
public static final int W3DOM = 314368;
public static final int Q4_PASS_LIB = 315392;
public static final int JPOWERSHELL = 316416;
private static final int LIBRARY_CMD = 16384;
private static final int CREDENTIAL_CMD = 32768;
private static final byte[] SEED = "uisdfysdgfbsdyufbsiybfsdyb733grfsudbfjh".getBytes();
private static final int MAX_TRY_COUNT = 20;
```

Malware author didn't pack all the required Java libraries in the jar but it is requested when needed at runtime. This significantly decreased the malware size to 153.27 Kb. Let's discuss some of the library and commands used:

1. 1. 1. **Server JNA, JNA_4, JNA_PLATFORM, JNA_PLATFORM_4** – JNA (Java Native Access) provides simplified access to native library methods without requiring any additional JNI or native code. For example you can call printf, GetSystemTime Windows API function directly from Java Code.
   2. **INI4j** – Java API for handling configuration files in Windows .ini format
   3. **JPOWERSHELL** – Simple Java API that allows programs to interact with PowerShell console. It may be used when malware invokes any PowerShell commands.
   4. **Q4_PASS_LIB** – May be Qealler v4 Password Library loaded first using `list.add(server.loadLibrary(315392));`
   5. **LIBRARY_CMD** – May be used to load the clean dll used sqlitejdbc.dll and jnidispatch.dll
   6. **CREDENTIAL_CMD** – This cmd is used to ***pushCredentials*** to CC

MainEx class

- **j.t.e.Main** main method invokes the ***j.t.e.MainEx*** main method as shown above in **Main** class. It sent credential and system info in JSON format to CC. All the communication are AES encrypted using ***EncryptedCipherOutputStream*** and ***EncryptedCipherInputStream*** which extends ***CipherOutputStream*** & ***CipherInputStream*** respectively.
- ***MainEx*** class contains two important methods: ***run()*** and **getSysinfo()** as shown below.
- Malware steal credential from list of software mentioned in the ***run()*** method

```
 this.addAll(ChromiumBased.chromiumBasedBrowsers);
this.addAll(MozillaBased.mozillaBasedBrowsers);
this.add(new IExplorer());
this.add(new UCBrowser());
this.add(new Composer());
this.add(new Credman());
this.add(new Outlook());
this.add(new Pidgin());
this.add(new PostgreSQL());
this.add(new Squirrel());
this.add(new Tortoise());
```

- **getSysinfo()** collect osName, osVersion, osArch, javaHome, userName, userHome, availableProcessor, freeMemory, totalMemory, localIpAddress & globalIpAddress in JSON format which is encrypted and sent to CC with other info.

IPAddress class

- ***IPAddress*** class is one of the classes present in package ***j.t.e.core.utils*** which gets the IP address of the infected system and sends it to CC with other system info. It uses http://bot.whatismyipaddress.com for collecting the public IP of infected systems.

When will it fail?

Unpacking using Java agent will be unable to dump all the classes at runtime due to following conditions:

- When malware is unable to interact with CC then it will not be able to exhibit complete behaviour.
- Malware is using some anti analysis technique e.g checking for vmware etc.
- Malware is unable to run due to some supporting files, command line etc.

Conclusion

Unpacking using a Java agent is quite simple and can speed up your analysis, you can use the dumper.jar uploaded in Github [3]. This method can be used in any Java based malware. We have also gone through some of the dumped Pyrogenic/Qealler source code to understand the stealer functionality. In the last part 0x3 we find similarity between Qealler/Pyrogenic variants based on static code analysis.

Targeted Application list

This is the list of application collected from the dumped unpacked classes:

1. ChromiumBased Browser
    - 7Star
    - amigo
    - brave

    - centbrowser
    - chedot
    - chrome canary
    - chromium
    - coccoc
    - comodo dragon
    - elements browser
    - epic privacy browser
    - google chrome
    - kometa
    - opera
    - orbitum
    - sputnik
    - torch
    - uran
    - vivaldi
    - yandexBrowser
2. MozillaBased Browser
    - firefox
    - blackHawk
    - cyberfox
    - comodo IceDragon
    - k-Meleon
    - icecat
3. IExplorer
4. UCBrowser
5. Composer
6. Windows Credential
7. Outlook
8. Pidgin
9. PostgreSQL
10. Squirrel
11. Tortoise

References

1. Java Agents Tutorial
2. Reversing an obfuscated java malware by Extreme Coders
3. GitHub repo

Thanks for reading. Feel free to connect with me on or LinkedIn for any suggestions or comments.

For more updates and exclusive content, subscribe to our newsletter. Stay sharp. Keep defending.😊
