ID: 492006
Sample Name: NRB-RTGS 28-Sept 2021.jar
Cookbook: defaultwindowsfilecookbook.jbs
Time: 09:21:35
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

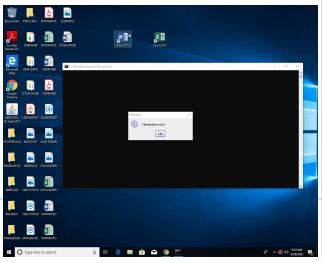
Windows Analysis Report NRB-RTGS 28-Sept 2021.jar

Overview

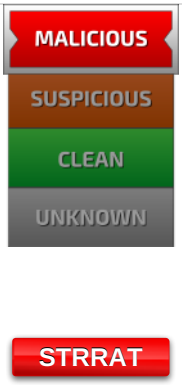
General Information

Sample Name:	NRB-RTGS 28-Sept 2021.jar
Analysis ID:	492006
MD5:	ccfdd7c24c9029f…
SHA1:	99dce2074fd2cca..
SHA256:	3ecc6468de96ac…
Tags:	jar STRRAT
Infos:	

Most interesting Screenshot:



Detection

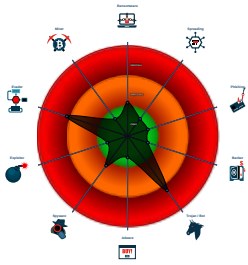


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected STRRAT
- Multi AV Scanner detection for subm…
- Yara detected AllatoriJARObfuscator
- Sample execution stops while proce…
- Uses cacls to modify the permission…
- Uses code obfuscation techniques (…
- Creates a process in suspended mo…
- Contains functionality to detect virtu…
- Contains functionality to query CPU …

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6364 cmdline: C:\Windows\system32\cmd.exe /c 7za.exe x -y -oC:\jar 'C:\Users\user\Desktop\NRB-RTGS 28-Sept 2021.jar' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - 7za.exe (PID: 584 cmdline: 7za.exe x -y -oC:\jar 'C:\Users\user\Desktop\NRB-RTGS 28-Sept 2021.jar' MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
- cmd.exe (PID: 4780 cmdline: 'C:\Windows\System32\cmd.exe' /c java.exe -jar 'C:\Users\user\Desktop\NRB-RTGS 28-Sept 2021.jar' carLambo.FirstRun >> C:\cmdlinestart.log 2>&1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 5408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - java.exe (PID: 5524 cmdline: java.exe -jar 'C:\Users\user\Desktop\NRB-RTGS 28-Sept 2021.jar' carLambo.FirstRun MD5: 28733BA8C383E865338638DF5196E6FE)
    - icacls.exe (PID: 4476 cmdline: C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant 'everyone':(OI)(CI)M MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 7036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\cmdlinestart.log	JoeSecurity_Allatori_JAR_Obfuscator	Yara detected Allatori_JAR_Obfuscator	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.930901668.0000000009DA4000.00000004.00000001.sdmp	JoeSecurity_Allatori_JAR_Obfuscator	Yara detected Allatori_JAR_Obfuscator	Joe Security	
00000008.00000002.930829373.0000000009D68000.00000004.00000001.sdmp	JoeSecurity_Allatori_JAR_Obfuscator	Yara detected Allatori_JAR_Obfuscator	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.929973894.00000000049EE000.00000004.00000001.sdmp	JoeSecurity_STRRAT	Yara detected STRRAT	Joe Security	
Process Memory Space: java.exe PID: 5524	JoeSecurity_STRRAT	Yara detected STRRAT	Joe Security	
Process Memory Space: java.exe PID: 5524	JoeSecurity_Allatori_JAR_Obfuscator	Yara detected Allatori_JAR_Obfuscator	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Data Obfuscation:

Yara detected AllatoriJARObfuscator

Stealing of Sensitive Information:

Yara detected STRRAT

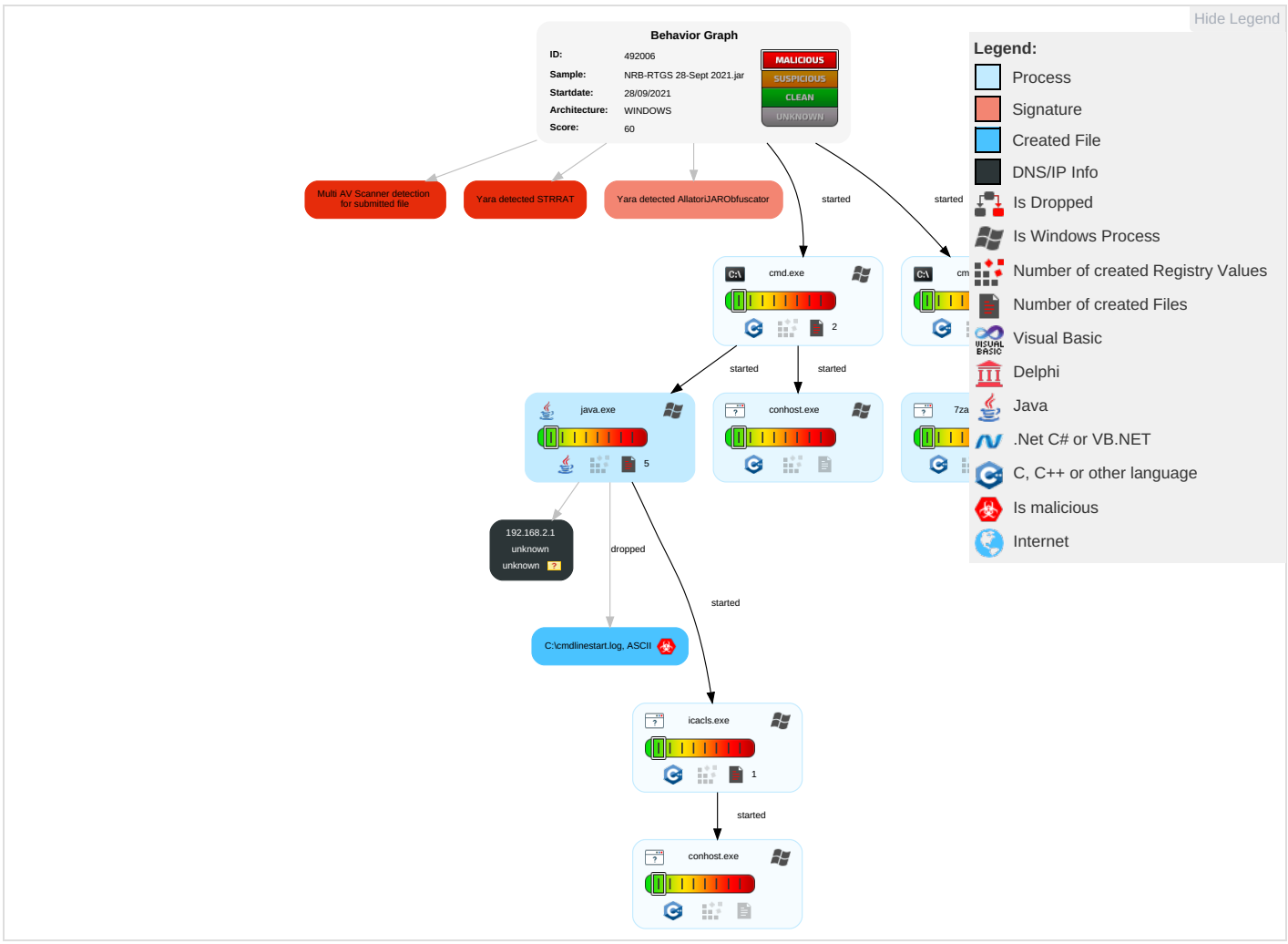
Remote Access Functionality:

Yara detected STRRAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Services File Permissions Weakness 1	Services File Permissions Weakness 1	Services File Permissions Weakness 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio

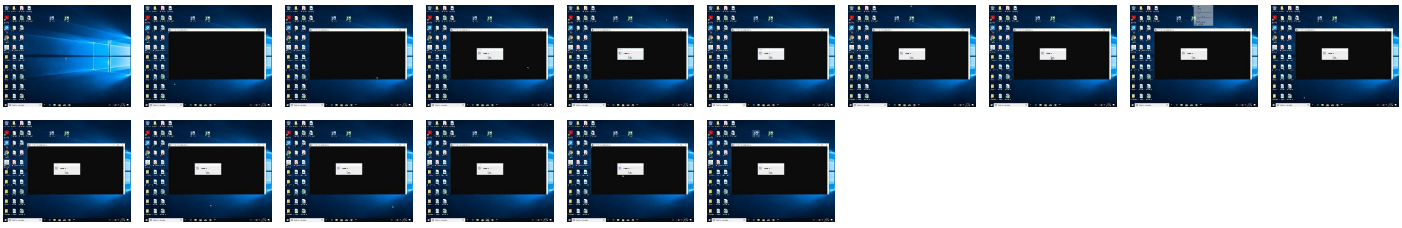
Behavior Graph

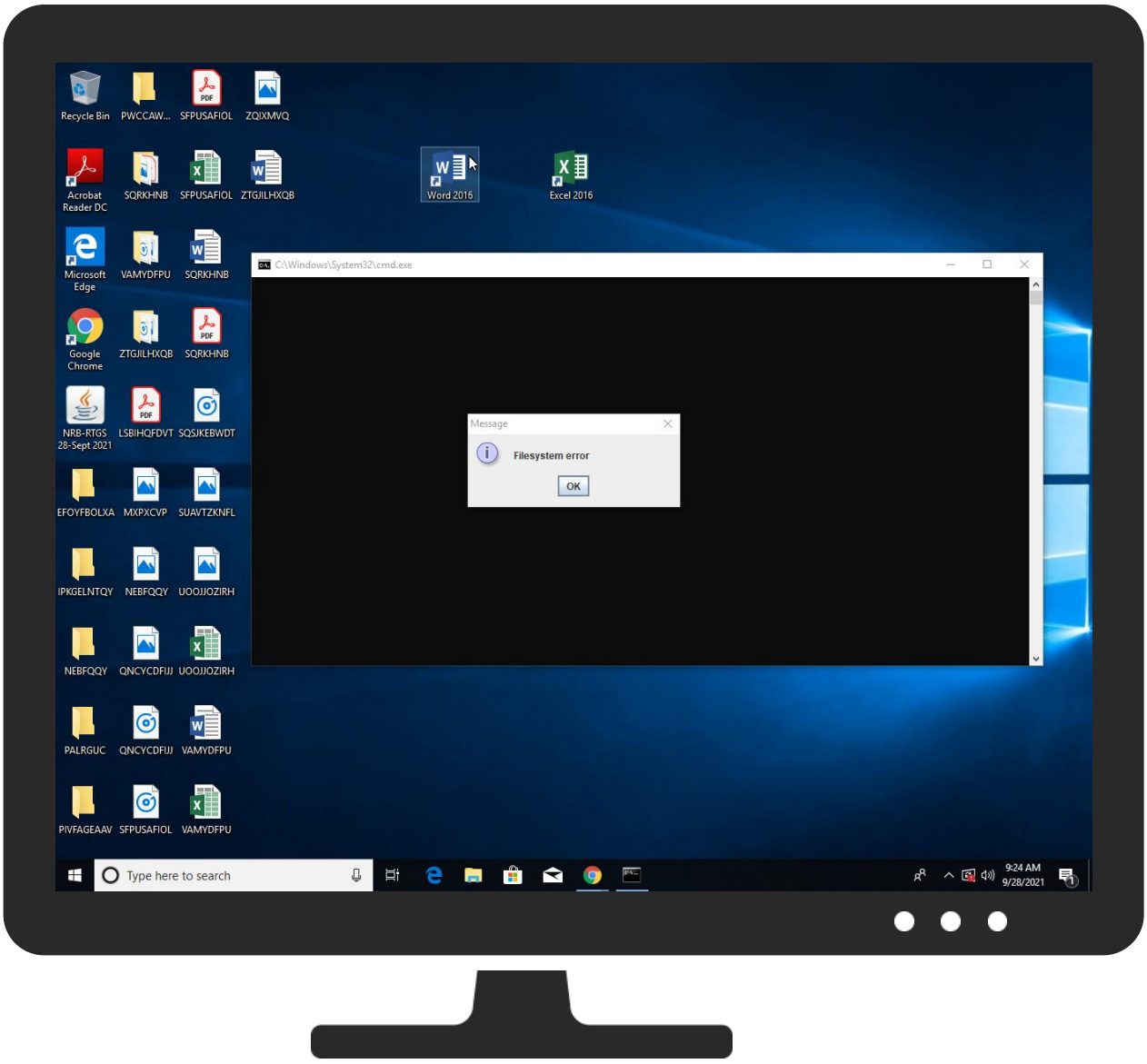


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
NRB-RTGS 28-Sept 2021.jar	22%	ReversingLabs	ByteCode-JAVA.Downloader.BanLoad	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.xrampsecurity.com/XGCA.crl	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl	0%	URL Reputation	safe	
http://bugreport.sun.com/bugreport/	0%	Virustotal		Browse
http://bugreport.sun.com/bugreport/	0%	Avira URL Cloud	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://jbfrost.live/strigoi/server/?hwid=1&lid=m&ht=5	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl	0%	URL Reputation	safe	
http://www.quovadis.bm	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://www.allatori.com	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl	0%	URL Reputation	safe	
http://www.chambersign.org	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492006
Start date:	28.09.2021
Start time:	09:21:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NRB-RTGS 28-Sept 2021.jar
Cookbook file name:	defaultwindowsfilecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Run name:	Without Tracing
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal60.troj.evad.winJAR@10/70@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 82% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .jar
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Oracle\Java\.oracle_jre_usage\cce3fe3b0d8d83e2.timestamp	
Process:	C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe
File Type:	ASCII text, with CRLF line terminators

C:\ProgramData\Oracle\Java\.oracle_jre_usage\cce3fe3b0d8d83e2.timestamp	
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.826151803897123
Encrypted:	false
SSDEEP:	3:oFj4I5vpN6yUaBSKn:oJ5X6yqy
MD5:	15B3464B5BC23F5081D8F3A065890445
SHA1:	071664F7CC8937AB309287821E7C36DE76D735FF
SHA-256:	114A7C21D54C375ED7216A1CE9D96D059FBD6589DBE1053E80B3E50F8BD7F03A
SHA-512:	DFF24B85E480728B80B931EF63CCE73A49DC1B71628F6DE1786D73E117B69C73992803286E2B0B41FD616FE097BCA8037E56DE047AEC0F183F72459CC41AA89
Malicious:	false
Preview:	C:\Program Files (x86)\Java\jre1.8.0_211..1632813753356..

C:\cmdlinestart.log	
Process:	C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	modified
Size (bytes):	591
Entropy (8bit):	1.945059257330099
Encrypted:	false
SSDEEP:	6:LLpG4/7s3FeFjtG22T0CgUS8F/SANtBomrGb4MEuigyy:nphg3FeFBio8FqANtaXNi1y
MD5:	51B3F0B0FC8D3569B20D44ACB265ED0E
SHA1:	BCDB0412FE416B952899A35F9294425FBCC5083B
SHA-256:	59A1122473B759357709DAF5170B04803C05EC24CBDE4D468C2DDB4421825737
SHA-512:	EB9388F875A55193FE5EF1333B82F00C13EC5F7C4510A8F2B2B974ACDB506F45B22CFF3A10E349F478E255C9A01871F002EB8BAF813D3AEEEA91F28EC4FAD91 C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Allatori_JAR_Obfuscator, Description: Yara detected Allatori_JAR_Obfuscator, Source: C:\cmdlinestart.log, Author: Joe Security
Preview:	.##.# #.# ## # # ## ### ### ## ### #.# # # # # # # # # # # # # #.# ### # # ### # # # ## # #.# # # ### ### # # # ### # # ### #.# #.# Obfuscation by Allatori Obfuscator v7.3 DEMO #.# #.# http://www.allatori.com #.# #.################################ ###################...

C:\jar\META-INF\MANIFEST.MF	
Process:	C:\Windows\System32\7za.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	305
Entropy (8bit):	5.120755883071443
Encrypted:	false
SSDEEP:	6:1KItJtf9FyucqNF2wuoxXbPWMXlUWKgLQAw0ZEc+sHK8FUs5Rr:1Tt/ffx1TBWMXZCLy59
MD5:	220D1487EEC578CBAAE87C65FB007D35
SHA1:	67C3B65562C7A72C8EE38625E3E5915D171307F3
SHA-256:	A1F4279A61FF6191D069A4AA9345FE3EA6BC14855AF52BF9B99A505EBF020CC0
SHA-512:	AAACA3BAD6D170A8C124632640BD158B8BC8E6BE8B73575D45DE1D5B134659C4BE42F9B40EEDD7980CFA1E1CC398D286E6084D5888C482B85BB3FBE746AF6 1C
Malicious:	false
Preview:	Manifest-Version: 1.0..Ant-Version: Apache Ant 1.7.1..Created-By: 24.80-b11 (Oracle Corporation)..Main-Class: carLambo.FirstRun..Class-Path: lib/system-hook-3.5.jar lib/jna-5.5.0.jar lib/jna-platform.. -5.5.0.jar lib/sqlite-jdbc-3.14.2.1.jar..X-COMMENT: Main-Class will be added automatically by build....

C:\jar\carLambo\FLUCgYjjYukBnLOPJmMXa.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	2481
Entropy (8bit):	6.124402884994097
Encrypted:	false
SSDEEP:	48:jzflW42KJQmfnhwl1zgoAZGMqNM5YQDKfe7lubETc6ddsj:P9W41CD0EGbQFubEVWj
MD5:	584C90BBD4586F1DF721CA80E6C0E680
SHA1:	C604B8B7C35534839A4D54ADD09BAD5274DEBE81
SHA-256:	FF7F4F863C0B1FF17B853847A55480DC1C4780E6641961840FA8D1C163D3CE6C
SHA-512:	2D62CD893288A5B9F61B1C2DC448AD3C4E370FCA28DAE05134E44332805015489CFB08A33E5AFDA5A858C5F69E6DC38FFAD6D168D7AC18B71ED104F0FB96CI 84
Malicious:	false

C:\jar\carLambo\FLUCgYjjYukBnLOPJmMXa.class	
Preview:	.....1....S..T..U..V..W..X..n..o..q..u..v.....x..y..z.....@....?....?....<....C....K....;....C....:....F....G....>....L....N....=....B....D....E....H....J....M....O....P....R....:....A....I....Q..p.^..p.c..p.d..p.l..p.m..t.h..t.s..w.i..{._..|.^..}.e..~.f....Z....[....g....b....Y....]....k....j....\....`....a....]....].....hiW(t:p&u-'.h<i-....C..@#?f<k='t'.b>*.e#b*siP i-h>tgT,d<us0).u,c,i=n(k:).f:t>h;c.f<k=.C...(....()I...()Ljava/io/InputStream;...()Ljava/io/OutputStream;...()Ljava/lang/Process;...()Ljava/lang/String;...()V...(I)C...(I)Ljava/lang/String;...(II)Ljava/lang/String;...(ILjava/lang/String;)Ljava/lang/StringBuilder;...(Ljava/io/InputStream;)V...(Ljava/io/Reader;)V...(Ljava/lang/CharSequence;)Z...(Ljava/lang/Object;)Z...(Ljava/lang/String;)I..&(Ljava/lang/String;)Ljava/lang/String;..-(Ljava/lang/String;)Ljava/lang/StringBuilder;..'(Ljava/lang/String;)[Ljava/lang/String;...(Z)Ljava/lang/ProcessBuilder;...([C)V...([Ljava/lang/Str

C:\jar\carLambo\FNfNjvjZirJsYBDQvbyXp.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	2073
Entropy (8bit):	5.9174646600433265
Encrypted:	false
SSDEEP:	48:j2OnZNtcPcK/mPyxPqNio9f/zWNaP+8t4IBaR7qe0:j2clckKOPYqv9t4IBo7qe0
MD5:	65F52523E6E9ADAEB24F2FFDCE0F6C00
SHA1:	A3E07B3B55978E5601EF8D01D3110334D50FE893
SHA-256:	475CBAC5F8FAEE4E2FDB75AE1FA1A4FB2AB4632E311E9E3DC9B8D072FA14B9C7
SHA-512:	C92E055CF5C2988545A6E9A597F1264BA0545302EBB955B251884DC9F5DB13952E71C2EA92443C05EF4DD855D32A39F97DC7E003C94F60F63995B6E7F483206E
Malicious:	false
Preview:	.....1.....^..b..c.....f..g..p..q..r..s..t..u..v..w..x..y..z....5....5....6....0..../....3....9....B....G....7....8....<....@....D....E....F....H..../....C....:....>....A....;....?....1....4....2....=..].J..].S..].X..].Z..].[..].\..`..P..`.T..d.N..e.K..h.M..i.Y..j.V..k.W..l.K..m.Q..m.R..n.I..o.O..{.I..|.X..}.W..~.N....I....L....W...()I...()V...()[B...()[C...(I)C...(I)Ljava/nio/ByteBuffer;..B(ILjava/security/Key;Ljava/security/spec/AlgorithmParameterSpec;)V..&(Ljava/lang/String;)Ljava/lang/String;..)(Ljava/lang/String;)Ljavax/crypto/Cipher;..3(Ljava/lang/String;)Ljavax/crypto/SecretKeyFactory;...(Ljava/lang/String;)V...(Ljava/lang/String;[B)Ljavax/crypto/SecretKey;...(Ljava/lang/String;[B)[B..6(Ljava/security/spec/KeySpec;)Ljavax/crypto/SecretKey;...([B)Ljava/nio/ByteBuffer;...([B)V...([B)[B...([BLjava/lang/String;)V...([C)V...([C[BII)V...<init>...=U&S+%:~..%z.t>_,&...Code...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG..SY.y.rMd.m.7.dM~.t.e.r.cC7 v.rMd.e.7...cMc.rM~.t.z.y.7.v.vM~.

C:\jar\carLambo\FirstRun.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	4242
Entropy (8bit):	6.107573787336715
Encrypted:	false
SSDEEP:	48:GDPxIEz+SLIFln3VoAwEVfKpJHVdFgPUT65Da84n0oqj/kTEeCY41tDNrbHClSk:ayanLlufOzgPKVHqot1SxrrDk
MD5:	FBA0657627C0F411F5873A5B23927FB2
SHA1:	8F8C0A5A8A96E110AC0B3AE682300590C874A2B2
SHA-256:	10ED85062C29848D11A0F297193E931C9FEB84099F4045FA5B7C6D4A76CDC277
SHA-512:	F4982C0DBD08B9ADDFBAE01C603A24F83E67B25B33E20B2EFB2537F25F9DDBE3E122EB5C0A96B1F96FB6C35A305B8EBFE70525975483E4A1C11A617CC73E0447
Malicious:	false
Preview:	.....1.....e....n....u.....o....t....d....u....v....\.....n....u.....$.....b....f....r....s....k....`....k....k....h.....`....f....l....r....a....i....q....k....j....m....a....g....p....c....a....z....}....~..... ....!.y..!....".x..#.`..#.w..#....#....$.{..$....$....%..... .....8.9B#.&.....K.qx+.K.qx)x+.K.qx){....o tiW.' tii&sit<w9h;s,cg...!s=w:)9u&s&d&k:...%n+...()Ljava/lang/Runtime;...()Ljava/lang/String;...()V...()Z...()[Ljava/lang/String;...(I)V...(ILjava/lang/String;)Ljava/lang/StringBuilder;..#(LcarLambo/HZFTeYcSoingkrwfACxsS;)V..#(LcarLambo/eWXALjSUSDRBlUrdVjYaX;)V..6(LcarLambo/eWXALjSUSDRBlUrdVjYaX;[Ljava/lang/String;)V..)(

C:\jar\carLambo\GDI32.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	254
Entropy (8bit):	5.154915202643433
Encrypted:	false
SSDEEP:	6:/GbUwCvWpsnIUwCvWpYIUwCvWOMh5358UwCmbRPYklKrl:/GAwCvWYwCvWOwCvWz95rwCgR2rl
MD5:	D751B938C1F33787EFCF737E4F7F1F76
SHA1:	F2429206AB8AA53CF704170DE324A931E186DC62
SHA-256:	06B611DD1DA1055F66A2B13097118AF7302BAEAE0B16F60CF063436D1FD0E752
SHA-512:	94E912566A304630BD6710A475734731E20E4043A6B655572CFF6E6D205F13932264E6D20D3886172E0B04F3FDD8EC36AD844088014F9E9D0DF7B30F8A4A2B9B
Malicious:	false
Preview:	.....1.....(Lcom/sun/jna/platform/win32/WinDef$HDC;IIIILcom/sun/jna/platform/win32/WinDef$HDC;IILcom/sun/jna/platform/win32/WinDef$DWORD;)Z...BitBlt...carLambo/GDI32.. com/sun/jna/platform/win32/GDI32...java/lang/Object.....

C:\jar\carLambo\HBrowserNativeApis.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)

C:\jar\carLambo\HBrowserNativeApis.class	
Category:	dropped
Size (bytes):	5499
Entropy (8bit):	5.713848727511768
Encrypted:	false
SSDEEP:	96:U8vtR4rh4iTH0uvp9CJFg4g4WfeI9s1RMHadVKa+:U8z4JTHnPn+WfeI9s7M2Kf
MD5:	65AF2D09480E4A1682C8884FF0CA18B2
SHA1:	D3C3E26D5AB7B423414D4E0A7A5CA076C46CA738
SHA-256:	75EA19972F9B877A601CBD0817CEA73DCC64602B0DA3331A94E1755C22D11CCB
SHA-512:	3EEC6CAF3CC5136A5BEEF720D768CFBB5383741CD55F11A855066858C2BA2766E556707AF764923CDE8D97845982286D90454686B371D689C181E88050A05236
Malicious:	false
Preview:	.....1.....F....G....L....;....K....5....W....T....5....6....R....V....S....X....7....C....E....U....8....9....:....<....=....B....M....>....?....@....A....D....H....I....J ....N....O....P....Q....[....~....b....a...._....d.....`....u....w....|....q....h....c....h....q....t.....l....n....m.....f....k....j....p....i....^....{....Z....\....Y....x....}...()I...()Ljava/lang/String;... ()V...(BBII)V...(BI)V...(I)C..P(Lcom/sun/jna/platform/win32/WinDef$HDC;)Lcom/sun/jna/platform/win32/WinDef$HDC;..*(Lcom/sun/jna/platform/win32/WinDef$HDC;)Z.. V(Lcom/sun/jna/platform/win32/WinDef$HDC;II)Lcom/sun/jna/platform/win32/WinDef$HBITMAP;...(Lcom/sun/jna/platform/win32/WinDef$HDC;IIIILcom/sun/jna/pla tform/win32/WinDef$HDC;IILcom/sun/jna/platform/win32/WinDef$DWORD;)Z...(Lcom/sun/jna/platform/win32/WinDef$HDC;Lcom/sun/jna/platform/win32/WinDef$HBIT MAP;IILcom/sun/jna/Pointer;Lcom/sun/jna/platform/win32/WinGDI$BITMAPINFO;I)I...(Lcom/sun/j

C:\jar\carLambo\HZFTeYcSoingkrwfACxsS.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	306
Entropy (8bit):	5.4571865680467235
Encrypted:	false
SSDEEP:	6:xbyCzGzsW4y1rHOmIz1hjXMOH5h3VYsQRP53zXMjOv0lm+lgmonQX:vGzYy1ruJphrMOj3VYsQRF7Mw0da7QX
MD5:	2A85029DE92E0DB3E9C484B8881F86D6
SHA1:	F3237ABB9701EF6DCEA73B17E11E3D795D7570E8
SHA-256:	80608C549DA03FE9AB792ED1BFF638936EC2007B695EC0E3FBF0A82FA7DE17C2
SHA-512:	C696F9AD452E6563CF1F934B25922CA2C84D7CC0A30127314B4556B0777A981CBB3411816B370F01DBDA24996A5B96C02CA7247B4026D1113B6B9630BE8D0371
Malicious:	false
Preview:	.....1.....()V...<init>...Code.. LcarLambo/xdIozHlUXHmwNaqNNEWok;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...[Ljava/lang/String;...c arLambo/HZFTeYcSoingkrwfACxsS...java/lang/Object...java/lang/String.0.....*Z.....

C:\jar\carLambo\lWRkRwQylUNIljRjtAkaC.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	9047
Entropy (8bit):	6.300527834318984
Encrypted:	false
SSDEEP:	192:MS9TwLwKIl1vJuAwrWCIDXlootD4nwzcMn7RxJnwzjI:MNsTlLDwrHID1ooLcONx4jI
MD5:	EEB8C296B86FACC20230E12A9B0BBE76
SHA1:	324C618E4BD9EAAAE3E47CF5035E564D8FAAF1C9
SHA-256:	271D815311F01B8D083785B3FCEE978CFCD681E993D54D676593ED0C0F5E1A5D
SHA-512:	A2EA9011FEA7ED1E3331B2F12098DA30B5B44CA9E67918E2DBC4982601CC304AC887E035B37715B8CBF1EB4831DB943BD5747708D4A280AEEC4ED50A847C71 8
Malicious:	false
Preview:	.....1..... .I..".#..$..%..&..Q..R..S..T..W..X..[..\..]..^..a..f..g..h..i..j..k..l..r..t..y.....z..{..|..}..~..... .....H...6....6....6....6....6....;....;....;....;....;....@....@....D....D....F....W....4....5....6....6....6....6....6....6....6....6....6....6....6....6....6....6....6....7....9....:....:....:.... <....=....>....?....@....@....@....@....@....A....A....B....B....B....C....D....E....E....E....F....F....F....F....G....G....G....H....H....H....J....K....K....L....M....M....N....O....O....O....O....O.... O....O....O....O....O....P....P....P....P....Q....Q....R....R....R....R....S....S....T....X....X....8....U....U....V....V....V....V./.V.2..V.7..V.8..V.<..V.@..V.E..V.G..V.O..Z.E..Z.d..`.,.. `._..`.d..m.e..o.,..o....o./..o.0..o.4..o.9..o.:..o.B..o.E..o.H..o.I..o.K..o.P..o._..o.b..o.d..p.,..p.E..p.F..p.J..p.c..

C:\jar\carLambo\lkqnNUVNYHrOTFlrdiXDE.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	584
Entropy (8bit):	5.724162230338508
Encrypted:	false
SSDEEP:	12:u4l77KxxEcTy1nJP5mIphYdqIWRIIeyX/aJ4d/:u4B+PTy1nJP8ehYdqxIeyvYE/
MD5:	C1A03E27DF3E4E2DC8F558ACB03EE57C
SHA1:	6595FD91FAD7EEB7431B349EE59BF2C41696DDFA
SHA-256:	2AC787BCEE63B894244EB68314CC96785D9BFAEE9640BA0A8DFDA6288766CA01
SHA-512:	34E0F3E110898E957772931C8AF8C15A5FBA0C2028C07A46D3408902FB2F58F8A5619965F12249B49A7629D4933E9B86499F973CBB5DCCF5C354F06319B8724F

C:\jar\carLambo\IkqnNUVNYHrOTFlrdiXDE.class	
Malicious:	false
Preview:	.....1.....()V..T(LcarLambo/IWRkRwQylUNIljRjtAkaC;Ljava/net/Socket;LcarLambo/InQtwvxSwGlKCGaPBlkoE;)V...<init>...Code..LcarLambo/IWRkRwQylUNIljRjtAkaC;.. LcarLambo/InQtwvxSwGlKCGaPBlkoE;...Ljava/net/Socket;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...carLambo/IWRkRwQylUNIljRjtAkaC...carLambo/IkqnNUVNYHrOTFlrdiXDE...java/lang/Object...java/lang/Runnable...run...vAJiRrxrPqrmdaYHqifDe.0.....*Y..._...*..... .....-*Z[,*+.....

C:\jar\carLambo\InQtwvxSwGlKCGaPBlkoE.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	120
Entropy (8bit):	5.1309197086340905
Encrypted:	false
SSDEEP:	3:Dbll52NVHTf8HmPQ+phHKHUtAKsQCK8P5GxzmlllIn:xobz3hqHssRP5ltl
MD5:	592705A100A5A0687C429157389BB6CA
SHA1:	F22567F4A18A47813F3A52FE2195AA30C68BA6A5
SHA-256:	D411A4598596487B4F3AD05A657F5760CD65E169616BEA1DA6D2C275C08C3964
SHA-512:	D32FF44D904FDD3F915002DEFF82045C49BB7778E62E781C33F3B2665716DCDC047DC991B50FD144097C4557AF4E2E5074D726B87204A0C147CABD360D925FF
Malicious:	false
Preview:	.....1.....()V...WAjaJbPBkhpSMiTfTlSfV...carLambo/InQtwvxSwGlKCGaPBlkoE...java/lang/Object.....

C:\jar\carLambo\JBOWUuMcvCkhdglJnhRMv.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	593
Entropy (8bit):	5.543833249002837
Encrypted:	false
SSDEEP:	12:S+MOagMBMcGsMkhy18y4uuERtB3RF7MsqMXa9Ali//L5fipI:S1MGy18yyEdz5E3L5MI
MD5:	2AB2C164B458AB0DB94599B621B8160C
SHA1:	D0FA7FE28391561A441C0CB973EF28E27D358FBA
SHA-256:	740002F5DAE72670BD3DD8B77C3C08415C7F18BC4CAB507181D1BA9DF5DC0112
SHA-512:	2584ED1A2B926CDCCCC1C763542CAB8BE6EB146C61C7E9B01712FDAF8B70EBA7FFA6E96CEA50D9D60367989AEC0D39B1B6B59DF597E8F91ACCDB9F92DF2A BF4A
Malicious:	false
Preview:	.....1.(.. .."..#..$..%.....!....&....'.....()Ljava/lang/String;...()V...(Ljava/io/InputStream;)V..-(Ljava/lang/String;)Ljava/lang/StringBuilder;...([BII)I...([BII)V...<init>...Code...Ljava/io/InputStream;...WAjaJbPBkhpSMiTfTlSfV...append...carLambo/JBOWUuMcvCkhdglJnhRMv...close...java/io/InputStream...java/lang/Object...java/lang/String...java/lang/StringBuilder...read...toString.1.....+*Z.....O.....C.....L...Y...M*....+_.....Y>....,*.....,...Y+.....W*.....

C:\jar\carLambo\KUmqyODGGRUyuSPgAiEHR.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	1435
Entropy (8bit):	5.887739513978212
Encrypted:	false
SSDEEP:	24:a61Z47G7WnOndZhsEjfotLBemQuljIRGmUTGvz5TQTG043S87R7G6JrEM:a61ZMRGfUJ6tUTUz5TQTXXCTVv
MD5:	160EB6EA2146B8298F2DD56F82A20467
SHA1:	C486ED777860189F54B46C98917E45AE6DDCD45A
SHA-256:	28DF8CD88DFB78449C670E8762245E8806820A1A2B8323A741F7B7FB64412934
SHA-512:	C46F4E65BAFA6CB547AA386F030AB6DFAC7186930C6FD6B6BF1F639FF64FD6BD3F3FEBC8445DA0FB7FB4087C7021A45C3DEA29C021412F5015155624046CA03 9
Malicious:	false
Preview:	.....1.\..>..@..I..J..K..L..M..N..S..T..U..V..W..X....'....&....(....#....*....$....%....%....0....!....+..../....!....)....-.....".....,..=.3..=.;..B.A..F.8..F.9..F.C..F.D..G.E..H.:...O.E..P.4..Q.1..R.6..Y.2..Z.5..[.<...()Ljava/io/OutputStream;...()Ljava/lang/String;...()V...()[B...(I)Ljava/lang/String;...(ILjava/lang/String;)Ljava/lang/StringBuilder;..#(LcarLambo/RhcfPXNPybLnSaSYqyEXw;)V..T(LcarLambo/RhcfPXNPybLnSaSYqyEXw;Ljava/net/Socket;LcarLambo/InQtwvxSwGlKCGaPBlkoE;)V..&(Ljava/lang/String;)Ljava/lang/String;..-(Ljava/lang/String;)Ljava/lang/StringBuilder;...(Ljava/lang/String;I)V...([B)V...<init>...?G.x.-...Code...FfFf...I...IkqnNUVNYHrOTFlrdiXDE.. LcarLambo/InQtwvxSwGlKCGaPBlkoE;.. LcarLambo/RhcfPXNPybLnSaSYqyEXw;...Ljava/lang/String;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...append...carLambo/InQtwvxSwGlKCGaPBlkoE...carLambo/KUmqyODGGRUyuSPgAiEHR...carLambo/RhcfPXNPybLnSaSYqyEXw...carLambo/YYCouWlWxqsvPFMgyBqwW...carLambo/aNhPdlHWbWcyZlRBjRTvT...carLambo/ifmTFpwQLw

C:\jar\carLambo\Kernel32.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped

C:\jar\carLambo\Kernel32.class	
Size (bytes):	240
Entropy (8bit):	5.29101145091102
Encrypted:	false
SSDEEP:	6:5iUwCvUB2JjGaS+Xz8XfpEf2UwCjvRPYklQe2:rwCvK2JSaS+Xz8XfE9wCjvRj2
MD5:	EDFFC21231185918905BF1A2B4D87984
SHA1:	0D85CAD56A24CFD129A04658F57B9BE10AF0B37D
SHA-256:	42C478F9F3334034C5C44A0CDE4B692600B503A79889DF5FBCFC1E7D0991F3F0
SHA-512:	E20309A2EC0B6E2D7E0BB28843620FA682E3DFE233A738C8804B112A367FA11048A2F2974D74DE9A9889CFCE7F97A8343A99BF7CE0830FE328B58F45052FAEC(
Malicious:	false
Preview:	.....1.....,(Lcom/sun/jna/platform/win32/WinNT$HANDLE;)Z...Wow64DisableWow64FsRedirection...Wow64RevertWow64FsRedirection...carLambo/Kernel32...java/lang/Object.....

C:\jar\carLambo\LMjLyRQVjrbfIpBrwheBI.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	1312
Entropy (8bit):	5.853196703713414
Encrypted:	false
SSDEEP:	24:jG6u1AcyKPWny1kJPhyvE0kdqjfwyzmQulwmUTGyJz5TQTGEajparn4ca:jXuKKQ7JJyPiFydmUTTz5TQTGbiza
MD5:	442564350D89ED77D7B6BDE0559BDAA2
SHA1:	AC53B7B4FD70C7F171939B0B641C944F82ECAB5E
SHA-256:	BE952FF082009748AB8760292B70E793ABFD215F840D2747D1457A6426B088C3
SHA-512:	526881B3A590BDCE22C5B83BCF4D776DDBD844DB7BE66D91F83A2D1D35326B988B8D4F6040DB472EBAFAC2C709452A59BE97EEBCAEA4210B623A88DD3A6FD 61D
Malicious:	false
Preview:	.....1.U..@..K..B..C..D..E..F..G..L..M..N..O..P..Q....%....$....I....'....#....".....#....,.....(....+.....&....*.... ....)..8./..8.6..;:..?.3..?.4..?.<..?.=..A.5..H.>..I.0..J.-..R....S.1..T.7...()Lja va/io/OutputStream;...()Ljava/lang/String;...()V...()[B...(I)Ljava/lang/String;..#(LcarLambo/IWRkRwQylUNIljRjtAkaC;)V..T(LcarLambo/IWRkRwQylUNIljRjtAkaC;Ljava/n et/Socket;LcarLambo/InQtwvxSwGlKCGaPBlkoE;)V..&(Ljava/lang/String;)Ljava/lang/String;..-(Ljava/lang/String;)Ljava/lang/StringBuilder;...(Ljava/lang/String;I)V...([B)V...< init>...Code...I...lkqnNUVNYHrOTFlrdiXDE.. LcarLambo/IWRkRwQylUNIljRjtAkaC;.. LcarLambo/InQtwvxSwGlKCGaPBlkoE;...Ljava/lang/String;...WAjaJbPBkhpSMiTf TlSfV...`.`....append...carLambo/FLUCgYjjYukBnLOPJmMXa...carLambo/IWRkRwQylUNIljRjtAkaC...carLambo/InQtwvxSwGlKCGaPBlkoE...carLambo/LMjLyRQV jrbfIpBrwheBI...carLambo/YYCouWIWxqsvPFMgyBqwW...carLambo/aNhPdlHWbWcyZlRBjRTvT...gMLqgzFILKCRhknogvWcQ...getBytes...getOutputStream...ihej. iny....java/io/OutputStream...

C:\jar\carLambo\LPFdzbdgUbctDqujAWZYI.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	3260
Entropy (8bit):	6.270455022132613
Encrypted:	false
SSDEEP:	48:kFvoplo6X1/l6KJU4EnvqTz5D6emPzF33QAJGmWRhadkb681:KvS9dH8nSFbMzFwAJuckb60
MD5:	E7DE9CA9C138CB314D2098CD610AC448
SHA1:	E9929571C793916290468670CE5C28B74C566026
SHA-256:	FD865C23201072C36F03876A78DDB43C346A8C264EBF200CDDFD51DDA8743B9C
SHA-512:	BE8D5B4572220527284605CDB269D0D4948C993150FA013E2C428A5B90806338DC864589025F2B9F16BF4703547955D200EB06E1022CD1A40C2895C88D20478A
Malicious:	false
Preview:	.....1....._..`.a..b..c..d.....G....D....E....F....G....B....N....O....R....T....U....A....Y....V....W....@....C....L....M....P....S....Z....[....\....]... .@....I....J....Q....^....H....K....X....h....s....z.....g....p....r....x....n....m....y....j....t....v....g....g....w....q....i....e....f....k....w....|....~....}....u....{....l....o....g.....-(.$.%.80..(.>.?B9.(\ .....$.*..0....#._...8.<.9.....$L;.8.<.9.k.$.%....()I...()J...()Ljava/lang/String;...()V...()Z...()[B...()[Ljava/io/File;...(I)Ljava/lang/String;...(I)Ljava/lang/StringBuilder;...(I)Ljava /nio/ByteBuffer;...(II)Ljava/lang/String;..'(ILjava/lang/String;)Ljava/lang/String;...(ILjava/lang/String;)Ljava/lang/StringBuilder;..:(ILjava/lang/String;Ljava/lang/String;I)Ljava /lang/String;...(Ljava/io/File;)V...(Ljava/lang/CharSequence;)Z..D(Ljava/lang/CharSequence;Ljava/lang/CharSequence;)Ljava/lang/String;...(Ljava/lang/Object;)Z...(Ljava/la ng/String;

C:\jar\carLambo\MwXUjyQKvUClJaqfYeEXR.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	6097
Entropy (8bit):	6.298772494935256
Encrypted:	false
SSDEEP:	96:l47i3xDc0eAFFONbHqzaHkzGFlEveYoRvkqChhSOreyVu6fVLsqZiA78LQG9:lh3eoS9qNyFeWYoRvkD4Oqe5RALH9
MD5:	893F01FF96A2D1B9DF3117065C801E0E
SHA1:	2F17231E4E257E6B7F34982BD4C45342F7DAF1E0
SHA-256:	EB14F25E094DDA700749875585078C27CD7B562D3DEB2AE3E30EF63E03158275
SHA-512:	8BCE3905BD81A5006399C9F09331F8FC35B68EE431245C1A1943BF349352B6106CCCFAB4F0C6824C7FA308DE15C084E33A132FAF6BB7C51175A3B261AF88EEF

C:\jar\carLambo\MwXUjyQKvUClJaqfYeEXR.class	
Malicious:	false
Preview:	.....1.T.... .....%..E..J..K..O..P..S.....)..*..+...-...../..0..1..2..3..4..5..6..7..8..9../..../..../....2....2....2....2....7....9....G.....1....1....1....1....1....1....3....4....5....6....8....8....8....9....9....9....9....9....9....9....:....;....=....=....>....?....?....@....B....C....D....D....D....E....E....E....E....E....E....E....E....E....E....F....F....F....F....H....H....0....0..... ....I...."....#....$....&....'....(....:....;....<....=....>....?....@....A....B....C....D....F....G....H....I....I....L....M....N....Q....R.....vMt.z..v.s.7.0.d.7.r.z.y....8.(.1.$..L(.&.%.$L9.>.(.?...../."."?.*.$.....&.e.3....0..&...&.%.'L8.9."...k.8L-.'..2L8.;.$.?./B..*...&.%.'L8.9."...k.8L8.;.$.?./L;.9."..'..2B..

C:\jar\carLambo\NRSgeibhpMRqnMXxHCtkH.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	4760
Entropy (8bit):	6.332554013887655
Encrypted:	false
SSDEEP:	96:r2wdEVidiZd0x8H2P+e1wjMtFlcqc1X3/9ivlRI:r2BsiZF2We1vFIRcVV
MD5:	AB3B59C751B2172C30FD6D89D43B30F1
SHA1:	C1055C8C2ED5E3697B4888D312C740DA11A35556
SHA-256:	34C49FFEABD2217D527C0EE4A8B3C2EF10E8EBBA432ADD68711E2388F81F1235
SHA-512:	CB41BA0DD86DBA05D7965345ED4BB3B2B08C7953C27196DE6DFA2BB518A0B7EE63B31AA00E6E505C4AE17E3A126BFE02E00EEFC311B5824EDE20FAA50FB6A06F
Malicious:	false
Preview:	.....1.....(.....i....l....m....n....k....k....c....j....k....e....s.....g....v....w....y....|....~..... .d.....!.g..!.s..!...."....$....$....%.b..&.h..&.t..&.u..&.z..&.}..&....&....&....&....'.b..'.p..'.q..'.{..'....).f..)....*.g..*....+.x..+....,.o...,r.,.....-(.$.%.80..(.>.?B9.(\.....$.*..0....#._..8.<.9....."$L;.8.<.9.k.$.%....()I...()J...()Ljava/io/InputStream;...()Ljava/lang/String;...()Ljava/net/URLConnection;...()V...()Z...()[B...()[Ljava/io/File;...(I)Ljava/lang/String;...(I)Ljava/lang/StringBuilder;...(I)Ljava/nio/ByteBuffer;...(II)Ljava/lang/String;..'(ILjava/lang/String;)Ljava/lang/String;...(I

C:\jar\carLambo\OfHKSMXcxdCQqFxyzUhpZ.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	377
Entropy (8bit):	5.48294210655134
Encrypted:	false
SSDEEP:	6:HU3lpzsdZuW4y1+Z7z3hsDYhcHh0ZVRPt+Ncl3ul2mlknM5UK/sxl:rZuNy1+Z7Vs8KB0ZVRl9luJkM5f/sj
MD5:	1BA27D09D679DCC08B0941DEEBBE6952
SHA1:	D647D66239C6449304FB3B9E92E1E2C6CE56D97E
SHA-256:	250E26869545649C1A2C39527AAC681617F7E136558F60FF87F729BA0AA68217
SHA-512:	DEF3D89EFA332790E0787D355616C4F4B007ED40541A28D7A303B557D04482FFB17324D21FB5A7B998A707FD65B839E278A71F163961D3C47F14B03FC468EE40
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/WFnpewDUZzidjcKbMnKqG;)V...<init>...Code.. LcarLambo/WFnpewDUZzidjcKbMnKqG;...WAjaJbPBkhpSMiTfTlSfV...carLambo/OfHKSMXcxdCQqFxyzUhpZ...carLambo/WFnpewDUZzidjcKbMnKqG...java/lang/Object...java/lang/Runnable...run.0.....*.....*Y+.....

C:\jar\carLambo\PRecjdEZwdifBquTYRlUl.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	11532
Entropy (8bit):	6.353478535183492
Encrypted:	false
SSDEEP:	192:MAdDYKDjl1YwV09lc8wX5wqq7SFKaWF8Z7Rv7Rgtv8Z7Rv7RJ47Wpf3fTES+WGqV:HYKYwYi8wXlaaWFk7Rv7Rgpk7Rv7Re7Y
MD5:	A182AE2369013B396E2F8E39DBDCE2C1
SHA1:	DA7756626820ABA3AD642A105DD41DF838E71D18
SHA-256:	5DCFA981AC0AF42C2759126AF2744FE37A1FF24440461BAA4C074A14F46A70AC
SHA-512:	A6607DB597AD980937743283DA535E5DD1BE2905F6881BA5726A8B0649368AA094731A13F7ECE04C5231737644A387954C0E8712E64D9B9F96B6408A4E6D0261
Malicious:	false
Preview:	.....1.?.....@.....V..W..X..Y..Z..[..\..]..^.._..`..a..b..c.....8..9..:..;..<..=..>.....?.fffff.@ 333333..3....3....3....3....3....3....3....3....3.!..3.N..5....5....<....<.8..<.?..<.K..>....?....?....?....?....?....?....A.T..A.U..B.4..B.Q..T.:..X....1....2....2....2....2....2....2....2....2....2....2....2....2....2....2....2....2....2....2....2....3....3....3....3....3....3....3....3....3. ..3.&..3.L..3.M..4....5.7..6....7....8....9....9.,..:....;....<....=....>....@....@.3..A....B....C.(..C.2..D....D.@..E....E.H..F....F.$..H.>..I.%..I.S..J.=..K./..L.;..M....M....N.<..P....Q....Q.C..R....R."..R.#..R.'..R.5..R.B..R.E..R.F..R.G..R.I..R.O..R.P..S....S....S....S.6..S.J..U....U.A..U.D..V.)..W....W....W.*..W.+..W.0..W.1..Y.-..Y.9..Z.R....o....y....z....}.....

C:\jar\carLambo\QdhsHELHRynENxdBimgsC.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)

C:\jar\carLambo\QdhsHELHRynENxdBimgsC.class	
Category:	dropped
Size (bytes):	644
Entropy (8bit):	5.87293372717388
Encrypted:	false
SSDEEP:	12:XNTFTlYdzBoiMBMOXMJy11LJbVdqct0H2sXLboR7zRlJZVhiH/sPt:9ZCBTy1pJJdqypswRXzLQEPt
MD5:	56851E9B871F276736E24640345FED4B
SHA1:	4E533688CAC9A13B9C7CC4FD66208D2406C3A406
SHA-256:	BDC2DDBE9E4E2334256ECB49701B06847D6DD0BA21E34AD812AFE42DBFAB826B
SHA-512:	88E035C055A3AA6B423F6C88579DAAEFEC98C5A8073D62B906A27220F5A475CA52C14CF26D260434BDDB3F331FC7CBE415E93EACF9279E47C856F8ED5677EB3
Malicious:	false
Preview:	.....1.!.....()V..#(LcarLambo/IWRkRwQylUNlljRjtAkaC;)V..&(Ljava/lang/String;)Ljava/lang/String;...(Ljava/lang/String;)V...<init>...Code...IkqnNUVNYHrOTFlrdiXDE.. LcarLambo/IWRkRwQylUNlljRjtAkaC;...WAjaJbPBkhpSMiTfTlSfV...carLambo/IWRkRwQylUNlljRjtAkaC...carLambo/QdhsHELHRynENxdBimgsC...carLambo/WKTBLojTnJupFuAfwhtUj..lg|JyVkW.VkV}LaK.FbJ`L`B.VzD|QkA .ZMgV.RgIb.zDe@.D.IaKi.zLc@.Qa.mJcUb@z@ /WJ{.yLbI.Gk.`JzLhLkA.Rf@`.mJcUb@z@ ...java/lang/Object...java/lang/Runnable...run.0..... .....*.....*Y+.....

C:\jar\carLambo\RhcfPXNPybLnSaSYqyEXw.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	5602
Entropy (8bit):	6.154826420979786
Encrypted:	false
SSDEEP:	96:/1l7aHFlCRkIJKX8D8B1rbs4p6eb4dB6eb4dz8e+:tVlICmIJ3D8z3s/eIAeIzL+
MD5:	59F66C51DD94A8BD0D0C8A5600C45DC9
SHA1:	2C7DCC9118776D54BD0FA923F6C529B53F3F0F59
SHA-256:	125C10231439B5550DB28531011F8C958E5E0384C7E7930398F526AD5D10B42F
SHA-512:	758E5C6BB2739D5B5DB9A1846F104B2DF511978C08D085F1DA19AFD3FCDDC26357BEE81C276E7D525F7BCE32BD1DF8C958E4DC1CEEA216032F6760D97AA3A6A
Malicious:	false
Preview:	.....1.....n....q.....i....x..,j....l....d....o....p.....l....c....m....e..!.s..!....".w.."....."....#.|..$.c..%....&....'.c..(.h..(.t..(.u..(.v..(.y..(.~..(....(....(....(....(....(....(....).c..).r..)....)....*.f..*....+.g..+.s..+.z..+.}..-.{..-.....k.....x.c.y.:.r.p.....()Ljava/io/InputStream;...()Ljava/io/OutputStream;...()Ljava/lang/String;...()V...()[B...(I)Ljava/lang/String;...(II)Ljava/lang/String;...(ILjava/lang/String;)Ljava/lang/StringBuilder;..#(LcarLambo/RhcfPXNPybLnSaSYqyEXw;)V..T(LcarLambo/RhcfPXNPybLnSaSYqyEXw;Ljava/net/Socket;LcarLambo/InQtwvxSwGlKCGaPBlkoE;)V..)(Ljava/io/I

C:\jar\carLambo\RyDWjwZKMcstuZbiMGYqA.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	3187
Entropy (8bit):	5.654330174598673
Encrypted:	false
SSDEEP:	48:tguLrvrrqZ23WoaZOqS3/JWMZfeW/6DHlJtO2Ie5SM3iv:gsnhDJWMb6DH8JQSM3iv
MD5:	32785C3C4C57DAE16650228A62FED0F8
SHA1:	C9A2E595EF68B5E35FC574FEEC53D42E9C608A9E
SHA-256:	335118B170A501D99EC471FF64F5484FC6D63E6603EF3B029F321DC2AB0AE9FF
SHA-512:	AC4D0220E13C246903724C678B9A65BEF63E842B72B33E180A14B271FBFBBBC518DC891829CF3F71CBA969E12C04C5C9F2D0659C0BCC552E7C416C3F6F8AC37
Malicious:	false
Preview:	.....1.w..<..E..F..G..H..I..J..K..L..M..N..O..P..Q..R..S..V..W..Z..[..\..]..^..._..`..a..b..c..d..e..f..g..h..i..j..k..l..q..t..u..#.6..".4..$.4..%.5..&.;..'.3..(.7..(.8..(.9..(.:..T.?..X.B..X.C..X.Y..m.=..n.>..o.@..p.@..v.A....b:d....()C...()I...()V...()Z...(C)Ljava/lang/String;..&(Ljava/lang/String;)Ljava/lang/String;...(Ljava/lang/String;)V..0(Llc/kra/system/keyboard/event/GlobalKeyEvent;)V...6S"@#J...6T.e.: J...6T.e.:"J...6T.e.:$J...6T.e.:&J...6T.e.:(J...6T.e.:*J...6T.e.:,J...6T.e.:.J...6T.e.:4J...6T.e.:8J...6T.e.::J...6T.e.:<J...6T.e.:>J...6U.t.J...<init>...Code...L(Y9R?J...L?^*_9J...WAjaJbPBkhpSMiTfTlSfV...Z...\.B.S....\.s;kdA....\.s;kdC....\.s;kdE....\.s;kdI....\.s;kdK....\.s;kdM....\.s;kdO....\.s;kdQ....\.s;kdS....\.s;kdU....\.s;kdW....\.s;kd]....\.s;kd_....\.W....carLambo/HBrowserNativeApis...carLambo/RyDWjwZKMcstuZbiMGYqA...carLambo/YYCouWIWxqsvPFMgyBqwW...carLambo/ppqPYkdOMPGLhnnFjoRgt...getKeyChar...getVirtualKeyCode...isControlPressed...isShiftPressed...java/lang/String..

C:\jar\carLambo\SpPnnJyNVMiKWFUPPBgAJ.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	577
Entropy (8bit):	5.7520425821807795
Encrypted:	false
SSDEEP:	12:KMugIgn0a0oiMBMOXMJy1nJbph3Eccti0y5dqwV9clSRl0V0diH/sPt:JTn0a0Ty1nJ9hn0kdqw3FzqkQEPt
MD5:	4A5D3D9C446CDD432DB497628B4051F7

C:\jar\carLambo\SpPnnJyNVMiKWFUPPBgAJ.class	
SHA1:	A533559A820551840D08C439CD7A38DE8A86BED6
SHA-256:	ABFF84FF1F8A2B318871A60039F099B9B03994CF36480CC2B59B503E88B7EDBC
SHA-512:	8F9E6BB73E029F0E860655AE8ED8D3073D4E61651C51627112F4197EE38EB1A4612FBF09D2EE1DDF3A65FCD5024756FBA908B16BE12706447F786FD740C8A02F
Malicious:	false
Preview:	.....1."..... .....()V..#(LcarLambo/IWRkRwQylUNIljRjtAkaC;)V..&(Ljava/lang/String;)Ljava/lang/String;...(Ljava/lang/String;)V...<init>...Code.. LcarLambo/IWRkRwQylUNIljRjtAkaC;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...WLVpZVKPTwBamUZoZCNyH...carLambo/FLUCgYjj YukBnLOPJmMXa...carLambo/IWRkRwQylUNIljRjtAkaC...carLambo/SpPnnJyNVMiKWFUPPBgAJ...hTHNH[MS[SO].rs~q...java/lang/Object...java/lang/Runnable...run.0... .....!.....*.....*Y+.....

C:\jar\carLambo\User32.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	320
Entropy (8bit):	5.376457698926428
Encrypted:	false
SSDEEP:	6:7BCLTKbUwCvWqdUwCvWiUwCvWqtGi1BoUwCFRPfAKmkl39lt:7BoT/wCvWfwCvWhwCvW6p1xwCFRHlTX
MD5:	74E3267A0A8A18C211B6A36A40D8D9C9
SHA1:	EA99375E085467B362EC1E3A2DA3854241BC37D5
SHA-256:	10D41BB5B9F1036663687723237F595050A98433AA129544490AF45E29150A70
SHA-512:	6F387D069E88AF484A007E60E9C5B85F4248C346C09BFBBB24B2662B0DD7C3972CAAF18753D658CA711914A9BECBFE5537DE3F71F1CDC58105936CE950A0CB6
Malicious:	false
Preview:	.....1.....(BBII)V..Q(Lcom/sun/jna/platform/win32/WinDef$HWND;)Lcom/sun/jna/platform/win32/WinDef$HDC;...(Lcom/sun/jna/platform/win32/WinDef$HWND;[BI)I...GetWindowDC...GetWindowTextA...carLambo/User32..!com/sun/jna/platform/win32/User32...java/lang/Object...keybd_event.....

C:\jar\carLambo\VMnlAvsfupVDCaszPEPjX.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	4649
Entropy (8bit):	6.246661559540902
Encrypted:	false
SSDEEP:	96:ePMVAL/ONMSW+OmfskSmZHU6wpqhbLVw0wsZk0sss:ePYI+M2OmrnLCqJLVw0wsZkl
MD5:	35CA5C17D175492903D21C14417824F2
SHA1:	BA4C1601B400D460DD5AA867E575EB910C75AC6A
SHA-256:	4004F361C091B3F475987E47CA9625A70912FB968F58CFC039E3826E016F9596
SHA-512:	94C3B8063E7495C55B806786B19ADA2B797554599674C8A26AA98BA1330242CDA6C35F5DD4A5E0C65181F4FBB1C390E00EB3FD68642E0CE5C4731E8FCE60208
Malicious:	false
Preview:	.....1.&.....$..%.....y..+.....v....w....x....z..... .v..!.u.."....#.q..#....#....#....$.p..$....%....&....'....(.n..).r..).t..)....)....)....*.n..*.{..*.|..*....*....+....,....,....,.....1....1....2.~..2....3....3....3....3....4.o..5.s..6....-.}..-....-..../.}../..../..../....0.}..0..... .....!....".....#.....h='/h<i-(*h;u<w=b-....B.....=.R:b;t...!.h<uiH.'a":.in:''h=':r9w&u=b-&i=a..9.F9w.f=f.K&d(k.@&h.k,[.o;h$b.R:b;'.f=f.C,a(r%s.K&` iiC(s(....B.B.Si-iA.H.'%h.n'tr...&tgi(j,...()I...()J...()Ljava/lang/String;...()Ljava/sql/Statement;...()V...()Z...()[B...(C)Ljava/lang/StringBuilder;...(I)Ljava/lan

C:\jar\carLambo\VuLgyZptDPIAaqUhBdkQg.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	1554
Entropy (8bit):	5.939703059837532
Encrypted:	false
SSDEEP:	24:me1VwvM4sVtvs25Ny1GZlwrlZEgQQQcqNM5AtRzb2NYZLbBfclYqZX/RQJ:me18rsVtvs2rvZluXqNM50XbLbBOY0XU
MD5:	E1CDB05EC45F28E834CC6CCDCD74B89A
SHA1:	143A2597A1F3F9495DC78134510D8D5E0D1DF6D3
SHA-256:	6CA1F706AFB84CBE8A8FD52C5742905D52E5D9848D975CF84C6310D1E067ADAC
SHA-512:	F6BD27F4580D9387EB3C52124E294AD6FBEEE3466CF67A36C296BA54C3FBB7D55A368523921AE9DC76406902CCA57A1C8A6D856C3B831E32AB371C23E70FB8C
Malicious:	false
Preview:	.....1.i..9..:..;..I..N..O..^..b..f..Q..R..S..V..W..X..Y..Z..[..\..]....-....,....,....*....2....1....)....(....0....+....3....5..../....4....6....8....(.....7..J.?..J.@..J.A..J.H..M.C..M.L..P.D..T.B..U.<..._.?..`.>..a.G..c.F..d.=..e.E..g.>..h.>.....m...(....()Ljava/io/InputStream;...()Ljava/lang/Process;...()Ljava/lang/String;...()V...(Ljava/io/InputStream;)V...(Ljava/io/Reader;)V...(Ljava/lang/Object;)Z..&(Ljava/lang/String;)Ljava/lang/String;..-(Ljava/lang/String;)Ljava/lang/StringBuilder;...(Ljava/lang/String;)Z..'(Ljava/lang/String;)[Ljava/lang/String;...(Z)Ljava/lang/ProcessBuilder;...([Ljava/lang/String;)V...*...<init>...Code...Ljava/lang/String;...WAjaJbPBkhpSMiTfTlSfV..c`..~.7By.s.-C7By.z.d.v.rW01K.x.c1t.z.%J7.v..M`.y^%2{.p.t.{.~.|Mp.cMa.{.z.d.e.v.y.z.r.7Bq.e..v.-.~.c...`....append...carLambo/VuLgyZptDPIAaqUhBdkQg...carLambo/WKTBLojTnJupFuAfwhtUj...carLambo/YYCouWIWxqsvPFMgyBqwW...equals...getInputStream...java/io/BufferedReader...java/io/IOException...java/io/InputStre

C:\jar\carLambo\WAjaJbPBkhpSMiTfTlSfV.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	377
Entropy (8bit):	5.440703205873086
Encrypted:	false
SSDEEP:	6:HU3lpzsTPjy4y1wSE4z3h0P3h6iRPt+Ncl3ul2mlknM5UK/sxl:NNy1HE4V0p/Rl9luJkM5f/sj
MD5:	53DFD3887CABB44B2F1B799E7E4FE6C9
SHA1:	A565446502726009F297385E851EE24A1E967D0D
SHA-256:	2A8034410F600DD67C8CBCC2D76B919F1AD6C2DFC761A3A320441B98F80623AC
SHA-512:	4270A76E460CA1B3BBDCF809FD1977F1353458490635289B5EF0830EABB65A0663FD2548934F7EB5317646F0D669DCD8763A916BD8A60C3D042D3C8B2BF1E8A9
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/YYCouWIWxqsvPFMgyBqwW;)V...<init>...Code.. LcarLambo/YYCouWIWxqsvPFMgyBqwW;...WAjaJbPBkh pSMiTfTlSfV...carLambo/WAjaJbPBkhpSMiTfTlSfV...carLambo/YYCouWIWxqsvPFMgyBqwW...java/lang/Object...java/lang/Runnable...run.0.....*.. .....*Y+.....

C:\jar\carLambo\WFnpewDUZzidjcKbMnKqG.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	5784
Entropy (8bit):	6.1685736253642665
Encrypted:	false
SSDEEP:	96:YCflVRgpEaD1qNElvI5kxNsTk4qEBUGnYr764z+:YclVRc1nVI5k/q8/6L
MD5:	FCCF5CE6775ADA0E1975038E815472EA
SHA1:	82ADDC90686D8CC880803A4E6205BAD5FF7DF4B6
SHA-256:	60EE7DFE6150C7441F08B8636E6A490C75B6AD7A392CC6E4F0AE0D8369C23DCF
SHA-512:	70667950FA8FF1B6E565648C0E7A4F28AF1B62FB0E3ED472159D153EA7A2B193A97BF62F7043011A624583C30DCBBECFBC0987B5FFF7CECDEB350873819A4E34
Malicious:	false
Preview:	.....1.S.....;..O..P..Q..R.....".#..$..%..&..'..(..)..*..+...-...../..0..1..2..3..4..5..6..7..8..9.....~..... ....!...."....#....#....$.}..%....&....'.}..(....)....)....)....*....*....+....+....+....+....+....+....+....+....+....+....+....+....+....+....+....+....+....,}..,...,...,...,...-....-...../..../..../..../..../..../..../..../....0.}..0... .1....1....1....3....3....4....5....6....2..... ... .!....:....<....=....>....?....@....A....B....C....D....E....F....F....G....H....I....J....L....M....N.....u....B...(....(.(....()I...()Ljava/io/InputStream;...()Ljava/io/OutputStream;...()Ljava/ lang/Process;...()Ljava/lang/Runtime;...()Ljava/lang/String;

C:\jar\carLambo\WKTBLojTnJupFuAfwhtUj.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	8556
Entropy (8bit):	6.289366511263343
Encrypted:	false
SSDEEP:	96:5MtAkMRl8vhNAdO2KDGww1xaAEFS4ES5uwKl8XObJRDRZbJRr8Gl3U+B4dl/Dkxz:ycl98Dlw1n4T5KNjZNN8T+BM8k
MD5:	DAB63D06BA5B929611DBB0942D7E5614
SHA1:	165C980E372367BCEA3E20CCFCF226E150952D55
SHA-256:	B5B9AC764128F8F9E023AA28CD61241A3B86BBAA2ED97E5C03A150FE19B3242B
SHA-512:	F1FD0CCDE362B2C71ECF6CCAC88CEB070F7ECE98B2B2415FB3DA6BF05AE2D37C684145E1579344E5129F4BC834DEC855DB0E1ECB2CF186D135C43FDF56E0D0A
Malicious:	false
Preview:	.....1.....>.....H..I..J..K..M..N..Q..R..Z..[..\..]..a..b..c..g..w..z.....h..i..j..k..l..m..n..o.....?.f fffff..!....!....!....!....)....)....<....!....!....!....!....!....!....!...."....#....#....#....#....#....#....$....%....&....'....(....)....*....*....+....+....,....-....-...../..../..../..../....0....0....1....1....1....1....1.. ..1....2....2....3....4....4....5....6....7....8....8....9....:....:....:....:....:....:....:....:....:....:....:....:....:....:....:....:....:....;....;....;....;....;....=....=....=....>....>....>....?....?....?....A....B....B....C....C....D.. ..D....D....D....@....@....L....L.#..L.%..L.*..L.+..L.1..L.2..L.8..L.=..L.F..L.G..P....P.Y..^....^.&..^.(..^./..^.:..^.=..^.U.._....._.V..d. ..e....e.;..f....p....q.3..r....s.5..t....u....v.-..x.>..y.7.. {....|....}....~.....0....<.....$.....0.....S....9

C:\jar\carLambo\WLVpZVKPTwBamUZoZCNyH.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	401
Entropy (8bit):	5.559373596696094
Encrypted:	false
SSDEEP:	12:UHqpMkNy1HE4phY06Eccti/Rl9luaPkM5f/sj:4qpMkNy1H9hYZ/z95cM5fEj
MD5:	C9799CFA362818622F4A8FA28EE82C9E
SHA1:	0BAF5DA07E269E17941C9435FDAFED8F37AD1688

C:\jar\carLambo\WLVpZVKPTwBamUZoZCNyH.class

SHA-256:	7DE9EE53064DF7D3D9AF877A9090982966A76D666EFF6631310544B1BB4B0121
SHA-512:	330241C6E98050DE3FE130B8B743F70CEDF3034F5776C39B5900E4392608BF65AC83B73170ABCAF158264D2601720C27A1A4A70859B18EA632C2F3CA38FEE170
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/YYCouWIWxqsvPFMgyBqwW;)V...<init>...Code.. LcarLambo/YYCouWIWxqsvPFMgyBqwW;...WAjaJbPBkh pSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...carLambo/WLVpZVKPTwBamUZoZCNyH...carLambo/YYCouWIWxqsvPFMgyBqwW...java/lang/Object...java/lang/Runnabl e...run.0.....*.....*Y+.....

C:\jar\carLambo\WinGDI.class

Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	324
Entropy (8bit):	5.260373383168725
Encrypted:	false
SSDEEP:	6:7eNVjnY+kaGZXy1eUwCvWOMh5nWDA3bUwCvWOMhc8UwCvDRPU3sz+wl85//l:yNVjnvkZy1lwCvWz0DxwCvWzcrwCvDRy
MD5:	7E7159FABF64B2A99614D43805EDD16C
SHA1:	8EEAC5BF0D2DC109B6F48164ED20A6470636E5CA
SHA-256:	D07BAA1E2E821904345458D0F8D4813FC079B73B101419EB2544C952D7C7BCC2
SHA-512:	4CD7CD7DB9FBCC804521641918006FB2100A41139592E1B604B3986CF9AEE82A8BF548A04BBF22B65995AFDFCBB4FDF5E972D02113C2FA41476D9BD93287FA2
Malicious:	false
Preview:	.....1..... .....()V...(J)V...<clinit>...<init>...Code..)Lcom/sun/jna/platform/win32/WinDef$DWORD;...SRCCOPY...carLambo/WinGDI..'com/sun/jna/pl atform/win32/WinDef$DWORD..!com/sun/jna/platform/win32/WinGDI...java/lang/Object.....Y.....

C:\jar\carLambo\WppqWwSRlQJiTLfjgsmCj.class

Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	358
Entropy (8bit):	5.342722847535142
Encrypted:	false
SSDEEP:	6:VGncDX1fJy4y1gfsHk4z3h0V+ySFP7NhCllQRPt+NclJl/lUkxVM92lsDElplll:0ncDThy1vV0VmDPIlQRl9Dl/xVP2ML/
MD5:	D1BD543BA945DCA1BB6FD8BA57AB3476
SHA1:	B9E65AB90703163D8BB7C7D977C1E3B50C3F99F0
SHA-256:	A7A2CB42EAB0713A4A3EACBF02C4CC991055BBE962F14A9C1D0873BDEBE5D874
SHA-512:	AAFD4E85DDEDAF52725C6086BA7BEEBB576D89194F293DE758301D4CDA22C74851C4EF0596B5C51D357289B0131FE86961DBFB322B02EE0CE6CE1BDF9D475 19
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/ppqPYkdOMPGLhnnFjoRgt;)V...<init>...Code.. LcarLambo/ppqPYkdOMPGLhnnFjoRgt;...WAjaJbPBkhpSMiTfTlSf V...carLambo/WppqWwSRlQJiTLfjgsmCj...carLambo/ppqPYkdOMPGLhnnFjoRgt...java/lang/Object...java/lang/Runnable...run.0.....*..... .....

C:\jar\carLambo\YGZckHbbfSSCkmxMSahob.class

Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	1615
Entropy (8bit):	5.711337211802536
Encrypted:	false
SSDEEP:	48:T+DxI0sTKobEWeCcRhkddN8W/z5ku9yqqumCIrt:aDxfJwB8zXaI5
MD5:	36F03EB25195DA759E5863765847CAA8
SHA1:	410FB214F80673FD6A5A105EF4AADA8A1F04AB52
SHA-256:	1ECF2A7A58E8161A5D568EC9B91E648E1DFEA4FF229F4FA5B62CD868A2758F4F
SHA-512:	A1D6EC99228A22EB481EEAC45DB4F38FD218F528E362DED6172960FEA33C0DBEE866EBD291D73BDC6AF0B758E0508C93D8CCB287B4CDD7590E9463841A985 7D
Malicious:	false
Preview:	.....1.e..B..E..T..V..W..X..Y..Z..[..\..]....'....(....*....+....,....)....#....$....%...."...."....&..../....2....3...."....-.....4...."....1....0..D.7..D.9..D.<..D.@..D.A..H.J..I.L..M.K..O.Q..P.J..R.Q.. S.>..U.;..^.5.._.:..`.=...a.8..b.?..c.6...()I...()Ljava/lang/String;...()V...()[C...(B)V...(I)I...(ILjava/lang/String;)Ljava/lang/StringBuilder;..((ILjava/util/Random;Ljava/lang/String;)V..&(Ljava/lang/Object;)Ljava/lang/Object;..-(Ljava/lang/String;)Ljava/lang/StringBuilder;..&(Ljava/util/Locale;)Ljava/lang/String;...(Ljava/util/Random;)V...([C)V...0123456789... <clinit>...<init>...ABCDEFGHIJKLMNOPQRSTUVWXYZ...Code...ConstantValue...FLUCgYjjYukBnLOPJmMXa...IkqnNUVNYHrOTFlrdiXDE...Ljava/lang/String;...Ljava /util/Locale;...Ljava/util/Random;...ROOT...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...WLVpZVKPTwBamUZoZCNyH...[C...anzYKctnLiQPVOOntxF FV...append...carLambo/YGZckHbbfSSCkmxMSahob...insert.."java/lang/IllegalArgumentException...java/lang/Object...java/lang/String...java/lang

C:\jar\carLambo\YYCouWIWxqsvPFMgyBqwW.class

Process:	C:\Windows\System32\7za.exe

C:\jar\carLambo\YYCouWlWxqsvPFMgyBqwW.class	
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	4681
Entropy (8bit):	6.058563993756935
Encrypted:	false
SSDEEP:	96:mhpWmMySbhghiMDqs764MKfMK4JhbblBsX:mhcmMfbhdo3MeM/hnLM
MD5:	DCFBBA41B8A11C3DED8F2538BD9F6AA5
SHA1:	5211BC1744780AD7A5AF564CC5BFBC5C8E8831DA
SHA-256:	7EAA130CDF604CC2E17FAC37EEC61B6208BE21C29DA376D4E073BA08725ED980
SHA-512:	ED4C854526325896A0FFB0C5B64D58BD38FB0D78844A4CFDA34B281127C34B6113AAFEF96A6C59F1BC10A14869B48E62555E39691232A0112A4774D325D980E6
Malicious:	false
Preview:	.....1.&.....%.....z....{....~.....|....m....m....|....}....p.....q.....n..... ..o.....s....l.....y.....u....w.....l.....r.....l..... ...."...."...."....#.t..$.x..%.v..!..... ....l...."....#....$.... $.....()I...()Ljava/io/InputStream;...()Ljava/io/OutputStream;...()Ljava/lang/Process;...()Ljava/lang/String;...()V...()[B...()[C...(I)C...(I)Ljava/nio/ByteBuffer;...(ILjava/lang/String;)Ljava/lang/StringBuilder;..B(ILjava/

C:\jar\carLambo\ZeiFKvzcxODidyLNIuqkn.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	1035
Entropy (8bit):	5.708962130694585
Encrypted:	false
SSDEEP:	12:LqcCYoFbjv4wMOQMBMc7GGeXrMaMPeIMziMBMOPMBMRMJy1Vefa4phrMOZEDeWQj:Llqbjvdswy14auh5ElT/IRHznQQx
MD5:	552E547EF589968B0998E1899E89B901
SHA1:	66D2DE33C6AA8B3E3A70248FCDF18C58A34B285E
SHA-256:	14E854B01D3348A5803BD5F544303B31EA37593F693AB37E278EF3A707AC2F96
SHA-512:	A72B61064B80AFEAA7C36FA3B136BB42C2E69546ACDDEFE4FAE530EA1F15C6AFB127FCF7313D87577E623085C87EC07843624ACCB2C4DB250AA9EFE444DE5 92
Malicious:	false
Preview:	.....1.=.....0..1..2..4..5..6..7..8.....(.!..,.#..,.%..,....-.*../.&..3."..9.+..:'..<. .....<.'.*...qL...()Ljava/lang/String;...()V...(ILjava/lang/String;)Ljava/lang /StringBuilder;..G(LcarLambo/NRSgeibhpMRqnMXxHCtkH;Ljava/lang/String;Ljava/lang/String;)V..6(LcarLambo/NRSgeibhpMRqnMXxHCtkH;[Ljava/lang/String;)V..&(Ljava/lang/String;)Ljava/lang/String;..-(Ljava/lang/String;)Ljava/lang/StringBuilder;...(Ljava/lang/String;)V...<init>...Code.. LcarLambo/NRSgeibhpMRqnMXxHCtkH;...Ljava/i o/PrintStream;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...[Ljava/lang/String;...append...carLambo/NRSgeibhpMRqnMXxHCtkH...carLambo/ZeiFKvzcxODi dyLNIuqkn...carLambo/ifmTFpwQLwUvcmBtqiUxG...insert...java/io/PrintStream...java/lang/Object...java/lang/Runnable...java/lang/StringBuilder...java/lang/System.. .out...println...run...toString.0.....,.....-.*.....;.!...)...C.....7*Y..._....2*....2.....Y.....*....2.....(.$..

C:\jar\carLambo\ZkwKzBMaxNbOlYdeHUyJr.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	120
Entropy (8bit):	5.187210437818789
Encrypted:	false
SSDEEP:	3:Dbll52NVHTf8HmPQ+phHZMfuHXbQCK8P5GxzmllIln:xobz3hOfuHLRP5ltl
MD5:	CECC2F9AB9D3ACCCD2505BF469FBF9D0
SHA1:	75C3DD97BFDCBC2E73354988075492D8B0A699D5
SHA-256:	0C58D99AB3BED205CCE92E0A5173C5B699F90D4DCFB88F7DF213761E285FA6E9
SHA-512:	624FDB36E679297D187890C8432B7C24A2463D82772A19C3D010EA9ED69AB28C2A41687D8E209FB35A4A062E941058796561FCF07D45CAE5181493C80514DD5B
Malicious:	false
Preview:	.....1.....()V...WAjaJbPBkhpSMiTfTlSfV...carLambo/ZkwKzBMaxNbOlYdeHUyJr...java/lang/Object.....

C:\jar\carLambo\aNhPdlHWbWcyZlRBjRTvT.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	15005
Entropy (8bit):	6.400759522485269
Encrypted:	false
SSDEEP:	384:faEgkM/DSUnXgbUdBNr9pT3XLI7j8wYkvhU6jsjZDyt9k0:iDkM/DS0bdXrHLlZHIyt9x
MD5:	43043D0CF13F702A7518BC4F1721CD51
SHA1:	0130E50731111F122474F5720313C9E2A8149A6E
SHA-256:	8A4542324585406904095 38F9D78D07EE8543783EAD705C2BA400F6DADBC61B7

C:\jar\carLambo\aNhPdlHWbWcyZlRBjRTvT.class	
SHA-512:	8D7941E0B25CCD070DE1235CD55AC70E02D6CDE4F071741936CEB3BA27AA0E7E1673BD8AFF375C7F0424F1A1111DDF77615AEC9979AEFBB18FA326C9E92163 9
Malicious:	false
Preview:	.....1.+.....C..D..E..F..G..H..I..J..K..L..M..N..O..P..Q..R..S..T..U..W..Y..Z..[..\..]..^.._..`..a..b..c..d. .e..f..g..i..j..k..o..s..u..v.....!..$..%..'..(..)..*..... .....d.....t...z....|.....w..... .....}....h.....m....h.....o.....m....h.....o.....o....q.....x....y....{....~.....r....h....i....h....h.....i....p....o.....h

C:\jar\carLambo\amywDpahHAvKsbAjnpCoO.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	500
Entropy (8bit):	5.48046280759905
Encrypted:	false
SSDEEP:	12:tZmqryKhy1CmlphYZZ8Imz9RF+ViYkloFbhJ1c:+qXhy1DehYkXzlTSw
MD5:	63DAAAE3B1D1F403D685F19F076B69E4
SHA1:	3D72DA3A613C26D498D3B7577DB73DAA13202FBE
SHA-256:	07364533B71683D01C5B95D0BC43D2F2FC227557AA434A8F7ED6DE8DD8D5915D
SHA-512:	FA90711E37FB5A161AFA824E2EE0877E5B091C4FE13A1A5C7EE2A53327957E5AA75C4266F8ACEAF80C8A6384FC669281E7C5BEF4736E4C76EC5D09DEFE8398 DC
Malicious:	false
Preview:	.....1.....()V...(Ljava/lang/Runnable;)V..%(Ljava/net/Socket;Ljava/net/Socket;)V...<init>...Code...Ljava/net/Socket;...WAjaJbP BkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...carLambo/amywDpahHAvKsbAjnpCoO...carLambo/anzYKctnLiQPVOOntxFFV...java/lang/Object...java/lang/Thread...start .1.....*.....K.....?,*Z+.....Y...Y*Y..._.....Y...Y*Y..._.....

C:\jar\carLambo\anzYKctnLiQPVOOntxFFV.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	1134
Entropy (8bit):	5.7005494671141905
Encrypted:	false
SSDEEP:	24:tWZaO8jMGy1RfqNehiPxzuKRuDlDpHsYNsuZzDtl:oZU5qCNM8z9ufauZzr
MD5:	B488A2A401AEB5B53A667E7901AF24E0
SHA1:	3745AC5FCD3F1E46404D69D8BBCF64903679593A
SHA-256:	48ADC9332685F624F40834163E441B09A39F04527A95DA4DFF395F2C661B02A8
SHA-512:	AF9A9B614E4A6B19BDAF813236FB4D0440FABA6C601E9124C65A481816AF65168E7390161B700892F778A169DE1B483CDE72374C2FFDEA3C761A6D17FDF2E16
Malicious:	false
Preview:	.....1.G..6..;..<..=..>..?..@..A.....$....".....#.....%...."..... ....!...,.(....1../.0..3.2..4.5..7.(..8.(..9.&..:.'..B.(..C.*..E.2..F.+...()Ljava/io/InputStream;...() Ljava/io/OutputStream;...()V..%(Ljava/net/Socket;Ljava/net/Socket;)V...([BII)I...([BII)V...<init>...Code...FLUCgYjjYukBnLOPJmMXa...IkqnNUVNYHrOTFlrdiXDE...Ljava /io/InputStream;...Ljava/io/OutputStream;...Ljava/net/Socket;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...Z...carLambo/anzYKctnLiQPVOOntxFFV...c lose...flush...getInputStream...getOutputStream...java/io/IOException...java/io/InputStream...java/io/OutputStream...java/lang/Exception...java/lang/Object...java/lang/Ru nnable...java/net/Socket...printStackTrace...read...run...vAJiRrxrPqrmdaYHqifDe...write.1.....3.2.....4.5.....E.2.....1...../.0.....,)...-...?.....+.*Z.....*,+*Z,*+.....W *.....#.$.....D.(...-.....`...M*.....I*....,_.`....Y<...''*YZ\.....*Y...,.

C:\jar\carLambo\chMqAfpdZnrPTUanWELCv.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	584
Entropy (8bit):	5.713856901984484
Encrypted:	false
SSDEEP:	12:u4l77KJscTy1VAsmlphY1lu3RlleyX/ahA/:u4B8Ty1VwehYeAzleyvAA/
MD5:	C4C8A3A69DB36133DC305F1C18A097A8
SHA1:	B2ADB4C39C2E8C21D604DF2DDB973DB171193BAE
SHA-256:	26E360C0334B390C739F960EC0A8E5BCE53578812589D9D9464E35BE666ECB74
SHA-512:	91341EB6D2DDF0D9B51BFDB7357897996E6377A68C7779641BA49BE306CE16C926795DEE43EAB21CB4AD9E16E936D411BD2530D5A93AAC369797F5AE4511FF4 7
Malicious:	false
Preview:	.....1.....()V..T(LcarLambo/RhcfPXNPybLnSaSYqyEXw;Ljava/net/Socket;LcarLambo/InQtwvxSwGlKCGaPBlkoE;)V...<init>...Code.. LcarLambo/InQtwvxSwGlKCGaPBlkoE;.. LcarLambo/RhcfPXNPybLnSaSYqyEXw;...Ljava/net/Socket;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG. ..carLambo/RhcfPXNPybLnSaSYqyEXw...carLambo/chMqAfpdZnrPTUanWELCv...java/lang/Object...java/lang/Runnable...run...vAJiRrxrPqrmdaYHqifDe.0..... .....*Y..._...*..... .....-*Z[.*+.....

C:\jar\carLambo\dAXHhOjprIGmjWiJRHaiQ.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	2338
Entropy (8bit):	5.672251853940972
Encrypted:	false
SSDEEP:	48:Oq/9ZjGI5hS6sONbz9VN+52ol5t2AN8XhtP5wL9:zpGI5YhOBNS2atLOx/wJ
MD5:	3FE6F3942E6AA5179F5199B5CE939A35
SHA1:	99949ECCDB3B7A757E68288D315642C544BABB15
SHA-256:	EBC0910E0E189A95CAE214017E52A0B5E6A7CD4D7D1B289CB0E7E963197E98BA
SHA-512:	62005A0CAED0206BC910FA34139D3E78255A71064FBF91F6680641450B6B6237367651823A1BF68BF96D56614556F0B475991D5D7F98830F9FC05189C85CF90B
Malicious:	false
Preview:	.....1.....d..e..k..l..m..n..o..p..q..r..s..t..u..v..w..x..y....3....4....E....1....2..../....C....0....?....@....A.....D.....8....=....6....<....9....>....5....7....;....B....:..].K..].N..].X..a.V..a .X..a.`..b._..c.Q..f.W..g.P..h.M..i.L..j.H..z.J..{.O..|.L..}.F..~.S....T....U....R....G....G....`...()Ljava/lang/Object;...()Ljava/lang/String;...()Ljava/util/Iterator;...()Ljava/util/List;... ()Ljava/util/Set;...()V...()Z...(I)Ljava/lang/String;...(Ljava/io/Reader;)V..3(Ljava/lang/CharSequence;)Ljava/util/regex/Matcher;..&(Ljava/lang/Object;)Ljava/lang/Object;...(Ljav a/lang/Object;)Z..8(Ljava/lang/Object;Ljava/lang/Object;)Ljava/lang/Object;...(Ljava/lang/String;)D...(Ljava/lang/String;)F...(Ljava/lang/String;)I..&(Ljava/lang/String;) Ljava/lang/String;..-(Ljava/lang/String;)Ljava/util/regex/Pattern;...(Ljava/lang/String;)V..8(Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String;..((Ljava/lang/String;Ljava/lan g/String;D)D..((Ljava/lang/String;Ljava/lang/String;F)F..((L

C:\jar\carLambo\dpKhbKrSnHDyRqwJknedZ.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	3902
Entropy (8bit):	5.937652363265064
Encrypted:	false
SSDEEP:	48:OAVjh/NH+dqXjvDPUpHVTAFgqF3UT2ZsN5DYFbCUEBA5WqjwulUJ8Tjfx8ffUqLG:/V9BkqMkgQKq+SzjwRJ8XCffssr27FH5
MD5:	7FEC2FA8DB915D5E4A7EBDB0D62D76DB
SHA1:	0388FBB13AE913537FF640244E0B110F61904483
SHA-256:	DC9DEEDE689FAF6DE22F534F6D882B34D89084FBDF3F952EAF431683C3208177
SHA-512:	94520ACC41FC90F7BA0DDA8F3914B61FA6096A446FC2319F278920C41B9A8C6BB1B53571764B61F1F69C1A125F4D6CE441860559656B4A0CDB1B6C6B88069F62
Malicious:	false
Preview:	.....1.....c....p...v.....b....d....i....p.....j.....g....g....o.....e....h....m....n....^....l....g....f....k....a.. ..q.....^....w....z....{....s.....~.....]....t....._....`.....]....r.....u....}.. .|..!....".y..#.x..$..... .....*.*B#.&.....8.9B#.&.....r.b.y.sMq.{.r....r.x.e.r.8.x.q.pCc.c...()Ljava/lang/Runtime;... ()Ljava/lang/String;...()Ljava/net/URI;...()Ljava/net/URL;...()Ljava/security/CodeSource;.."()Ljava/security/ProtectionDomain;...()V...()Z...()[Ljava/lang/String;...(I)V...(ILj ava/lang/String;)Ljava/lang/StringBuilder;...(Ljava/io/File;Ljava/io/File;)V...(

C:\jar\carLambo\eSHYGKVncDlRweeZuClPC.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	1815
Entropy (8bit):	5.863072245263095
Encrypted:	false
SSDEEP:	48:9eX9SOwob5DXaFe/mg8/1pY5yjsqkS1qpj2S1W:pSce4fYAvX8pxs
MD5:	2766C88B7F0D3673D823173B399ED1D6
SHA1:	987208F42947CF3EADC66820A860C7F6450246D1
SHA-256:	65BCB39C9209EAD2BC9F5473E3D93442DCFE807AB75DB2C510AE236DD845BAD7
SHA-512:	6CE659016F7C947938E30720BD3D2B82F06CAFCCFD0C75C698F8938763F53EDC49E1097B0DE93C4FC3E3F55823E82A0F16F7015EA0F4F30D9F422DA498CB025
Malicious:	false
Preview:	.....1.`..3..4..D.._..F..G..K..L..M..N..O..P..Q..R..S..T..U...,....%....*....+....2....#.....'...-....$..../....1....#....&....)....0....(..?.6..?.=..B.:..E.;..H.<..I.9..J.8..V.7..W.7..X.A..Y.6..Z.=.. [.>..\.5..].5..^.=..*.gV.KaQ.AkCgKkA.L`.dDxD DyQ @x@`Q nk\KSkKz....gV.L`SoIgA.Nk\....()Ljava/lang/String;...()V...(I)V...(ILjava/lang/String;)Ljava/lang/StringBuilder;...(L java/lang/Object;)I..&(Ljava/lang/String;)Ljava/lang/String;..-(Ljava/lang/String;)Ljava/lang/StringBuilder;..-(Ljava/lang/String;)Ljava/lang/reflect/Field;...(Ljava/lang/String;)V ..'(Ljava/lang/String;)[Ljava/lang/String;...<init>...Code...Ljava/io/PrintStream;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...XnQ...append...carLambo/WKT BLojTnJupFuAfwhtUj...carLambo/eSHYGKVncDlRweeZuClPC...getField...getInt...insert...java/awt/Robot...java/awt/event/KeyEvent...java/io/PrintStream...java/lang/Class.. java/lang/IllegalAccessException.."java/lang/IllegalArgumentException...java/lang/NoSuchFieldException...java/lang

C:\jar\carLambo\eWXALjSUSDRBlUrdVjYaX.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	3671
Entropy (8bit):	6.248447147576148
Encrypted:	false
SSDEEP:	96:ZyZIAydtBK3C2YqRhx6NvrQf7Oiqwqey0:ZyZ5yd3bAhnIwq6

C:\jar\carLambo\eWXALjSUSDRBlUrdVjYaX.class	
MD5:	2060BBAB80A54538B32E4B59043A4141
SHA1:	5E5EBC1B50F32253E62B56240FC6D25763D780DF
SHA-256:	C2BEA44C28DA1FCE8609C91A8741B50AC0BBBB401B71AD8EC0C918C2F8AE3740
SHA-512:	449263311F19385AF75899E7951037A0CB0F89252464EFAC982A5ED9EE3C4268CB94441556DF9E18D013A723702927BD46AE904BCA07C5F727295FAFD8AFE085
Malicious:	false
Preview:	.....1.....m..n..o.....T....U....R....P....R....R....S....R....Q....K....[....^....K....J....N....Y....e....j....J....W....d....k....V....X.. ..]....b....g....h....i....l....J....f....Z....`....c....\....a....L....O.. .M...._....r.....|....}.....x....~....t....w.....s.....q....t.....p....z....y....p.....x.. ..p....u....q.....Y.?.;.qCd...$]e.*...e.9.d.*...yC$.,C3.9.*..d.:..".A!.).d_e].ByBzC8.'.?.f./.(AxBzXe^e]e.*...G.?.;.qCd...$]e.*...e.9.d.*...yC%.?C!.=.d...d.%.d.%.dYeYe\d.%.fYeYe\ e.*.....%.fYeYe\e.*....()I...()Ljava/lang/String;...()V...()Z...()[B...()[C...()[Ljava/io/File;...(I)C...(I)Ljava/nio/ByteBuffer;...(ILjava/lang/String;)Ljava/lang/StringBuilder;..B(ILjava/security/Key;Ljava/security/spec/AlgorithmParameterSpec;)V..#(LcarLambo/eWXALjSUSDRBlUrdVjYaX;)V...(Ljava/io/File;Ljava/io/File;)V..&(Ljava/lang/String;)Ljava/la

C:\jar\carLambo\eXJaDawGGAXnThaaGUiMt.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	3500
Entropy (8bit):	5.98972725586379
Encrypted:	false
SSDEEP:	96:lBtvbdAZrO3J7bqQ9QqTLtkVjXnSL7Tf9:lyZi3JPlzSRSL7TV
MD5:	D5F399FD0E4967F75429E5BE60EE2E93
SHA1:	91AD0AD1A898C07CDA0205C049DCAAD3BF1021CE
SHA-256:	20F893C86C99CBC19A5CD1106516DB3E8BFBB626AC1B6D92680AB5B2E3B0EC74
SHA-512:	8BCF8B9959C43BCF4CF544794B902A29877EAA610E31BF904F6596EFE1710FDEE122D76814C3AC88D878B3834EB96453821233257CCF54B7B01D955A1A583BA2
Malicious:	false
Preview:	.....1....r..s..t..u..v.....X....Y....p....R....V....Q....S....W....T....U....o....V....Q....^....b....O....\....j....O....b....N....k....m....N.... [....e....n....c....N....a....g.. .Q..!.P..!.\..!.]..!._..!.i..!.q....d....h....Z....`....f....l....|.....{.....|....|....}....|....~.....y.....}.....z.....x..... ...w.....y....|.....$.".8B!.$.....8.9B#.&.....u&a k,.....?....()I...()Ljava/lang/Object;...()Ljava/lang/String;...()Ljava/util/Iterator;...()Ljava/util/List;...()V...()Z...(I)Ljava/ lang/Object;...(ILjava/lang/String;)Ljava/lang/StringBuilder;...(Ljava/io/File;)V..>(Ljava/io/File;Ljava/io/File;Ljava/io/File;)Ljava/lang/String;..;(Ljava/io/FileInputStream;Ljava /util/zip/ZipOutputStream;)V...(Ljava/io/OutputStream;)V..D(Ljava/lang/CharSequence;Ljava/lang/CharSequence;)Ljava/lang/String;...(Ljava/lan

C:\jar\carLambo\gMLqgzFlLKCRhknogvWcQ.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	1938
Entropy (8bit):	5.931741612690193
Encrypted:	false
SSDEEP:	24:z2aHEnqithD+yRY5KFyCsR3CzPyuLQQuljUUTFdIRlEHlOhzT5DV5UDCrVEn6GKR:zFituuc32PNUTMiIzT5DV/GvVMGa1
MD5:	F1EB7AEFFB3D0E2252E3BB9AE138D4A4
SHA1:	A0B3B45143C3706DC24848BC3399B1A6A09A34FF
SHA-256:	269BD2F880AF8D1F10D30CC3529890F01C58574D0CAED291DF74ACC0061D19A5
SHA-512:	CC9172ACF3EA5E979A2DD5DE55D0A71ADDDCB49168F944E3F951785D2045DDCFA53C8B234BB8BDA3641A09A720FFCC3EDA010AFD904F9A9841AB00D011E1E D8E
Malicious:	false
Preview:	.....1.....L..M..N..]..._..f..}..h..i..j..k..l..m..n..o..t..u..v..w..x..y..z..{..|.....@....H....9....?....8....:....<....=....?....>....;....7....B....C....G....G....6....F....J....6....A....E....K.... D....I..^.P..^.\..a.P..c.O..c.P..c.R..c.U..c.V..c.X..c.Z..d.e..g.[..p.Q..q.O..r.Z..s.T..~.Y....P....b....W....S....O....*.*.e.3.iLf.*.kN....*.*B#.&.... ...()Ljava/lang/String;...()V...()Z... (I)Ljava/lang/String;...(II)Ljava/lang/String;...(ILjava/lang/String;)Ljava/lang/StringBuilder;..:(ILjava/lang/String;Ljava/lang/String;I)Ljava/lang/String;..:(ILjava/lang/String;L java/lang/String;Ljava/lang/String;)V...(J)V...(Ljava/io/File;Ljava/io/File;)V...(Ljava/lang/String;)I..&(Ljava/lang/String;)Ljava/lang/String;..-(Ljava/lang/String;)Ljava/lang/Str ingBuilder;...(Ljava/lang/String;)V...,...<init>..-?$.?.*..0..(.$.$.?0..%.$.80..9...?:..8.$..>>....Code...FLUCgYjjYukBnLOPJmMXa...Ljava/lang/String;...WAjaJbPBkhpSMiTfTlS fV...WLVpZVKPTwBamUZoZCNyH...Z..-]JhQyD|@RhgF|J}JhQRrgKjJyVR

C:\jar\carLambo\gPLIBbXIRgEqoywxWrJpW.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	6316
Entropy (8bit):	6.112633424300488
Encrypted:	false
SSDEEP:	192:JGsDYb2tB62fbwVz2Dq2MqC2Z2U2S2aws2q:JJDVtBdfbOaDNMq1IvFawXq
MD5:	A1FDAC3393F29E0588B36F6C16EE2BFA
SHA1:	9349387FEC59AFAED3B5CA13D954C0A75F69BD54
SHA-256:	93E4ED7FFECA1FC05431389E045CEE13D6DE775096BFFF65A2F67A2668ACE506
SHA-512:	1E58EBBD0DB39A835F3FEDE9F51A5787F978B48EC07EDCDB341B03124D0958F27A43E670AE0E55322EBFF9EC6CD2827738F5B00B8FF2041AC1ADCF3BB865FD 7A
Malicious:	false

C:\jar\carLambo\gPLIBbXIRgEqoywxWrJpW.class	
Preview:	.....1.....?.....a....b....k....n....o....p....q....r....t....x....~.....#.c....e....e....d....f... .g....h....i....j....l....m.. .z..!....".._..#.^..#.|..#....$.]..$.y..%.`..%.w..%....%....&.]..&.u..&.v..&.{..&....'.}..'....(.]..).]..)....+....+....*.s..... .....n'c&p:U,`.w,i.b0....n'c&p:U,`.u,f=b.b0B1....n'c&p:U,`.b%b=b.f%r,....n'c&p:U,`.r ,u0N'a&L,~x...!l,~t...'il,~t...()I...()Ljava/lang/Class;...()Ljava/lang/String;...()Ljava/util/prefs/Preferences;...()V...(I)C...(I)Ljava/lang/Integer;...(I)Ljava/lang/StringBuilder;...(I)V... (ILjava/lang/String;)Ljava/lang/StringBuilder;...(ILjava/lang/String;)V..%(ILjava/lang/String;I)Lj

C:\jar\carLambo\gnZAbPgVxflhpdLkKRSEC.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	401
Entropy (8bit):	5.51572627382003
Encrypted:	false
SSDEEP:	12:UHqpMtyXk5hy17yhphYVubZyr3Rl9l6/s8uPkM50:4qpMtyXYy17yvhYQbZyDz9cE8FM50
MD5:	315554C1F4620FA90E12CE9FC91584AC
SHA1:	75A2990546E07BC6639346CC059A5F447257B3D8
SHA-256:	CD87CB34D3B3B18C76C6481E80FE3094F2C2EB9DF97B0777E66B4DFCFC428052
SHA-512:	2B296D87503E281B3AD3906108D4CBC4C6A7A8C783955988BEA2B22B390120F821BF39B4E948D00BBA5497F59888D2AB27778B28F0904C5F8833694609CD008C
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/vmvXFcYvTedJqkhtugLYR;)V...<init>...Code.. LcarLambo/vmvXFcYvTedJqkhtugLYR;...WAjaJbPBkhpSMiTfTlSf V...WFnpewDUZzidjcKbMnKqG...carLambo/gnZAbPgVxflhpdLkKRSEC...carLambo/vmvXFcYvTedJqkhtugLYR...java/lang/Object...java/lang/Runnable...run.0..... .....*Y+.....*.....

C:\jar\carLambo\hBSMFRWfUehfEMRTcdxur.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	377
Entropy (8bit):	5.405420348593946
Encrypted:	false
SSDEEP:	6:ps3lpzsgKD94y1JKDxlbz3hPKD+he5pRPt+NuIcuI2mlknM5UK/sxl:osiy1JsxVVPsMOpRlnlcuJkM5f/sj
MD5:	6F9C22881F42373AA66B479CB68FE571
SHA1:	2837FFCA59D5C197440340AFA51100537C31BEB3
SHA-256:	AFBA90450FBBE8BE34C7153A031583CD230F8905473F3948E3C4F4A5F2BCF798
SHA-512:	55CF76E129A61FDA9ADF8A02735D259DD257BF0EE86EE6EB7BE000754CF016D3EE7BC59A982F53116ACB865652FBD4C076DF75B6448C3E8B2A3FE9C04013EA 02
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/PRecjdEZwdifBquTYRlUl;)V...<init>...Code.. LcarLambo/PRecjdEZwdifBquTYRlUl;...WAjaJbPBkhpSMiTfTlSf V...carLambo/PRecjdEZwdifBquTYRlUl...carLambo/hBSMFRWfUehfEMRTcdxur...java/lang/Object...java/lang/Runnable...run.0.....*..... .....*Y+.....

C:\jar\carLambo\hcHXKAfoYuEiOypNbthOq.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	277
Entropy (8bit):	5.126380357113838
Encrypted:	false
SSDEEP:	6:xkdHfW4y1vhQ5wlZhAORPt+NkqXUTHS500lplln0OloFv:ODy15QuljAORIleyLLNNlod
MD5:	15C28E72D9B25D494B398DDC0CEDAE49
SHA1:	7F9C1441BC7D88DD59C25ABC13B341FF82FB5BE2
SHA-256:	2F9F984CDAE9649578B74EEED01C98D9D3572B548138D6A741511C6D8388A6DC
SHA-512:	B9A60388515267BE1B9F9D1337C6169659FFBF8D41F7A52A7B47C839D41A4CD3BEB5D5E3E1827EB5A9B69AA02462B0FE5D0FC3F4A4E958617831D6C2803A041
Malicious:	false
Preview:	.....1.....()V...<init>...Code...carLambo/aNhPdlHWbWcyZlRBjRTvT...carLambo/hcHXKAfoYuEiOypNbthOq...java/lang/Object...java/lang/Runnable ...run...vAJiRrxrPqrmdaYHqifDe.0.....*.....

C:\jar\carLambo\ifmTFpwQLwUvcmBtqiUxG.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	3407
Entropy (8bit):	6.234242281513743
Encrypted:	false

C:\jar\carLambo\ifmTFpwQLwUvcmBtqiUxG.class	
SSDEEP:	48:8OL5Nz3HzVVYCvK06NCvpPqC1GCKLCvERcz5GV4C+WWgdNhHxCIP6/nh9Ji6lTYs:P3E0ZxMYGhlHM3jJdlTYpil
MD5:	2BD926A757B877389CE7BDB8E9A3EEE4
SHA1:	6E8BFE20DE5389BA6DD3A049B077075CF4B7FA79
SHA-256:	01CA59E05A0AA640CAD628CE879E78D06D417E088BA05722AA0D9BBF7A70A072
SHA-512:	E77C7B20B203D3CBF1950BA7115024542F77B091AEF5A12CF886712FE1C42A3C5FF6D64D55CEE4A4DE466CA3E8CA54E0B77646F3458817EB40ABBC4BBD3153 E
Malicious:	false
Preview:	.....1....f..g..h..i..j..k..l..m..n..o..p.....!.M....N....O....P....Q....a.. .V..".`..#.J..$.K..$.L..$.T..$.U..$.W..$.Y..$.^..$. b..$.d..%.J..%.S..%.[..%.e..&.J..'.Z..'._..(.R..(.\..(.c..).X..).]..*.\....v.....y....\|.....~....x....w....z....t....u....q....r....v....{....}....q....s....s..... .....!...()I...()Ljava/lang/Object;...()Ljava/lang/String;...()Ljava/util/Iterator;...()Ljava/util/Set;...()V...()Z...()[B...(I)C...(ILjava/lang/String;)Ljava/lang/Stri ngBuilder;..O(Lcom/sun/jna/platform/win32/WinReg$HKEY;Ljava/lang/String;)Ljava/util/TreeMap;...(Ljava/lang/CharSequence;)Z..D(Ljava/lang/CharSequence;Ljava/lang /CharSequence;)Ljava/lang/String;..&(Ljava/lang/Object;)Ljava/lang/Object;...(Ljava/lang/Object;)Z..&(Ljava/lang/String;)Ljava/lang/String;..-(Ljava/lang/String;)Ljava/la ng/StringB

C:\jar\carLambo\jNOmAVANbBsSwqYRQpxgY.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	377
Entropy (8bit):	5.468036378189545
Encrypted:	false
SSDEEP:	6:HU3lpzsD1y4y1m54z3hGWHW28E0hcRiRPt+Ncl3XK/sxBPmlknM50:Zy1+4VGW2jfhRl9l6/sXqkM50
MD5:	A9C88B80291D2DF071A48CE420ED4C4E
SHA1:	8E0E401398DFCF1BF0EF14DF2E2FBDD87E578F8E
SHA-256:	8CD4A696A5A0FF27A01D6DC136E37767BD06CD3F83EFFB65FBFC721DA5357908
SHA-512:	59960196F5D008FA67F9C75FC1424584A803BAB011A51175B5F6D969DC41FF4888E4CD1D9DCB123CB66D6B87A9D6E7E3F233FFB8C96238E43F5783637CFB48E 5
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/prIukYBcIICdhLpsxJGHU;)V...<init>...Code.. LcarLambo/prIukYBcIICdhLpsxJGHU;...WAjaJbPBkhpSMiTfTlSf V...carLambo/jNOmAVANbBsSwqYRQpxgY...carLambo/prIukYBcIICdhLpsxJGHU...java/lang/Object...java/lang/Runnable...run.0.....*Y+..... .....*.....

C:\jar\carLambo\jadywgihJVmemkhExuzpm.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	951
Entropy (8bit):	5.841792973296077
Encrypted:	false
SSDEEP:	24:IcbsYpk+xrhCvWL9/CvWty1S47CvWFZh7yPnQTKCvW+z4eC9dIXzN:1brPCvg9/CvCg7CvQfRKCvW+z4z9CXzN
MD5:	FEAF62E9BB9DC0C1EC0FCEB77947870C
SHA1:	DCBC5F0B7101B999FEEFFE4B68045B983B5D16B8
SHA-256:	08146CA5485E4D37521605CC0AC897F309EC140E717992AF7C39438D06554D8F
SHA-512:	1B69882B85B3BBAE9BAEF785E53EA3243063DCE86DF8B252801E6F05F39DE66B7687AA088A6DADD2D22049D042120C3F1E0BD115DB46C609247DD4EFB69F3D 8
Malicious:	false
Preview:	.....1.3..(..)..*..+.,../..0.....%....%.$..&."..-.....1....2.#...()V...()Z..5(LcarLambo/PRecjdEZwdifBquTYRlUl;Ljava/lang/String;)V..@(Lcom/su n/jna/platform/win32/WinDef$HWND;Lcom/sun/jna/Pointer;)Z..-(Lcom/sun/jna/platform/win32/WinDef$HWND;[B)I...(Ljava/lang/CharSequence;)Z...([B)Ljava/lang/String;... <init>...Code...I.. LcarLambo/PRecjdEZwdifBquTYRlUl;..(Lcom/sun/jna/platform/win32/WinDef$HWND;...Ljava/lang/String;...WAjaJbPBkhpSMiTfTlSfV...WFnpe wDUZzidjcKbMnKqG...callback...carLambo/HBrowserNativeApis...carLambo/PRecjdEZwdifBquTYRlUl...carLambo/jadywgihJVmemkhExuzpm...com/sun/jna/Native...com /sun/jna/platform/win32/WinUser$WNDENUMPROC...contains...isEmpty...java/lang/Object...java/lang/String...toString...vAJiRrxrPqrmdaYHqifDe.0.....%.$.....&."....2. !..... .....*Y,*+.....'..... ...E.....9.....M+,...W,...YM.....,*.....*.....*...+.....

C:\jar\carLambo\jxScqCFTjrLlWNGYXdNEZ.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	347
Entropy (8bit):	5.380272805006072
Encrypted:	false
SSDEEP:	6:xbEgEf44y1sWHahGs736l4z1hyhmkr3RPMvuUTYTOlorlbHU/:2gEzy1shJ/4phYmkr3R0We0OlorlbH0
MD5:	B30D6582FE821A8C7898FF7334E131C7
SHA1:	366D1B82393B1AF9795E39423B868BD60DEEA08C
SHA-256:	426D217CB41C35139A0B5CE80EB020679B2ED653BFC11D9ECF45A08E89C935E9
SHA-512:	9DAAADA281AF7198C8C82B383F88931A658984B95C4530F1C7AE67D8B90D5A5AE6F228C9587A29E9F14AC0457CF9B2188C31995A4F67DD5FB2C2ECF8C809025
Malicious:	false

C:\jar\carLambo\jxScqCFTjrLlWNGYXdNEZ.class	
Preview:	.....1.....()V...(B)V...<init>...Code...I.. LcarLambo/lWRkRwQylUNIljRjtAkaC;...Ljava/io/InputStream;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...carLambo/jxScqCFTjrLlWNGYXdNEZ...java/lang/Object...vAJiRrxrPqrmdaYHqifDe.0.....*.....*.....

C:\jar\carLambo\koPaEdvZZnsDCtKcfImQC.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	377
Entropy (8bit):	5.460414295510513
Encrypted:	false
SSDEEP:	6:HU3lpzscnJkVs4y1BnJkDy7z3hs5lZhfnJkiRPt+Ncl3ul2mlknM5UK/sxl:u0y1tiIVAfPRl9luJkM5f/sj
MD5:	089F5537104D79ACB9961EDB3F5695AA
SHA1:	E7D324ED4E34C94454E6C849BA4369DB3ED7DE12
SHA-256:	A4916ABA9DED73AD35BC4DBC45DAB78461660AD644CF0B26E25A387CBE5E5232
SHA-512:	E1039556CF9049DB1D6AF7D1D31AB2F2C75B1589345930E648070222F9667ADFD39FD9DDFB82CB5410158BD4C79E7CFF5069FC9A92B06E4D3FD02CD83B39E8
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/vADhEfSlROOWFitmByjkH;)V...<init>...Code.. LcarLambo/vADhEfSlROOWFitmByjkH;...WAjaJbPBkhpSMiTfTlSfV...carLambo/koPaEdvZZnsDCtKcfImQC...carLambo/vADhEfSlROOWFitmByjkH...java/lang/Object...java/lang/Runnable...run.0.....*.....*Y+.....

C:\jar\carLambo\lIljmvPgJhDKnHUcdUMQJ.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	468
Entropy (8bit):	5.588180604185896
Encrypted:	false
SSDEEP:	12:tqsIaf6svMJy1Jsxr6/MObphYPsM6NhvRlnlkj0GxYylNlqj/:tYS6/y1J4r6ZhYPnWvzlkj0DyFm
MD5:	2EDA03836B9EC36010844F6D4D504988
SHA1:	C5D40F942B324B1BB0C26AD9821B6C26B1630064
SHA-256:	5D37875F31B2F2285E263A9245F96A86F193FA9683C167A593EC715AAB593D45
SHA-512:	FDA706FBD16954E8F362862090CD520B52305A5A613A681A3269D37FB38B194A9AF273BB2F6A8897141CF79BF744FC06BB20CBC66CEF5E7631755B76BB339DA4
Malicious:	false
Preview:	.....1.....()V..5(LcarLambo/PRecjdEZwdifBquTYRlUl;Ljava/lang/String;)V...<init>...Code.. LcarLambo/PRecjdEZwdifBquTYRlUl;...Ljava/lang/String;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...carLambo/PRecjdEZwdifBquTYRlUl...carLambo/lIljmvPgJhDKnHUcdUMQJ...java/lang/Object...java/lang/Runnable...run.0.....,*Z[+.....*Y..._.....

C:\jar\carLambo\nTSsWfapOWJzCPxPKlsSa.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	377
Entropy (8bit):	5.410274157662414
Encrypted:	false
SSDEEP:	6:HU3lpzsiyOSk5y4y17yOx34z3hNyZ1mhZyOe3RPt+Ncl3XK/sxBPmlknM50:IyXk5hy17yhVNk1kZyr3Rl9l6/sXqkM6
MD5:	4F7C8349C4CCAE3FBCCD931E1D8299C7
SHA1:	4ACD409776A2F4CA2E1569F0BCB01C99B5576419
SHA-256:	3319818E6D091A1B4A123CA26070C0833C8775ECC98BB2C1A4FDEB66179EAC1E
SHA-512:	89A5C7A84D8C7E62559CCBEA4021BF51185EE908C91BA6CC2408AD063BBBF75B3E5217B4288AF5D8B7B7279B2786A1640BD28C73C4D706719A58D56D0E433D A
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/vmvXFcYvTedJqkhtugLYR;)V...<init>...Code.. LcarLambo/vmvXFcYvTedJqkhtugLYR;...WAjaJbPBkhpSMiTfTlSfV...carLambo/nTSsWfapOWJzCPxPKlsSa...carLambo/vmvXFcYvTedJqkhtugLYR...java/lang/Object...java/lang/Runnable...run.0.....*Y+.....*.....

C:\jar\carLambo\oKVVeurDdXccUodgtAiki.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	401
Entropy (8bit):	5.477120189312424
Encrypted:	false
SSDEEP:	12:uqpMoHzhy1+HqH7phY0Hx2VRlnlcuaPkM5f/sj:uqpMay1fhYQUzlqcM5fEj
MD5:	C47D466CD9574C913D11DDFFA52F91AD

C:\jar\carLambo\oKVVeurDdXccUodgtAiki.class	
SHA1:	9A59DC42066DB8E10E649C4DFD0DEDBF7F6B247B
SHA-256:	7B71751D9018D85A417E386A48EA3499CFCBA3B57C125709D6A7E09968174606
SHA-512:	72BC8D97C16EF55D79C9BB484E88DFCD2849B2BDA521138837E0A3D32D07336B34A836E69F2B6D16CF3995329BB59DC6290FC12AAFB6016BC3D5BA9A0BD535A
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/WKTBLojTnJupFuAfwhtUj;)V...<init>...Code.. LcarLambo/WKTBLojTnJupFuAfwhtUj;...WAjaJbPBkhpSMiTfTlSfV...WFnpewDUZzidjcKbMnKqG...carLambo/WKTBLojTnJupFuAfwhtUj...carLambo/oKVVeurDdXccUodgtAiki...java/lang/Object...java/lang/Runnable...run.0.....*.....*Y+.....

C:\jar\carLambo\ppqPYkdOMPGLhnnFjoRgt.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	4943
Entropy (8bit):	6.3217273334119
Encrypted:	false
SSDEEP:	96:MHtvY/9I/KOE4f0MzVcTuM0GwKLseblAnDhohpGhohDgShO:EtvYlYKOBfhzMusw2enD8pG8DgShO
MD5:	05F428C6F52A41A6029BD6FFB3F9C7CA
SHA1:	86342D397A6F983DB729690933F765F50A173B05
SHA-256:	F5BB37ED48E50C5008ED0E5F91ED7A3F3AE3C8AE2C0039B24056BFDBBCF76A05
SHA-512:	B236368A0CB6693FB6D3A9AB4E8275D56B9427619E68E6216BF95101FA3E2ABF20C1008489D4EDC609BCD4912A285F1FCB8138910D74B15E6323933D6F493FA3
Malicious:	false
Preview:	.....1....}..~.....[....]...._....a....b....c....e....h....k....z....o....^....S....^....T....`....\....x....y....S....V....g....r....W....g....j....{....g....j....|....q....S....Y....Z....i....l....s....S....f....n....w....U....u....v....g....m....p....X....d....t......./.#WaR#.0..../aAfZ|^`.MzHb.2MzHb.2MkDj.2Vz\b@0GaAw^hJ`Q#Vg_k.?.~]5CaKz.hDcLb\4SkWjD`D"MkIx@zLmD"D|LoI"VoK}.}@|Lh.mJbJ|.-.8.8.8.lDmNiWaP`A#FaIaW4.=.=.=.5HoWiL`.>Uv.sQoGb@uGaWj@|.mJbIoU}@4FaIbD~Vk.yLjQf.?.>..5FaIaW4.?.?.?.5QoGb@#Io\aPz.hLv@j.sQ|^lDmNiWaP`A#FaIaW4.hChChC5XzMuFaIaW4.hChChC5GoFeB|J{Kj.mJbJ|.-.>.>.;.lJ|AkW4.~].VaIgA..?.7.;.5UoAjL`B4.~]5SkWzLmDb.oIgB`.zJ~.z@vQ#DbLiK4IkCz.sQj^lJ|AkW4.~].VaIgA..j.j.j.5UoAjL`B4.~]

C:\jar\carLambo\prIukYBcIlCdhLpsxJGHU.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	6656
Entropy (8bit):	6.2084901718098395
Encrypted:	false
SSDEEP:	96:/FZuWuiB+tQ2wJK8eXkVINkCBXWPLKJj+wuW2DC:/FUiBcKK8YiINRmeMwtcC
MD5:	4F7AE7EA9260F4221A535BC2A101ABF6
SHA1:	B9E4C46D04BAE70466226105821A50A8DEA3C2A7
SHA-256:	B10D6B8393429BB9621033EBDEA6FC9CA4F1D8AB274603FB2B7C6B2CD8F3AC2C
SHA-512:	2F5780265F3C60529791743153168D100DC90796605A37AAC6544F9EDCE22B378EF5DC969548BF30AE7F01D45B6A392DD090C285DD0568D19F76464BBA41E1AB
Malicious:	false
Preview:	.....1.p.....!../..1..;..Y..Z..^._..`..a..l..m..n..o..#..$..%..&..'..>..?..@...A..B..C..D..E..F..G..H..I..J..K..L..M..N..O..P..Q..R..S..2....2....2....4....G...../....0....1....2....2....2....2....2....2....2....3....3....4....4....4....4....4....4....4....5....6....7....8....8....8....8....9....:....:....:....:....;....<....=....>....?....@....@....@....A....A....B....B....B....B....B....B....B....B....B....B....B....C....C....C....C....C....D....E....E....F....F....H....H..... .....".....".....(....)....*....+....,....-.....0....2....3....4....5....6....7....8....9....:....<....=....T....U....V....W....X....[....[....\....]....b....c....d....d....e....f....g....h....i....j....k....k.....W.....K[S....B.....G.....()I...()Ljava/io/InputStream;...()Ljava/io/OutputStream

C:\jar\carLambo\qaFhxuVWqPsAXIszXSnWD.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	377
Entropy (8bit):	5.4375516608993335
Encrypted:	false
SSDEEP:	6:ps3lpzsdH6Ky4y1+H6hHk4z3h0H68h5UckZRPt+Nulcul2mlknM5UK/sxl:VHzhy1+HqH7V0Hx5UckZRlnlcuJkM5f8
MD5:	669049BDD6A0C81FF3657638B49B5A79
SHA1:	4616A96A4C1201ED6C500D4EDA41DEB7157F469F
SHA-256:	AC230BD0D0E1C88CA2352360C3CAAD1CBE1206D5A9879626703BBE944FB0CE39
SHA-512:	05D1BA02EEF04C7645390CF12B5BFE68414C9D36F8B0FF03C58442928CE5F92871ADC2AB52C8C9358A304D81650D59204A8FBAB275B4610339EDE4A174DDB81
Malicious:	false
Preview:	.....1.....()V..#(LcarLambo/WKTBLojTnJupFuAfwhtUj;)V...<init>...Code.. LcarLambo/WKTBLojTnJupFuAfwhtUj;...WAjaJbPBkhpSMiTfTlSfV...carLambo/WKTBLojTnJupFuAfwhtUj...carLambo/qaFhxuVWqPsAXIszXSnWD...java/lang/Object...java/lang/Runnable...run.0.....*.....*Y+.....

C:\jar\carLambo\resources\config.txt	
Process:	C:\Windows\System32\7za.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	220
Entropy (8bit):	5.694514131418305
Encrypted:	false
SSDEEP:	3:WptCGzd9V9BWkjBRDOSCJDWmkJuwHzgdpMyLZqodR+pBVN//gCzIAOVPUJXQ6IO9:cx9VpWSCJXwTCUKU3/4CzI0XhJtNleo
MD5:	90805675E22C4D9663DA43C9B95CFC54
SHA1:	04F2FD1FDD7325B8268C7FE8855D75CF4A385C7F
SHA-256:	BA3D8E857057C6D0BCA2E10632D28406A9CC5C877C9AECE47657DB5A0763AE9C
SHA-512:	E82D0EA40CDC75049245824396DAF534ED65A268B9022B14408656937B5884EE0FA53B3063C4E67A09894110B3CE82D5870B2D550E1A0AE0ABB6DA6E544A79A2
Malicious:	false
Preview:	AAAAEligsFjVxwNuKmt443aFIsKSyshdoiJl9j3Vnqcl3DNInzQP/d4sa+wj3hlN23EoA24PMlKUrrVEhjB9jwFjG2DWAZA6njDZN3M1a4BVwfPo2zEztA2YkcgfMUoNX4 DVSdHdKBjngP1AeaBpjqjuaEqG4vxTJep/i4U26Sm0AsXRVpgVXrAHsSQIOC/XfnKWIBLrh4mwuspRaY/JRgbnUqw=

C:\jar\carLambo\trsUGiegHrIdlKYyegTti.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	1576
Entropy (8bit):	5.843715099571609
Encrypted:	false
SSDEEP:	48:pK84TCvW0JF0EC3wdGQCyCvW8tz5D1MiTY+XG6Kxfq:EHQFxGx5FpIfq
MD5:	39ED7041161B0F18F5868FF168BDD0C3
SHA1:	81F32C78FB13F0757CC813B12E9B5B0002468088
SHA-256:	2018E5594F28BD0940CDECA4BE82FB1920532C72CD08B35740C670910CAA29F3
SHA-512:	E0B0DDD14969FEAF97035DD128DC78ED787B0603EDFA51C35EAD344E34E304CB23B71BC6C4B1D05A984C3EC29AAA7D5F151820EE8D523FA0A7238A27968CE 18
Malicious:	false
Preview:	.....1.f..<..=..>..I..P..Q..a..b..c..U..V..W..X..Y..]..^.._..`.....:.....<.....3....0....7....2....2....1.....:...;.....4....5....8....9....6..../..J.A..L.E..N.R..S.C..S.G. .S.O..T.D..T.H..Z.?..[.M..\.B..d.@..e.C..e.F....]@m....fW.....}@m...()J...()Ljava/lang/String;...()V...(ILjava/lang/String;)Ljava/lang/StringBuilder;...(J)Ljava/lang/String;...(J)L java/lang/StringBuilder;..5(Lcom/sun/jna/platform/win32/WinUser$LASTINPUTINFO;)Z..&(Ljava/lang/Object;)Ljava/lang/String;..&(Ljava/lang/String;)Ljava/lang/String;..- (Ljava/lang/String;)Ljava/lang/StringBuilder;....HgK....<init>...Code...GetLastInputInfo...I...INSTANCE...J...L&.%L...L/.2L..#Lcom/sun/jna/platform/win32/User32;...W AjaJbPBkhpSMiTfTlSfV...append...carLambo/WKTBLojTnJupFuAfwhtUj...carLambo/ifmTFpwQLwUvcmBtqiUxG...carLambo/trsUGiegHrIdlKYyegTti..!com/sun/jna/platfor m/win32/User32..0com/sun/jna/platform/win32/WinUser$LASTINPUTINFO...currentTimeMillis...dwTime...insert...java/lang/Obje

C:\jar\carLambo\vADhEfSlROOWFitmByjkH.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	4759
Entropy (8bit):	6.102514568058537
Encrypted:	false
SSDEEP:	96:XuS1rv2pG9DGSY1U6VnQ/O9e0E6Vn4a/Ybq:XuS0pG9aSY1L9Xe0794B2
MD5:	AB15D5B6188843977B86490D2EE7638A
SHA1:	C7462FBB125B1E152A58B47EB378ADDAA7E4A751
SHA-256:	515A8F03F656F5578D9D1B020EA980D75A852FCE35F3A7C1854D82E45E50D41F
SHA-512:	3D3059D29D5EEC93E8C73C163106BBF5D586DADDF41B738145073A4D73AEB02C566305C49D34CE48AD3FC70DFDB9269950A1EA8894EB67FC6B9FD64BD76CB DE
Malicious:	false
Preview:	.....1...D.....h...l....o.....j....c....i....k....m....n.....f....t....|.....d....s.....f....s..... .....x.....b..... .b..!.w..!....".g.."u.."v.."z.."...."...."...."....#.b..#.p..#.q..#.r..#....#....$.~..%.e..%....&.s..&.{..&.}..'.f..'.y..... .....g.y....v.~.v.r....r.r.r....z.9.o.7BtM5....v.r.~.r...()I...()J...()L java/io/InputStream;...()Ljava/io/OutputStream;...()Ljava/lang/Runtime;...()Ljava/lang/String;...()V...()Z...()[B...()[Ljava/io/File;...(D)Ljava/lang/String;...(I)Ljava/lang/String;... (I)Ljava/lang/StringBuilder;...(II)Ljava/lang/String;...(ILjava/lang/String;

C:\jar\carLambo\vAJiRrxrPqrmdaYHqifDe.class	
Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	381
Entropy (8bit):	5.279728124095983
Encrypted:	false
SSDEEP:	6:rnimb29ky30I/bks4y1LyhCllCWhxUW3RPt+M+8k6Ol3ylUvloJlHxNEtoCklfvH:rniy29ZNbk3y1LYIlCUxB3RIT+8Mtrvm
MD5:	318235A335892B02669FBB2F5DA2D61F
SHA1:	644F70D6A88368542375669E4F7609B8BBF7F58A

C:\jar\carLambo\vAJiRrxrPqrmdaYHqifDe.class

SHA-256:	8ED95779230C5AD2D0695A4974B2E486DD69EB7678ED05479E177CADB6B298B8
SHA-512:	4C4F70C6F34025BBE56E1862A63E0B0A0401B2880E452F958E9545420A069C62C23F9D3615774E4078AD6E51BE487DE3677EC48003289EDEEA65F12F9DDE3B0B
Malicious:	false
Preview:	.....1.....u0.....()V...()Z...(J)V...<init>...Code...WFnpewDUZzidjcKbMnKqG...carLambo/ppqPYkdOMPGLhnnFjoRgt...carLambo/vAJiRrxrP qrmdaYHqifDe...java/lang/Exception...java/lang/Object...java/lang/Runnable...java/lang/Thread...run...sleep.0.....*.....!.....W.W.....

C:\jar\carLambo\vmvXFcYvTedJqkhtugLYR.class

Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	5718
Entropy (8bit):	6.150000862032383
Encrypted:	false
SSDEEP:	96:XcTPKkne+QJ7qO/tF9oYo1+4DgLkdGA8s3NtLkdGAdsU:XcTjenJeO/loYo1pkLPArLC5
MD5:	0C495B1799663BAEB56E1D6F4CE289CF
SHA1:	9D26A30497E048D2B6EDFB8DDA416C8E2DE36B30
SHA-256:	73EF42F53E640C385AEA9C919A16BA2C9550B5F10F451F7868E678F0FB07D1CE
SHA-512:	FD61AD2346A0C30714A16FDCA5026E60ED23CF6F42413A387051A9A5093783B30C6CD85C959F61CD9304ADFD99B480DD751F8F57B1CF96C7D93FBDCD9340B6
Malicious:	false
Preview:	.....1.....@.....p....r.....".k....l....l....l....o....q....n....f....f....m....e.....i....x....{....}..... .....g....w.....g....w....|.....e....z.....e....u.....h.....t....v.....e.....e..#....#....$.y..$.~..$....%.j.. ....!.s..!..... .....b:l=h9....h'biC,d;~9s i.....h*r$b's:....h>i%h(c:...()J... ()Ljava/lang/Object;...()Ljava/lang/String;...()Ljava/util/Iterator;...()Ljava/util/List;...()V...()Z...()[B...()[Ljava/io/File;...(I)Ljava/nio/ByteBuffer;...(II)Ljava/lang/String;...(ILjav a/lang/String;)Ljava/lang/StringBuilder;..B(ILjava/security/

C:\jar\carLambo\xdIozHlUXHmwNaqNNEWok.class

Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	4594
Entropy (8bit):	6.308342963176622
Encrypted:	false
SSDEEP:	48:WL7xRTlSrDbX1/fHy6KKU4ZMr9kr9VgMzz5DFEWoEDU5bDwHDDBb7bD/mY3ceWsB:mTOXdfBJTgjzv5b25z7mYs5Fig3JAV
MD5:	3FD0BDD0F57B8F9935D21547FEF602F9
SHA1:	DEC21F06BE1651D0A5E2F7531898A0C553510019
SHA-256:	003152073E1C4982B7AA6CAD392BCFC9B6CA3F482705446F03D1722117032966
SHA-512:	05813349AA5BCB2F3E5FA432179450474AA4E9FB2112922DC715DE90408ED944169E1F587538F6735BE0A5F9D547E08F41349BCE6444442F7920ADC1BFFB52EB
Malicious:	false
Preview:	.....1.....g....l....o.....!.....k....k....k....n....d....i....k....j....h....m..... .f.. .p.. ....!.d..!.x. .!.z..!.~..!....!....".c.."....#.c..#.u..#.y..%....%....&.b..'.e..'.v..'.w..'.|..'....'....'....'....'....(.b..(.r..(.s..(.}..(....).{..*.q..*.t..*....+...., ...*.*B#.&.....-(.$.%.80..(.>.?B9.(\.....$.*..0....#._...8.<.9....."$L;.8.<.9.k. $.%....%h*lga k,...()I...()J...()Ljava/lang/String;..!()Ljava/nio/channels/FileChannel;...()Ljava/nio/channels/FileLock;...()V...()Z...()[B...()[Ljava/io/File;...(I)Ljava/lang/String;...(I)L java/lang/StringBuilder;...(I)Ljava/nio/ByteBuffer;...(II)Ljava/lang/String;..'(

C:\jar\carLambo\yphecTSiezxVkeTiKHCVh.class

Process:	C:\Windows\System32\7za.exe
File Type:	compiled Java class data, version 49.0 (Java 1.5)
Category:	dropped
Size (bytes):	8218
Entropy (8bit):	6.370366248160064
Encrypted:	false
SSDEEP:	192:mqomueuNs+iJEfLoL4i34x0GsIGQa7pndWI:meueuNMEfLoVIjundp
MD5:	595FDEBF9673C04DE5ED404CA1697AF3
SHA1:	5182196DCFCD8C44689DA2D4C7D1536978CC89C9
SHA-256:	F1F291BAA875F9A8A690707ED9AA00257DB12B3E7353E21D8774DD426C6CB163
SHA-512:	E5201CACDA7AC68E95D8BE4DCD89F0163EF966D4E77CB8FE4CD859DB6E82F49B39252FF6D0B90B772567B61BE805CEE439CB170783F068DEBEC825A20039BA 98
Malicious:	false
Preview:	.....1.....?..@..A..B..C..D..E..F..G..H..I..K..L..M..N..Q..R..S..Z..[..\..]..^._..`..g..h..i..|..}.....m..n..o..p..q..r ..s..t..u..w..x..y.....M....N....P....^....C....D....D....E....F....F....G....G....H....H....H....I....J....K....K....K....L....O....O....O....P.... P....P....P....P....P....Q....R....R....S....T....T....T....U....V....W....X....Y....Z....Z....Z....[....[....\....\....\....\....\....\....\....\....\....\....\....\....]....]....]....^....^....^....^...._....`....`....`....`....`....`....`....`....a....a....a....a....b....b....d....M....c....c....J....J.+..J.,...J.3..J.6..J.<..J.>..P.1..T.V..a.W..b.)..d....d....d.!..d.%..d.&..d.'..d.*..d.1..e.3..j....l.2..v....z....{....~.....4.....0..... .."....-.....1...../....$..../.....X..../....9..

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.9272410126162995
TrID:	• Java Archive (13504/1) 62.80% • ZIP compressed archive (8000/1) 37.20%
File name:	NRB-RTGS 28-Sept 2021.jar
File size:	106220
MD5:	ccfdd7c24c9029f301ee94dbc9441ace
SHA1:	99dce2074fd2cca2ede69a3b08cf33a574a4a976
SHA256:	3ecc6468de96ac9ae350154c117610dd3062f968be547d6b67b3f126fee512e9
SHA512:	3ca8410aca55b1acb92e1c5316fffb01815b7b69b850c1637cc4b04f43a83f2cf52c21c0785c4af30ce9655782c1d285d82055bb120e41d103f0758bf37fe258
SSDEEP:	3072:Q+0dMqzH4I51/j6SJtXr3JN0GMAxoKQ9YDQ:QFesH4i1BJVr5QACKD0
File Content Preview:	PK.....,;S.....META-INF/MANIFEST.MF].=O.0..wK..7.`..VT.J....!.z....c.....e.C...G.....;Q...Rv1..d..!."...@PY.7Rq.%.BV..-I.r....\...O..4...._r.....s....N:.{.ry^B.:...eh.;}..\h.C...Z.....2{,..&.....Hu.....w./-.....{..h-Y..

File Icon

Icon Hash:	d28c8e8ea2868ad6

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/28/21-09:10:03.953293	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57875	8.8.8.8	192.168.2.3
09/28/21-09:10:34.139310	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53910	8.8.8.8	192.168.2.3
09/28/21-09:11:35.017296	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58058	8.8.8.8	192.168.2.3
09/28/21-09:12:05.111863	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55393	8.8.8.8	192.168.2.3
09/28/21-09:12:35.215615	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55108	8.8.8.8	192.168.2.3

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 6364 Parent PID: 6548

General

Start time:	09:22:30
Start date:	28/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c 7za.exe x -y -oC:\jar 'C:\Users\user\Desktop\NRB-RTGS 28-Sept 2021.jar'
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: 7za.exe PID: 584 Parent PID: 6364

General

Start time:	09:22:30
Start date:	28/09/2021
Path:	C:\Windows\System32\7za.exe
Wow64 process (32bit):	true
Commandline:	7za.exe x -y -oC:\jar 'C:\Users\user\Desktop\NRB-RTGS 28-Sept 2021.jar'
Imagebase:	0x60000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 4780 Parent PID: 6548

General

Start time:	09:22:31

Start date:	28/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /c java.exe -jar 'C:\Users\user\Desktop\NRB-RTGS 28-Sept 2021.jar' carLambo.FirstRun >> C:\cmdlinestart.log 2>&1
Imagebase:	0x7ff622070000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

Analysis Process: conhost.exe PID: 5408 Parent PID: 4780

General

Start time:	09:22:31
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: java.exe PID: 5524 Parent PID: 4780

General

Start time:	09:22:32
Start date:	28/09/2021
Path:	C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe
Wow64 process (32bit):	true
Commandline:	java.exe -jar 'C:\Users\user\Desktop\NRB-RTGS 28-Sept 2021.jar' carLambo.FirstRun
Imagebase:	0x250000
File size:	192376 bytes
MD5 hash:	28733BA8C383E865338638DF5196E6FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Java
Yara matches:	• Rule: JoeSecurity_Allatori_JAR_Obfuscator, Description: Yara detected Allatori_JAR_Obfuscator, Source: 00000008.00000002.930901668.0000000009DA4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Allatori_JAR_Obfuscator, Description: Yara detected Allatori_JAR_Obfuscator, Source: 00000008.00000002.930829373.0000000009D68000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_STRRAT, Description: Yara detected STRRAT, Source: 00000008.00000002.929973894.00000000049EE000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: icacls.exe PID: 4476 Parent PID: 5524

General

Start time:	09:22:33
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\icacls.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant 'everyone':(OI)(CI)M
Imagebase:	0x240000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 7036 Parent PID: 4476

General

Start time:	09:22:33
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis