

# Java Bayt Kod Hata Ayıklaması

written by Mert SARICA | 1 July 2015

Tarık Y. sağolsun 10 Ekim 2013 tarihinden bu yana kendisine gelen ve ekinde zararlı yazılım bulunan çoğu sahte e-postayı incelemem için benimle paylaşıyor. Kendisine gönderilen e-postalara bakıldığında, 2013 yılından bu yana aktif olarak java ile zararlı yazılım geliştiren (indirici/dropper) ve sahte e-postalar gönderen bir grubun bu e-postaların arkasında olduğunu anlamak çok zor değil. Antivirüs yazılımlarını atlama için çeşitli gizleme (obfuscator) araçlarından da faydalanan bu grup, her salgında ikna adına aşağıdaki gibi yeni senaryolar kullanmaktan çekinmiyor.

## Task sonucu bilgilendirme.



extratap.turkcell.com.tr Kişilere ekle 03.03.2015 ▶

Kime: tarik

Değerli Bayiimiz;

Aşağıda kimlik bilgileri bulunan abonemiz için açmış olduğunuz task sonuçlanmıştır.

Akışı izlemek için lütfen linke tıklayınız..

<http://global-bilgi.com.tr/attachmt/tasksonucu/>



Zararlı yazılım geliştiricileri çoğunlukla indiricileri geliştirirken Java programlama dilinden faydalanyor olmalarının en büyük sebebi, Java'nın

yorumlanan (interpreted) bir programlama dili olmasıdır. Bu sayede CLASS dosyasına derlenen .JAVA uzantılı bir kod, Java Virtual Machine (JVM) tarafından çalışma esnasında yorumlanarak makine diline dönüştürülmektedir. Bu durum da JAVA programlama dili ile yazılan zararlı yazılımların Antivirüs yazılımları tarafından kimi durumlarda yorumlanamamasına sebebiyet vermektedir. Ayrıca JVM tarafından çalıştırılan JAR uzantılı yürütülebilir dosyalar veya CLASS uzantılı dosyalar, Ollydbg veya Immunity Debugger gibi hata ayıklayıcılar tarafından çalıştırılmaz dolayısıyla dinamik kod analizi ile analiz edilmesi, PE dosyalara kıyasla daha zordur.

Ancak yorumlanabilir diller, diğer dillerin aksine kaynak koduna geri çevrilebilmektedir (decompile). Zararlı yazılım analistleri için ilk bakışta bu büyük bir nimet gibi görünse de, bunu bilen zararlı yazılım geliştiricileri, Allatori gibi gizleme araçlarından (obfuscator) faydalanmaktadırlar. Böyle bir durumla karşılaştığınız zaman statik bayt kod analizi ile ilerlemek iyi bir tercih gibi görünse de, dinamik bayt kod analizinin yerini zaman ve pratiklik açısından tutmayacaktır.

Allatori gibi araçların özelliklerine baktığınız zaman analizi güçleştiren çeşitli özellikler ile donatıldığını görebilirsiniz dolayısıyla kaynak koduna çevirme ve dinamik bayt kod analizi konusunda sıkıntı yaşayacağınız bir gerçektir!

Örneğin aşağıdaki sahte e-posta ile gönderilen JAR dosyasını Java Decompiler aracı ile kaynak koduna çevirmeye çalıştığımızda kaynak kodunu görüntülemiyor olmamız bizi pek şaşırtmıyor.

FW: 12.01.2015 Tarihli [redacted] Platinum TL Hesap Özeti (Ref:5150228026)?

↑ ↓ ×



bank.com 05:59

Kime: [redacted]

Eylemler

Kimden: bank.com (info@bank.com) Bu gönderen kişi listenizde var.

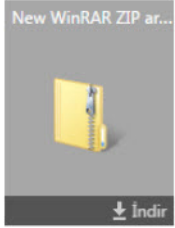
Gönderme tarihi: 13 Ocak 2015 Salı 05:59:58

Kime: [redacted]

Dikkatli olun! Bu gönderen, sahtekarlık algılama denetlememizi geçemedi.

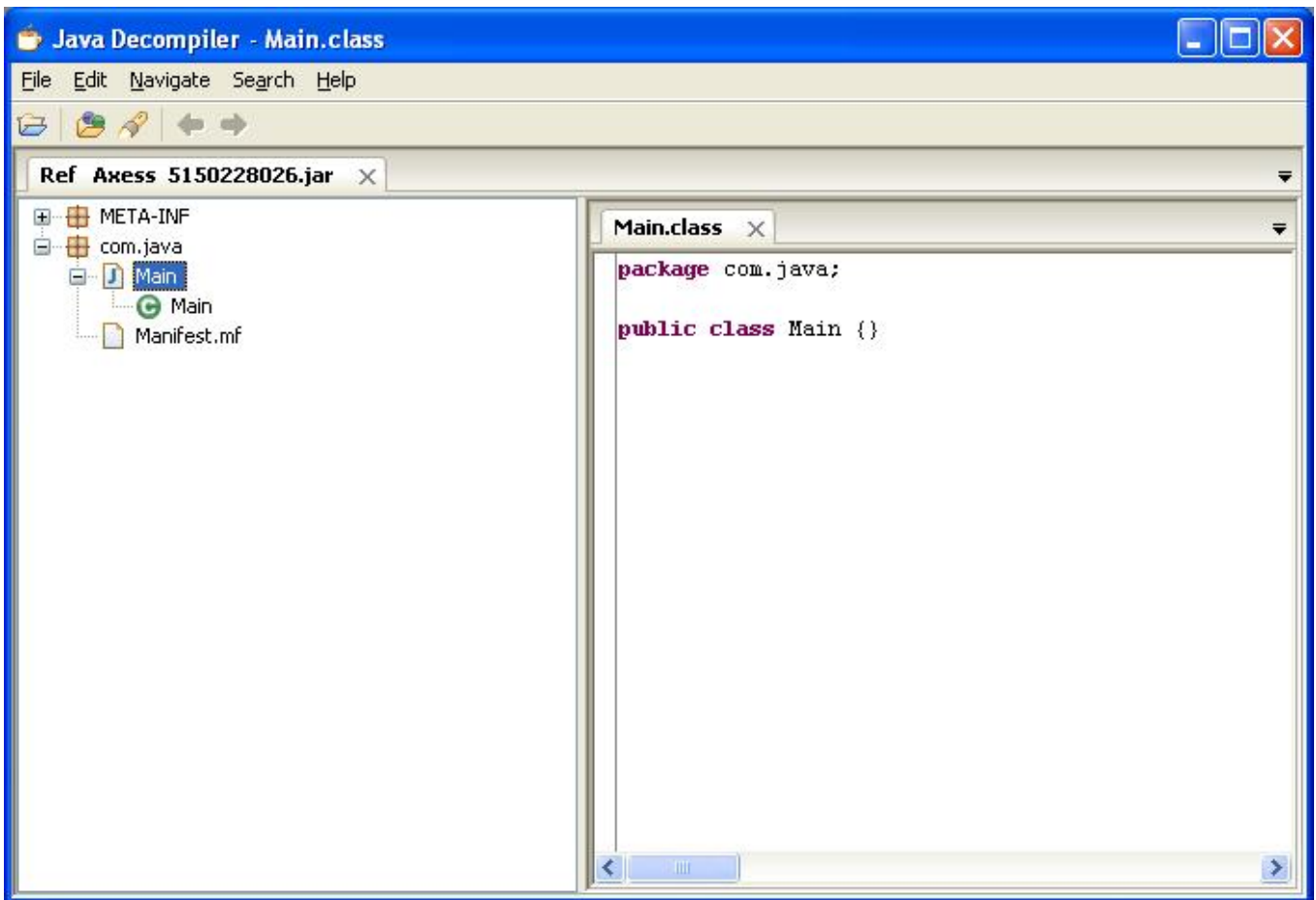
1 ek (4,8 KB)

Outlook.com Etkin Görünüm

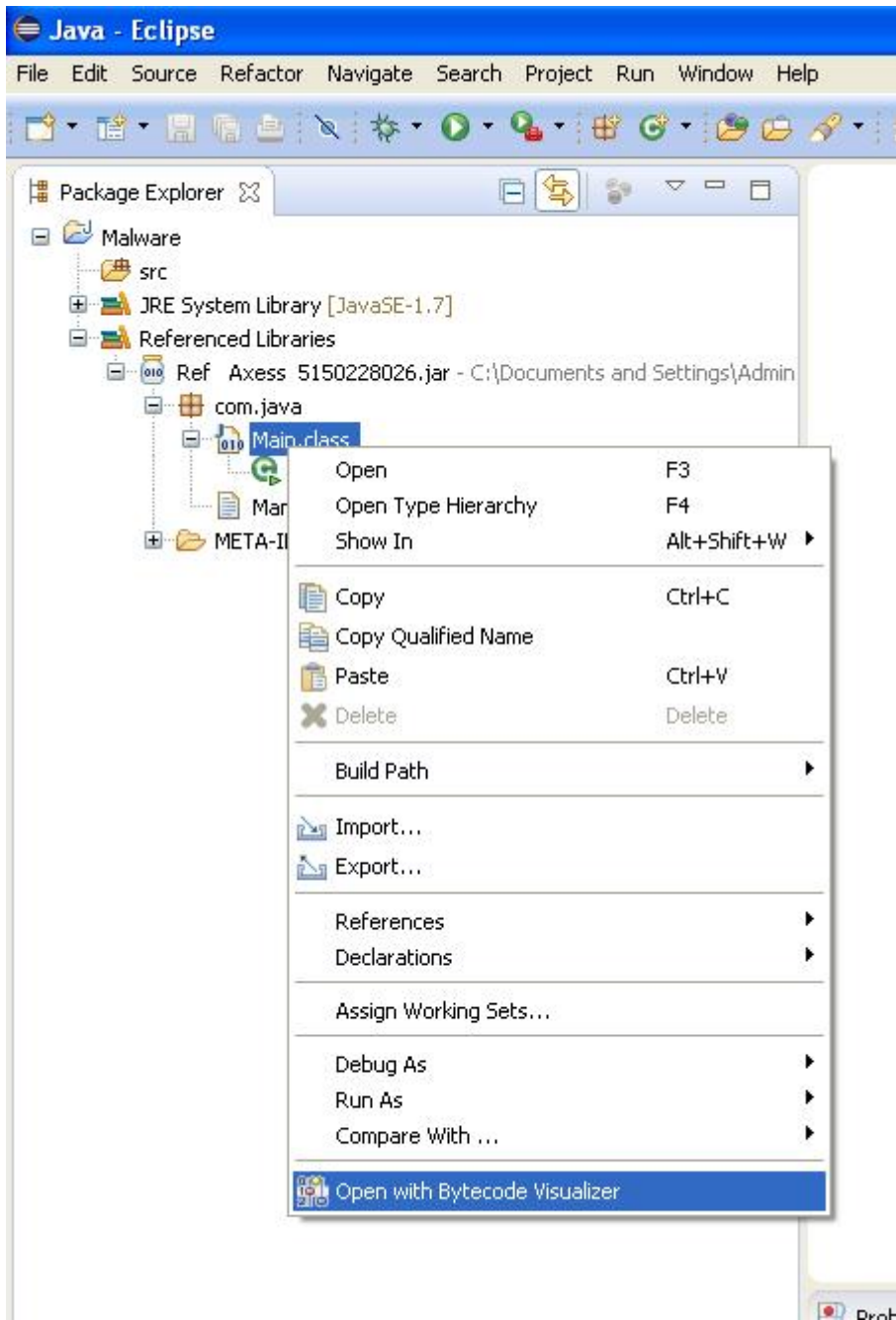


Zip olarak indir

\*\*\*\*\*2159 numaralı [redacted] Platinum TL hesap özeti ekteki dosyada bilgilerinize sunulmuştur



Aynı şekilde Eclipse eklentisi olarak kullanılan ve bir bayt kod hata ayıklayıcısı olan Dr. Garbage Bytecode Visualizer aracı ile de JAR dosyasını çalıştırdığımızda bir hata ile karşılaşmamız da bizi şaşırtmıyor.



```
/* ***** */
/* Generated by Dr. Garbage Bytecode Visualizer */
/* http://www.drgarbage.com */
/* Version: 4.4.1.201408050542 */
/* Class retrieved from: Filesystem */
/* Retrieved on: 2015-03-21 12:53:03.062 */
/* ***** */

/* class file format version 50.0 (java 1.6) */
package com.java;

public class Main {

    /* compiled from i */

    private static boolean IiiIIIIIII;

    private static boolean IIIIiIIIII;

    private static boolean ALLATORIXDEMOPalermoAustralia;

    public static void main(java.lang.String[] IiiIiiIIII) throws java.io.I
0  getstatic 2;          /* java.lang.System.out */
3  ldc_w 337;           /* "w1\u0011\u000fr#^+V,Q/R#^+V,Q!\\-P/R1
6  invokestatic 324;    /* java.lang.String com.java.Main.ALLATOR
9  invokevirtual 3;     /* void println(java.lang.String arg0) */
/* L403 */
12 ldc_w 339;          /* "0:Vb\u0002o\u000fn)\u0018<\u001c\\=a
15 invokestatic 324;   /* java.lang.String com.java.Main.ALLATOR
```

```
/* ***** */
/* Generated by Dr. Garbage Bytecode Visualizer */
/* http://www.drgarbage.com */
/* Version: 4.4.1.201408050542 */
/* Class retrieved from: Filesystem */
/* Retrieved on: 2015-03-21 12:53:03.062 */
/* ***** */

/* class file format version 50.0 (java 1.6) */
package com.java;

public class Main {

    /* compiled from i */

    private static k

    private static k

    private static k

    public static v
0  getstatic 2;          /* java.lang.System.out */
3  ldc_w 337;           /* "w1\u0011\u000fr#^+V,Q/R#^+V,Q!\\-P/R1
6  invokestatic 324;    /* java.lang.String com.java.Main.ALLATOR
9  invokevirtual 3;     /* void println(java.lang.String arg0) */
/* L403 */
12 ldc_w 339;          /* "0:Vb\u0002o\u000fn)\u0018<\u001c\\=a
15 invokestatic 324;   /* java.lang.String com.java.Main.ALLATOR
```

Aşağıdaki adımlardan sırasıyla geçerek hızlıca Dr. Garbage araçlarını yükleyebilir ve zararlı JAR dosyasını analiz edebilirsiniz.



Java - Eclipse

File Edit Source Refactor Navigate Search Project Run Window Help

Package Explorer

Help

- Welcome
- Help Contents
- Search
- Dynamic Help
- Key Assist... Ctrl+Shift+L
- Tips and Tricks...
- Report Bug or Enhancement...
- Cheat Sheets...
- Check for Updates
- Install New Software...
- Installation Details
- Eclipse Marketplace...**
- About Eclipse


Eclipse Marketplace

Select solutions to install. Press Finish to proceed with installation.  
Press the information button to see a detailed overview and a link to more information.

Search Recent Popular Installed January 02/24

Find:  All Markets All Categories

**Bytecode Visualizer 4.4.0**




Bytecode Visualizer is a tool used for visualizing and debugging Java byte code.  
Features Overview: Bytecode Viewer Signatures of classes, fields and methods...  
[more info](#)

by Dr. Garbage Community, Apache 2.0  
[java bytecode decompiler debugger control flow graph](#)

★ 32  Installs: **11,6K** (360 last month)

---

**Bytecode Outline 2.4.3**




Bytecode Outline plugin shows disassembled bytecode of current java editor or class file, allows bytecode compare for java/class files and shows ASMifier code for...  
[more info](#)

by Andrey Loskutov, EPL  
[java bytecode decompiler asm](#)

★ 43  Installs: **13,7K** (327 last month)

---

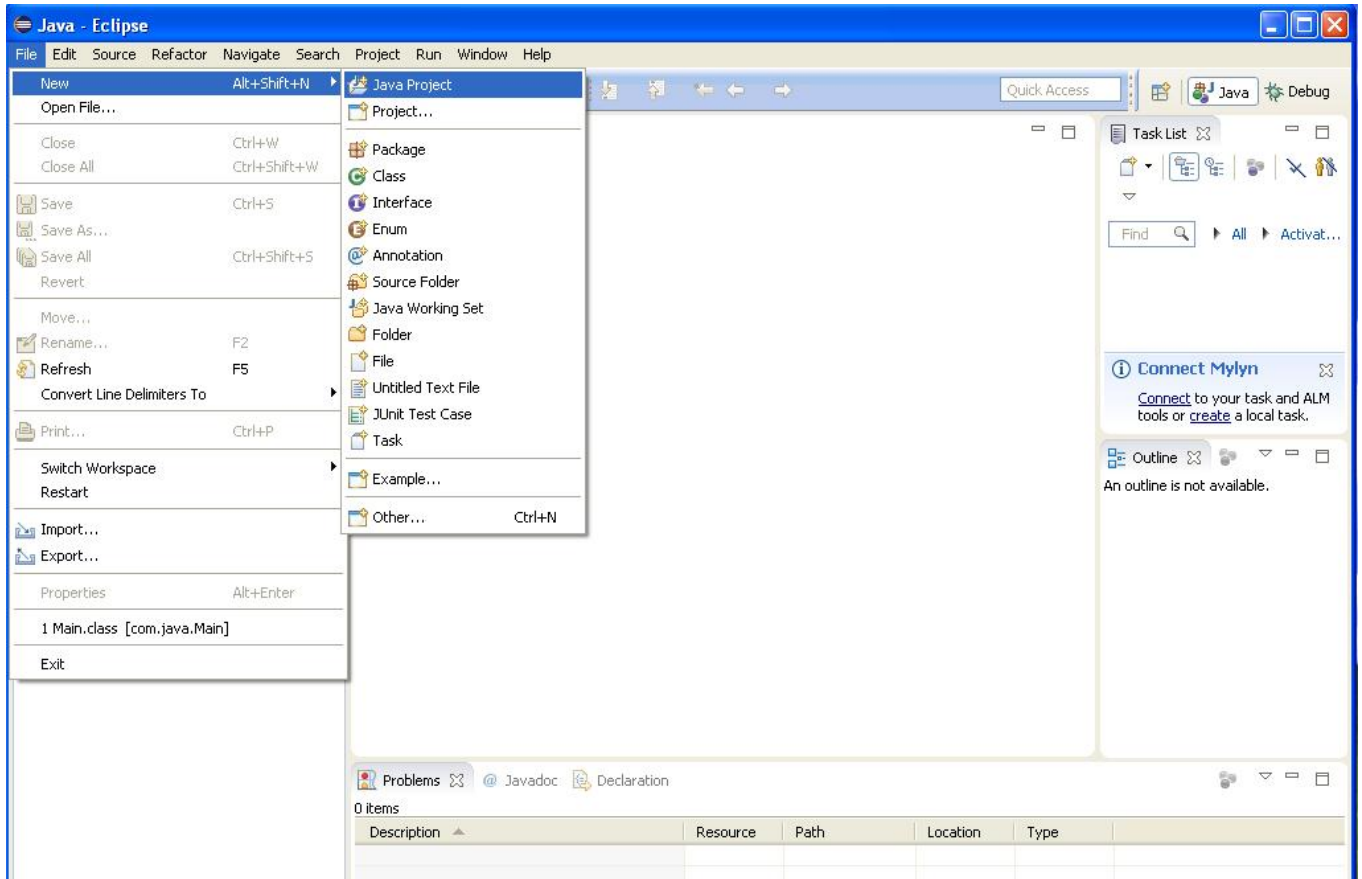
**BLU AGE LC2C - application modernization of PowerBuilder, NatStar, VisualBasic, Delphi... 2014 Edition**



MDA compliant and built on Eclipse, BLU AGE ® generates UML models from legacy applications' source code and instantly transforms them into "Cloud ready" Java EE...  
[more info](#)

by Blu Age Corp., Commercial

★ 1  Installs: **0** (0 last month)



## New Java Project

### Create a Java Project

Create a Java project in the workspace or in an external location.



Project name:

Use default location

Location:

#### JRE

Use an execution environment JRE:

Use a project specific JRE:

Use default JRE (currently 'jre7') [Configure JREs...](#)

#### Project layout

Use project folder as root for sources and class files

Create separate folders for sources and class files [Configure default...](#)

#### Working sets

Add project to working sets

Working sets:



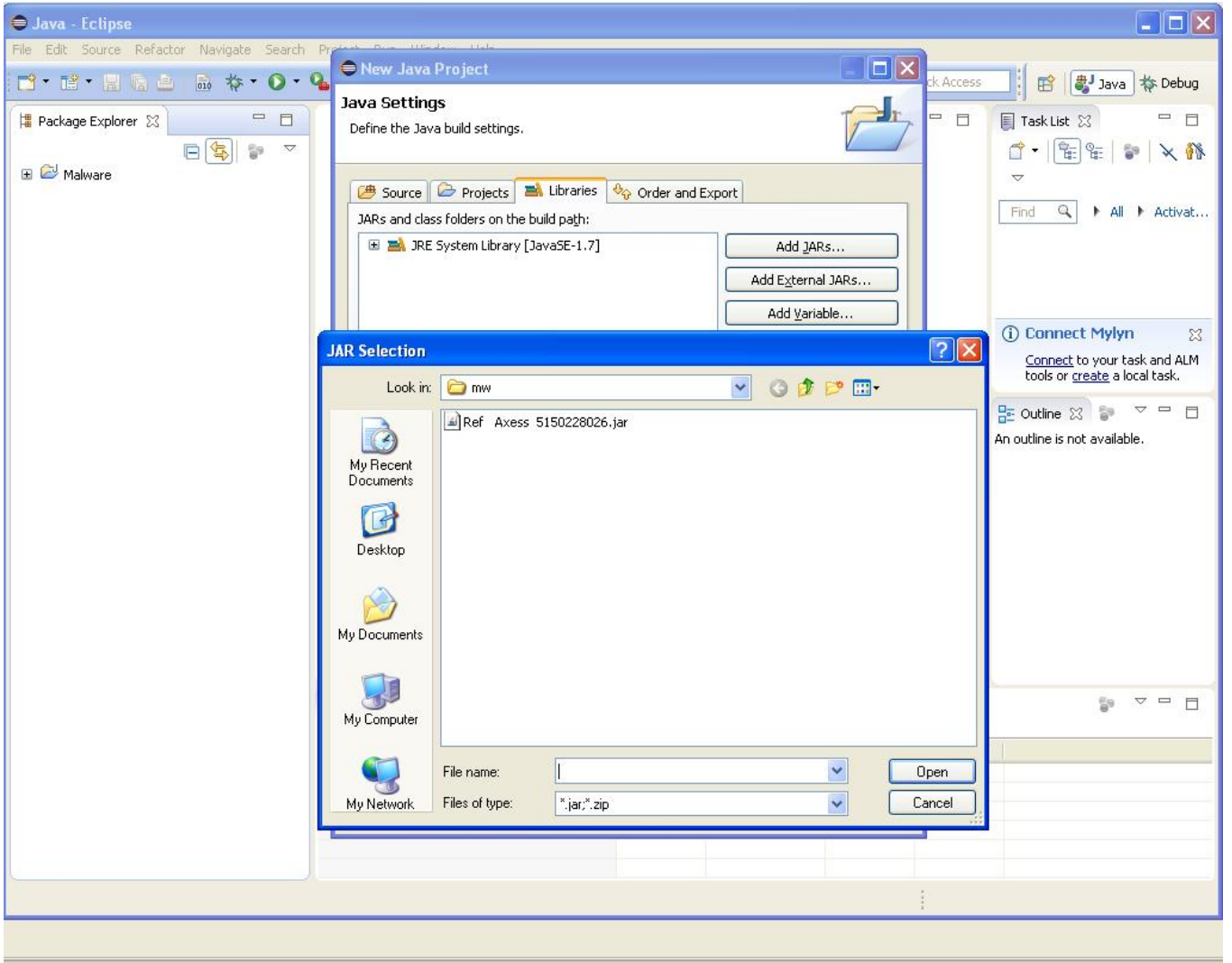
< Back

Next >

Finish

Cancel





Bu tür analizi zorlaştırmaya yönelik yöntemlerden faydalanan Java zararlı yazılımlarına karşı reJ isimli, Java bayt kodunu manipüle etmeye imkan tanıyan araçlardan faydalanabilirsiniz. Örneğin reJ aracı ile Ref Axess 5150228026.jar dosyasını incelediğimizde Main fonksiyonunda tanımlanan çok sayıda istisnanın (exceptions) şüpheli olduğu dikkatimizi çekiyor. İstisna listesini kısaltıp kayıt ettikten sonra bu Java dosyasını başarıyla Dr. Garbage'nin bayt kod hata ayıklama aracı ile analiz edebildiğimizi görüyoruz. Bundan sonrası ise artık ilgili yerlere kesme noktası (breakpoint) koymaya ve analiz etmeye kalıyor.

reJ - C:\Documents and Settings\Administrator\Desktop\mw\Ref\_Acess\_5150228026.jar

File Edit Navigate View Tools

Open Save Save as... InsertL Remove Find... Exit

Files Editor

Bytecode Editor: com.java.Main

```

import java.io.File;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.io.OutputStream;
import java.io.Reader;
import java.net.URL;
import java.net.URLConnection;
import java.util.ArrayList;
import java.util.List;
import java.util.zip.GZIPInputStream;
import java.util.zip.ZipEntry;
import java.util.zip.ZipInputStream;
import javax.swing.JOptionPane;
import javax.swing.UIManager;
import javax.swing.UnsupportedLookAndFeelException;

// SourceFile = 1
// Class Version: 50.0
public class Main {

    private static boolean Iiiiiiii;
    private static boolean Iiiiiiii;
    private static boolean ALLATORIXDEMOpalermoAustralia;

    public static void main(String[] p0) throws IOException, ClassNotFoundException, InstantiationException, IllegalAccessException, UnsupportedLookAndFeelException {
        0  getstatic PrintStream System.out
        1  ldc_w String Constant "al r#^+V, Q/R#^+V, Q/\-D/r1 (U#^4I#^1 z#^+V, Q/R#^ V/R"_,S, Qo +V ]T] o q ](U/R, Q ](U/R"_,S, Qo +V#^#4J ]o q ^+U, R, Q# ](U/Q! -P/Q1 (V#^7J#^1 q ](U/Q R ](U/R^\.P, Ro +U ]?
        2  invokestatic String Main.ALLATORIXDEMOpalermoAustralia(String)
        3  invokevirtual void PrintStream.println(String)
        4  Iiiiiiii_start:
        5  String[] Iiiiiiii (#0 12 - 45)
        6  ldc_w String Constant "0:Vb o n]u < \#k D |
        7  invokestatic String Main.ALLATORIXDEMOpalermoAustralia(String)
        8  ldc_w String Constant "N f z ~ Gn . ( A +[X#r KID]
        9  invokestatic String Main.ALLATORIXDEMOpalermoAustralia(String)
        10 invokestatic Object UIManager.get(Object)
    }
}

```

Method editor

public  static

synchronized  native

protected  private

abstract  final

Name: main

Return type: void

Parameters: java.lang.String[]

Exceptions: java.io.IOException, java.lang.ClassNotFoundException

Max Stack Size: 3

Max Locals: 1

Exception Chooser

java.lang.ClassNotFoundException

java.lang.InstantiationException

java.lang.IllegalAccessException

javax.swing.UnsupportedLookAndFeelException

Move Up

Move Down

Add... Edit... Remove

OK Cancel

Situation under control.

reJ - C:\Documents and Settings\Administrator\Desktop\mw\Ref\_Acess\_5150228026.jar

File Edit Navigate View Tools

Open Save Save as... InsertL Remove Find... Exit

Files Editor

Bytecode Editor: com.java.Main

```

import java.util.ArrayList;
import java.util.List;
import java.util.zip.GZIPInputStream;
import java.util.zip.ZipEntry;
import java.util.zip.ZipInputStream;
import javax.swing.JOptionPane;
import javax.swing.UIManager;
import javax.swing.UnsupportedLookAndFeelException;

// SourceFile = 1
// Class Version: 50.0
public class Main {

    private static boolean Iiiiiiii;
    private static boolean Iiiiiiii;
    private static boolean ALLATORIXDEMOpalermoAustralia;

    public static void main(String[] p0)
    {
        0  getstatic PrintStream System.out
        1  ldc_w String Constant "al r#^+V, Q/R#^+V, Q/\-D/r1 (U#^4I#^1 z#^+V, Q/R#^ V/R"_,S, Qo +V ]T] o q ](U/R, Q ](U/R"_,S, Qo +V#^#4J ]o q ^+U, R, Q# ](U/Q! -P/Q1 (V#^7J#^1 q ](U/Q R ](U/R^\.P, Ro +U ]?
        2  invokestatic String Main.ALLATORIXDEMOpalermoAustralia(String)
        3  invokevirtual void PrintStream.println(String)
        4  Iiiiiiii_start:
        5  String[] Iiiiiiii (#0 12 - 48)
        6  ldc_w String Constant "0:Vb o n]u < \#k D |
        7  invokestatic String Main.ALLATORIXDEMOpalermoAustralia(String)
        8  ldc_w String Constant "N f z ~ Gn . ( A +[X#r KID]
        9  invokestatic String Main.ALLATORIXDEMOpalermoAustralia(String)
        10 invokestatic Object UIManager.get(Object)
        11 invokestatic Object UIManager.put(Object, Object)
        12 invokestatic String UIManager.getSystemLookAndFeelClassName()
        13 invokestatic void UIManager.setLookAndFeel(String)
        14 new Main
        15 dup
        16 invokespecial void Main.<init>()
        17 pop2
        18 return
    }
}

```

Method editor

public  static

synchronized  native

protected  private

abstract  final

Name: main

Return type: void

Parameters: java.lang.String[]

Exceptions: java.io.IOException

Max Stack Size: 3

Max Locals: 1

Exception Chooser

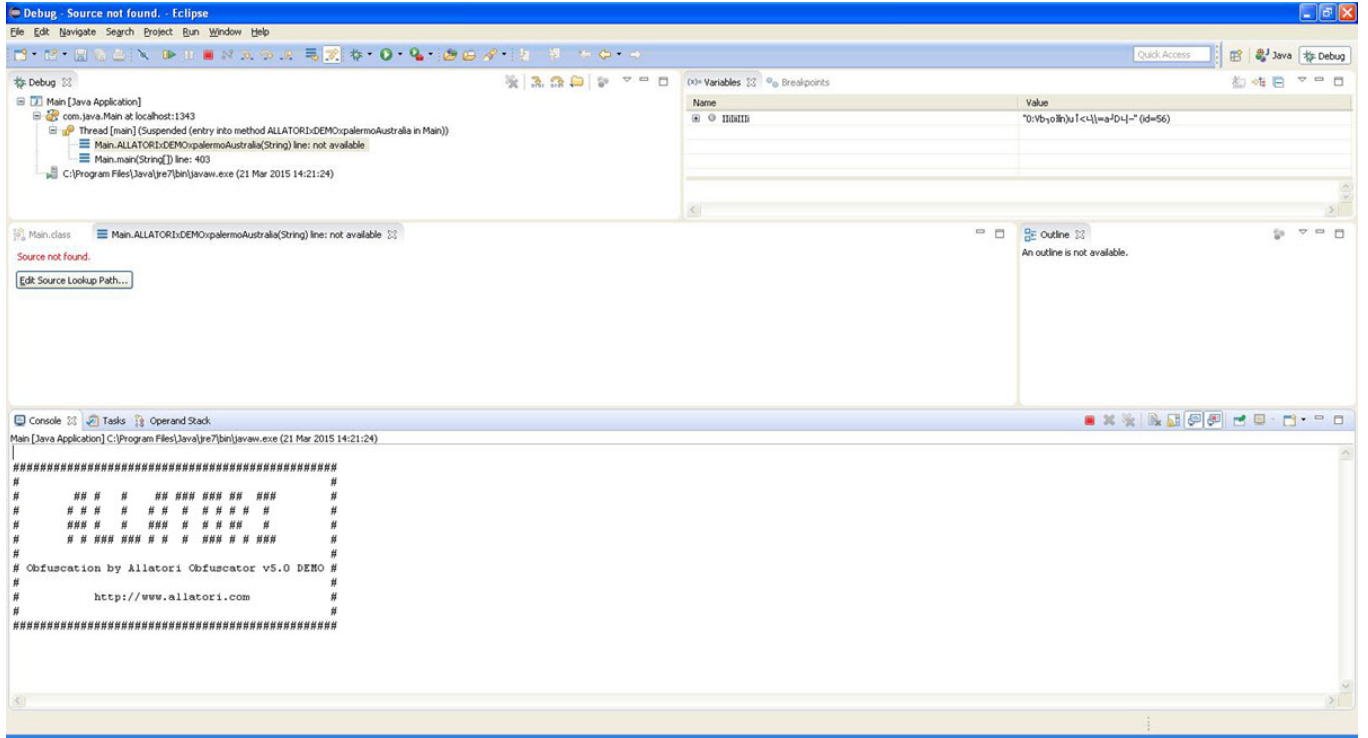
java.io.IOException

Move Up

Move Down

Add... Edit... Remove

OK Cancel



Java ile geliştirilen zararlı yazılımları analiz etme konusunda elinizin, kolunuzun bağlı olmadığını bilmeniz adına yazdığım bu yazı, umarım sizler için faydalı olmuştur. Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.