ID: 492179
Sample Name: Quotation.jar
Cookbook:
defaultwindowsfilecookbook.jbs
Time: 12:51:05
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Quotation.jar 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Dropped Files 3
Sigma Overview 3
Jbx Signature Overview 4
AV Detection: 4
Data Obfuscation: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 5
Thumbnails 5
Antivirus, Machine Learning and Genetic Malware Detection 6
Initial Sample 6
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 7
Contacted Domains 7
URLs from Memory and Binaries 7
Contacted IPs 7
Public 7
Private 7
General Information 7
Simulations 8
Behavior and APIs 8
Joe Sandbox View / Context 8
IPs 8
Domains 8
ASN 9
JA3 Fingerprints 10
Dropped Files 11
Created / dropped Files 11
Static File Info 12
General 12
File Icon 12
Network Behavior 12
Network Port Distribution 13
TCP Packets 13
DNS Queries 13
DNS Answers 13
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: cmd.exe PID: 6312 Parent PID: 4660 14
General 14
File Activities 15
File Created 15
Analysis Process: conhost.exe PID: 6328 Parent PID: 6312 15
General 15
Analysis Process: java.exe PID: 6376 Parent PID: 6312 15
General 15
File Activities 15
File Created 15
File Written 15
File Read 15
Analysis Process: icacls.exe PID: 6484 Parent PID: 6376 15
General 15
Analysis Process: conhost.exe PID: 6532 Parent PID: 6484 16
General 16
Disassembly 16
Code Analysis 16

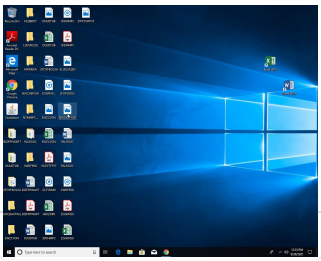
Windows Analysis Report Quotation.jar

Overview

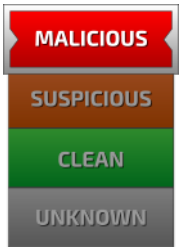
General Information

Sample Name:	Quotation.jar
Analysis ID:	492179
MD5:	8eab8f1a928fa55..
SHA1:	491e913225a8c8..
SHA256:	20351665df8b2d4.
Tags:	jar STRRAT
Infos:	

Most interesting Screenshot:



Detection

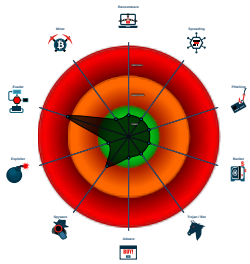


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AllatoriJARObfuscator
- Queries the volume information (nam…
- Uses cacls to modify the permission…
- Sample execution stops while proce…
- JA3 SSL client fingerprint seen in co…
- Creates a process in suspended mo…
- IP address seen in connection with o…
- Java Jar is obfuscated using Allatori
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6312 cmdline: C:\Windows\system32\cmd.exe /c "C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe' -javaagent:'C:\Users\user\AppData\Local\Temp\jartracer.jar' -jar 'C:\Users\user\Desktop\Quotation.jar'' >> C:\cmdlinestart.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 6328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - java.exe (PID: 6376 cmdline: 'C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe' -javaagent:'C:\Users\user\AppData\Local\Temp\jartracer.jar' -jar 'C:\Users\user\Desktop\Quotation.jar' MD5: 28733BA8C383E865338638DF5196E6FE)
    - icacls.exe (PID: 6484 cmdline: C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant 'everyone':(OI)(CI)M MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 6532 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	

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

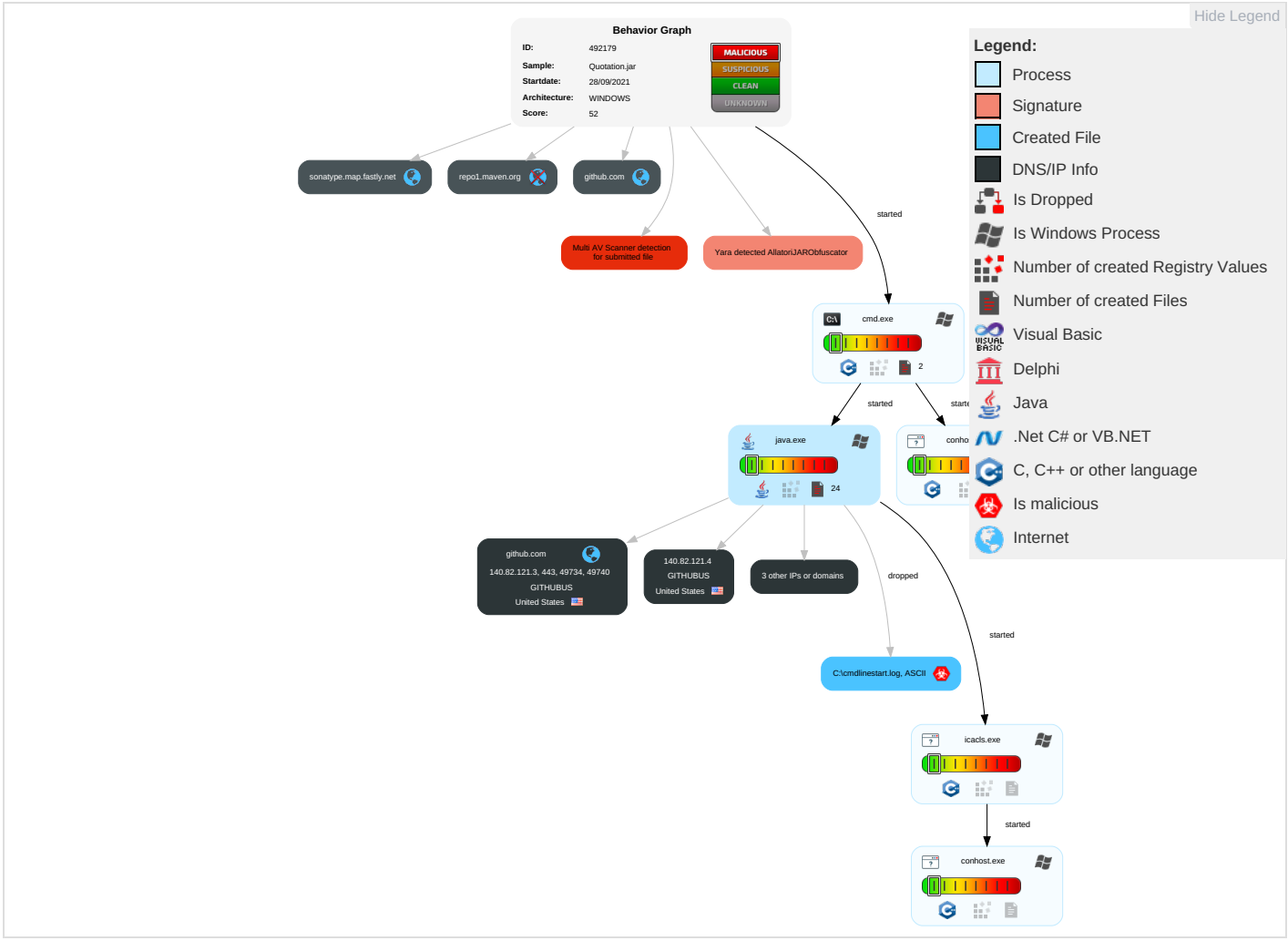
Data Obfuscation:

Yara detected AllatoriJARObfuscator

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Windows Management Instrumentation	Services File Permissions Weakness 1	Services File Permissions Weakness 1	Masquerading 1	OS Credential Dumping	System Information Discovery 1 2	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Dev Without Authorizati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1	Services File Permissions Weakness 1	LSASS Memory	Remote System Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	System Network Configuration Discovery	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 Communication	

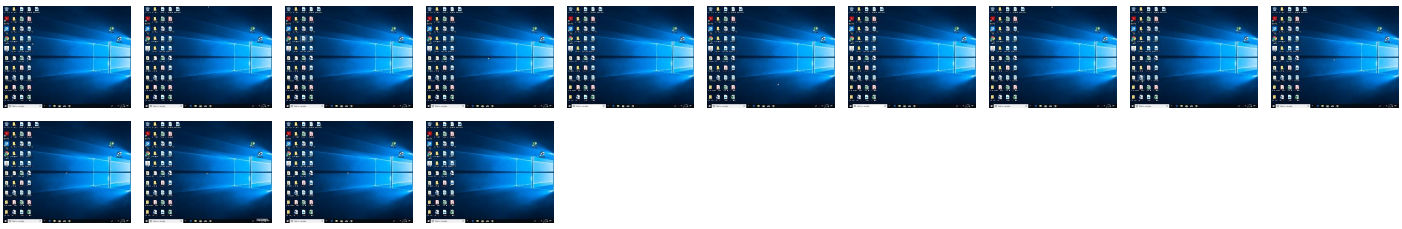
Behavior Graph



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
Quotation.jar	27%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
sonatype.map.fastly.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.allatori.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sonatype.map.fastly.net	199.232.192.209	true	false	• 0%, Virustotal, Browse	unknown
github.com	140.82.121.3	true	false		high
repo1.maven.org	unknown	unknown	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.232.192.209	sonatype.map.fastly.net	United States		54113	FASTLYUS	false
140.82.121.3	github.com	United States		36459	GITHUBUS	false
140.82.121.4	unknown	United States		36459	GITHUBUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492179
Start date:	28.09.2021
Start time:	12:51:05
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation.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
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 • GSI enabled (Java) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal52.evad.winJAR@7/3@12/4
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.232.192.209	NRB-RTGS 28-Sept 2021.jar	Get hash	malicious	Browse	
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	
	Quotation sheet.jar	Get hash	malicious	Browse	
	RFQ_40ft Container.jar	Get hash	malicious	Browse	
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	
	Quotation sheet.jar	Get hash	malicious	Browse	
	RFQ_40ft Container.jar	Get hash	malicious	Browse	
	Quotation.jar	Get hash	malicious	Browse	
	02_extracted.jar	Get hash	malicious	Browse	
	02_extracted.jar	Get hash	malicious	Browse	
	dhl paket.jar	Get hash	malicious	Browse	
	dhl paket.jar	Get hash	malicious	Browse	
	RQF 10020213.jar	Get hash	malicious	Browse	
	Quotation.jar	Get hash	malicious	Browse	
	Quotation Sheet.jar	Get hash	malicious	Browse	
	Quotation Sheet.jar	Get hash	malicious	Browse	
	SWIFT_DETAILS.jar	Get hash	malicious	Browse	
	Quotation Sheet.jar	Get hash	malicious	Browse	
	Quotation Sheet.jar	Get hash	malicious	Browse	
	USpstracKER.jar	Get hash	malicious	Browse	
140.82.121.3	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	
	Quotation sheet.jar	Get hash	malicious	Browse	
	RFQ_40ft Container.jar	Get hash	malicious	Browse	
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	
	Quotation sheet.jar	Get hash	malicious	Browse	
	RFQ_40ft Container.jar	Get hash	malicious	Browse	
	02_extracted.jar	Get hash	malicious	Browse	
	02_extracted.jar	Get hash	malicious	Browse	
	dhl paket.jar	Get hash	malicious	Browse	
	dhl paket.jar	Get hash	malicious	Browse	
	CxarNMwOrM.exe	Get hash	malicious	Browse	
	ZamCfP5Dev.exe	Get hash	malicious	Browse	
	AsvL372I1U.exe	Get hash	malicious	Browse	
	RQF 10020213.jar	Get hash	malicious	Browse	
	Quotation Sheet.jar	Get hash	malicious	Browse	
	Quotation Sheet.jar	Get hash	malicious	Browse	
	Quotation Sheet.jar	Get hash	malicious	Browse	
	Quotation Sheet.jar	Get hash	malicious	Browse	
	W2FDqQa9Da.exe	Get hash	malicious	Browse	
	USpstracKER.jar	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sonatype.map.fastly.net	NRB-RTGS 28-Sept 2021.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	dhl paket.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	dhl paket.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	RQF 10020213.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	SWIFT_DETAILS.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	USpstracKER.jar	Get hash	malicious	Browse	• 199.232.19 2.209

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FASTLYUS	ova9jpkxjW.dll	Get hash	malicious	Browse	• 151.101.1.44
	6fRcd4Q1n1.dll	Get hash	malicious	Browse	• 151.101.1.44
	M76Vc463El.dll	Get hash	malicious	Browse	• 151.101.1.44
	FROqdaZTXE.dll	Get hash	malicious	Browse	• 151.101.1.108
	FmtpSM8PqG.dll	Get hash	malicious	Browse	• 151.101.1.44
	jl9fLPhFtU.dll	Get hash	malicious	Browse	• 151.101.1.44
	amm4Lw6xgJ.dll	Get hash	malicious	Browse	• 151.101.1.44
	bT2842KdOz.dll	Get hash	malicious	Browse	• 151.101.1.44
	6SYurvkD8X.dll	Get hash	malicious	Browse	• 151.101.1.44
	ZXRYejz88D.dll	Get hash	malicious	Browse	• 151.101.1.44
	NRB-RTGS 28-Sept 2021.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	Quotation.jar	Get hash	malicious	Browse	• 199.232.19 2.209
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.19 2.209

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.192.209
GITHUBUS	NRB-RTGS 28-Sept 2021.jar	Get hash	malicious	Browse	• 140.82.121.4
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 140.82.121.4
	Quotation sheet.jar	Get hash	malicious	Browse	• 140.82.121.4
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 140.82.121.4
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 140.82.121.4
	Quotation sheet.jar	Get hash	malicious	Browse	• 140.82.121.4
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 140.82.121.4
	Quotation.jar	Get hash	malicious	Browse	• 140.82.121.4
	02_extracted.jar	Get hash	malicious	Browse	• 140.82.121.4
	02_extracted.jar	Get hash	malicious	Browse	• 140.82.121.4
	dhl paket.jar	Get hash	malicious	Browse	• 140.82.121.4
	dhl paket.jar	Get hash	malicious	Browse	• 140.82.121.4
	CxarNMwOrM.exe	Get hash	malicious	Browse	• 140.82.121.3
	ZamCfP5Dev.exe	Get hash	malicious	Browse	• 140.82.121.3
	AsvL372I1U.exe	Get hash	malicious	Browse	• 140.82.121.3
	RQF 10020213.jar	Get hash	malicious	Browse	• 140.82.121.3
	AW QUOTE 21505 HQ1-Scan-068703_PDF.exe	Get hash	malicious	Browse	• 140.82.121.4
	DHL QA-Tracker.doc	Get hash	malicious	Browse	• 140.82.121.4
	Quotation.jar	Get hash	malicious	Browse	• 140.82.121.4
	Quotation Sheet.jar	Get hash	malicious	Browse	• 140.82.121.4

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
d2935c58fe676744fecc8614ee5356c7	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	Quotation sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	Quotation sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	dhl paket.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	dhl paket.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.3 • 140.82.121.4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209 • 140.82.121.3 • 140.82.121.4
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.19 2.209 • 140.82.121.3 • 140.82.121.4
	USpstracKER.jar	Get hash	malicious	Browse	• 199.232.19 2.209 • 140.82.121.3 • 140.82.121.4
	USpstracKER.jar	Get hash	malicious	Browse	• 199.232.19 2.209 • 140.82.121.3 • 140.82.121.4
	Invoice.jar	Get hash	malicious	Browse	• 199.232.19 2.209 • 140.82.121.3 • 140.82.121.4
	payment slip.jar	Get hash	malicious	Browse	• 199.232.19 2.209 • 140.82.121.3 • 140.82.121.4
	Invoice.jar	Get hash	malicious	Browse	• 199.232.19 2.209 • 140.82.121.3 • 140.82.121.4
	payment slip.jar	Get hash	malicious	Browse	• 199.232.19 2.209 • 140.82.121.3 • 140.82.121.4

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Oracle\Java\.oracle_jre_usage\cce3fe3b0d8d83e2.timestamp	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.852639084674789
Encrypted:	false
SSDEEP:	3:oFj4I5vpN6yUaekpov:oJ5X6yIv
MD5:	2E1C86353094522C49619B36DEF4D335
SHA1:	73E4B01FF53B455F03ACC9BB3FEB6F90B0882C7E
SHA-256:	94F67278D64327ED7AC762B230BED4FB51878871A5295E79F6F29E08285FCD64
SHA-512:	33B5FE79B500EB3CCCA761351B2AA6DE11119CAF0D950F650357D3F5AC42F3564A025D819D33B1DB1065F07272F1C3A6BF5373E2E5F5C3BEEFBC7ED32362CA6
Malicious:	false
Reputation:	low
Preview:	C:\Program Files (x86)\Java\jre1.8.0_211..1632858722398..

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\83aa4cc77f591dfc2374580bbd95f6ba_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	data
Category:	dropped
Size (bytes):	45
Entropy (8bit):	0.9111711733157262
Encrypted:	false
SSDEEP:	3:/lwlt7n:WNn
MD5:	C8366AE350E7019AEFC9D1E6E6A498C6
SHA1:	5731D8A3E6568A5F2DFBBC87E3DB9637DF280B61
SHA-256:	11E6ACA8E682C046C83B721EEB5C72C5EF03CB5936C60DF6F4993511DDC61238

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\83aa4cc77f591dfc2374580bbd95f6ba _d06ed635-68f6-4e9a-955c-4899f5f57b9a	
SHA-512:	33C980D5A638BFC791DE291EBF4B6D263B384247AB27F261A54025108F2F85374B579A026E545F81395736DD40FA4696F2163CA17640DD47F1C42BC9971B18CD
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....J2SE.

C:\cmdlinestart.log	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	635900
Entropy (8bit):	5.037897156829055
Encrypted:	false
SSDEEP:	192:EmMYrvGGGgOOOe3Or3OeOO3wfwfee3OOOee7mmvp3OOOOre3reeeeOeHOOYrOee8:M0
MD5:	08923501DF2652C5C94152A85F19602D
SHA1:	A0698F85DE2E1FB811B41ABED6ED5709E34B9D58
SHA-256:	4AF5DE3F723274F515E5789C63F58A97D9B54798A3FE4E15A2111FBF1B19E455
SHA-512:	B64B72D00A2748D739680A1F543ADF9715708EDF0790C352F9878992F51BF639AEE8874CAB809B2A4F6ED99C3E8954810C3EF099D440C539858F0A506D1E8607
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Allatori_JAR_Obfuscator, Description: Yara detected Allatori_JAR_Obfuscator, Source: C:\cmdlinestart.log, Author: Joe Security
Reputation:	low
Preview:	.###.# #.# ## # # ## ### ### ## ### #.# # # # # # # # # # # # # #.# ### # # ### # # # ## # #.# # # ### ### # # # ### # # ### #.# #.# Obfuscation by Allatori Obfuscator v7.3 DEMO #.# #.# http://www.allatori.com #.# #.################################## ###################...Inside main method..Inside constructor..Executing else..Inside InitLib..Inside completeJob..returned false..C:\Users\user\lib\jna-5.5.0.jar ..EXCEPTION: https://repo1.maven.org/maven2/net/java/dev/jna/jna/5.5.0/jna-5.5.0.jar..EXCEPTION: https://repo1.maven.org/maven2/net/java/dev/jna/jna-platform/5.5.0/jna-platform-5.5.0.jar..EXCEPTION: https://repo1.maven.org/maven2/org/xerial/sqlite-jdbc/3.14.2.1/sqlite

Static File Info

General

<table>
<tr><td>File type:</td><td>Zip archive data, at least v2.0 to extract</td></tr>
<tr><td>Entropy (8bit):</td><td>7.970588409725289</td></tr>
<tr><td>TrID:</td><td>• Java Archive (13504/1) 62.80%
• ZIP compressed archive (8000/1) 37.20%</td></tr>
<tr><td>File name:</td><td>Quotation.jar</td></tr>
<tr><td>File size:</td><td>188977</td></tr>
<tr><td>MD5:</td><td>8eab8f1a928fa55303b7558536079a2a</td></tr>
<tr><td>SHA1:</td><td>491e913225a8c8d144c538fe27cf62f5a8465b38</td></tr>
<tr><td>SHA256:</td><td>20351665df8b2d441524a21163e0aa95ea3d3805a87303
2eb6f55fa1001f3941</td></tr>
<tr><td>SHA512:</td><td>886928d68f14c012186872429739d1317350f329e5afa4e
c820779e7f312d776433e8926000f522a3393e2ad454779
eee1245ba266226bd0c8421f1fb97ba4a0</td></tr>
<tr><td>SSDEEP:</td><td>3072:vCcBIJZi3Kd1+Fv2CmQMKMh4BoRAnm8KELI09
Cu/qinGVexOvwGyJ5e/wWR5inCw:6jc3Kd1xDQMKoT
AnmEL6enGVZdyy/QCw</td></tr>
<tr><td>File Content Preview:</td><td>PK........5V<S................META-INF/MANIFEST.MFU..N.
0..wK~...p&......&B.B.....S...#...e.J....~....'.2~..l..HQqv...a.
~0PX..Br.FC.h|X.....B%%l..zg..q..r9...#..u.R.=.g.T.O6.....
u1.Jyh.Yu.....C.g....).....e....(.B.....l.r6....K........'...{|yo..7....
2@Z...</td></tr>
</table>

File Icon

Icon Hash:	d28c8e8ea2868ad6

Network Behavior

Network Port Distribution

TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 28, 2021 12:52:07.047632933 CEST	192.168.2.5	8.8.8.8	0x8995	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 12:52:07.047760963 CEST	192.168.2.5	8.8.8.8	0x6fb8	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 12:52:37.174921989 CEST	192.168.2.5	8.8.8.8	0xb45f	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 12:52:37.176800013 CEST	192.168.2.5	8.8.8.8	0x14b3	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 12:53:08.076505899 CEST	192.168.2.5	8.8.8.8	0xd97b	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 12:53:08.080358028 CEST	192.168.2.5	8.8.8.8	0x9ea0	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 12:53:38.290983915 CEST	192.168.2.5	8.8.8.8	0x557d	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 12:53:38.295867920 CEST	192.168.2.5	8.8.8.8	0xdd50	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:08.354011059 CEST	192.168.2.5	8.8.8.8	0x4d3c	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:08.354984999 CEST	192.168.2.5	8.8.8.8	0x2775	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:38.467590094 CEST	192.168.2.5	8.8.8.8	0x2c98	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:38.474905014 CEST	192.168.2.5	8.8.8.8	0x76bc	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 12:52:07.068727016 CEST	8.8.8.8	192.168.2.5	0x8995	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 12:52:07.068727016 CEST	8.8.8.8	192.168.2.5	0x8995	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:52:07.068727016 CEST	8.8.8.8	192.168.2.5	0x8995	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:52:07.068867922 CEST	8.8.8.8	192.168.2.5	0x6fb8	No error (0)	github.com		140.82.121.3	A (IP address)	IN (0x0001)
Sep 28, 2021 12:52:37.195182085 CEST	8.8.8.8	192.168.2.5	0xb45f	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 12:52:37.195182085 CEST	8.8.8.8	192.168.2.5	0xb45f	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:52:37.195182085 CEST	8.8.8.8	192.168.2.5	0xb45f	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:52:37.204977989 CEST	8.8.8.8	192.168.2.5	0x14b3	No error (0)	github.com		140.82.121.3	A (IP address)	IN (0x0001)
Sep 28, 2021 12:53:08.097497940 CEST	8.8.8.8	192.168.2.5	0xd97b	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Sep 28, 2021 12:53:08.099559069 CEST	8.8.8.8	192.168.2.5	0x9ea0	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 12:53:08.099559069 CEST	8.8.8.8	192.168.2.5	0x9ea0	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:53:08.099559069 CEST	8.8.8.8	192.168.2.5	0x9ea0	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 12:53:38.312550068 CEST	8.8.8.8	192.168.2.5	0x557d	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Sep 28, 2021 12:53:38.316076040 CEST	8.8.8.8	192.168.2.5	0xdd50	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 12:53:38.316076040 CEST	8.8.8.8	192.168.2.5	0xdd50	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:53:38.316076040 CEST	8.8.8.8	192.168.2.5	0xdd50	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:08.374155998 CEST	8.8.8.8	192.168.2.5	0x2775	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 12:54:08.374155998 CEST	8.8.8.8	192.168.2.5	0x2775	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:08.374155998 CEST	8.8.8.8	192.168.2.5	0x2775	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:08.375171900 CEST	8.8.8.8	192.168.2.5	0x4d3c	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:38.499931097 CEST	8.8.8.8	192.168.2.5	0x2c98	No error (0)	github.com		140.82.121.3	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:38.499957085 CEST	8.8.8.8	192.168.2.5	0x76bc	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 12:54:38.499957085 CEST	8.8.8.8	192.168.2.5	0x76bc	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 12:54:38.499957085 CEST	8.8.8.8	192.168.2.5	0x76bc	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 6312 Parent PID: 4660

General

Start time:	12:51:58
Start date:	28/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c "C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe' -javaagent:'C:\Users\user\AppData\Local\Temp\jartracer.jar' -jar 'C:\Users\user\Desktop\Quotation.jar'' >> C:\cmdlinestart.log 2>&1
Imagebase:	0x150000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 6328 Parent PID: 6312

General

Start time:	12:51:58
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6376 Parent PID: 6312

General

Start time:	12:51:59
Start date:	28/09/2021
Path:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe' -javaagent:'C:\Users\user\AppData\Local\Temp\jartracer.jar' -jar 'C:\Users\user\Desktop\Quotation.jar'
Imagebase:	0xed0000
File size:	192376 bytes
MD5 hash:	28733BA8C383E865338638DF5196E6FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Java
Reputation:	high

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: icacls.exe PID: 6484 Parent PID: 6376

General

Start time:	12:52:02
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:	0xc30000
File size:	29696 bytes
MD5 hash:	FF0D1D4317A44C951240FAE75075D501
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6532 Parent PID: 6484

General

Start time:	12:52:03
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis