ID: 492006
Sample Name: NRB-RTGS 28-Sept 2021.jar
Cookbook: defaultwindowsfilecookbook.jbs
Time: 09:09:00
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

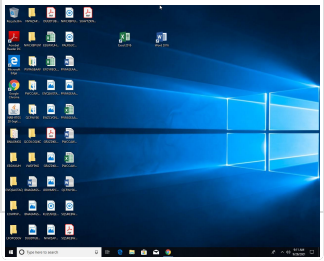
Windows Analysis Report NRB-RTGS 28-Sept 2021.jar

Overview

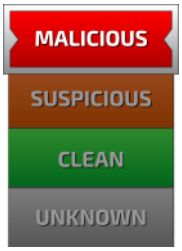
General Information

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

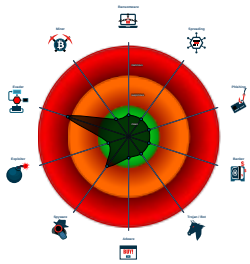


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AllatoriJARObfuscator
- Queries the volume information (nam…
- Uses cacls to modify the permission…
- Uses code obfuscation techniques (…
- 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

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 4536 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\NRB-RTGS 28-Sept 2021.jar" >> C:\cmdlinestart.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 4660 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - java.exe (PID: 4348 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\NRB-RTGS 28-Sept 2021.jar' MD5: 28733BA8C383E865338638DF5196E6FE)
    - icacls.exe (PID: 6780 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

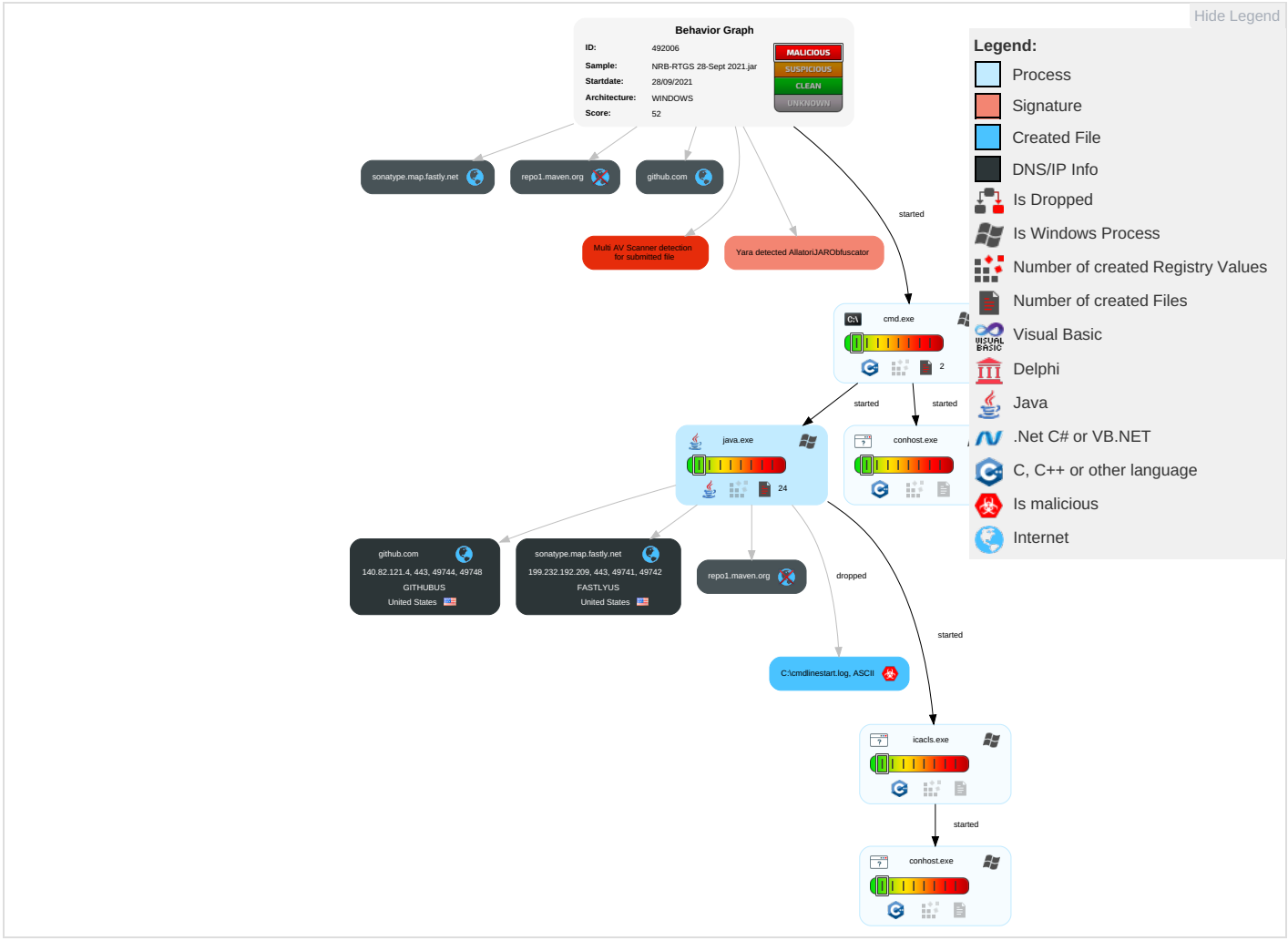
Data Obfuscation:

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	Command and Scripting Interpreter 2	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 Device Without Authorization
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 Authorization
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 2	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

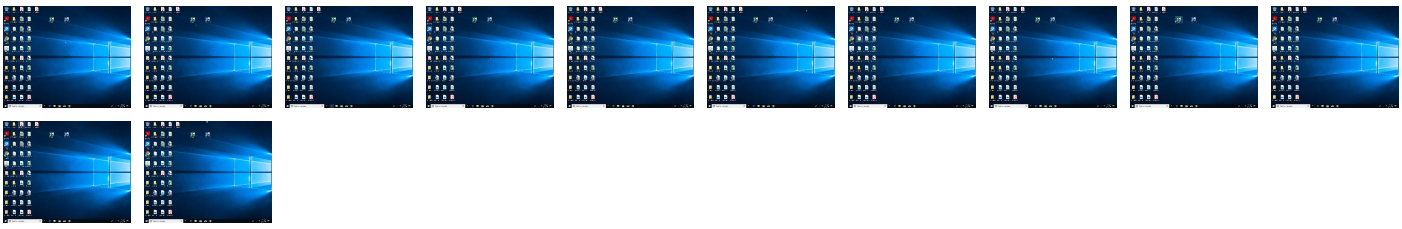
Behavior Graph



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
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://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
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		unknown
github.com	140.82.121.4	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
140.82.121.4	github.com	United States		36459	GITHUBUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492006
Start date:	28.09.2021
Start time:	09:09:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 32s
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
Number of analysed new started processes analysed:	22
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@12/2
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	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	
	USpstracKER.jar	Get hash	malicious	Browse	
140.82.121.4	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	
	AW QUOTE 21505 HQ1-Scan-068703_PDF.exe	Get hash	malicious	Browse	
	DHL QA-Tracker.doc	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	
	WDDzCTWnXh.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
github.com	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	• 140.82.121.3
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 140.82.121.3
	Quotation sheet.jar	Get hash	malicious	Browse	• 140.82.121.3

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 140.82.121.3
	Quotation.jar	Get hash	malicious	Browse	• 140.82.121.4
	02_extracted.jar	Get hash	malicious	Browse	• 140.82.121.3
	02_extracted.jar	Get hash	malicious	Browse	• 140.82.121.4
	dhl paket.jar	Get hash	malicious	Browse	• 140.82.121.3
	dhl paket.jar	Get hash	malicious	Browse	• 140.82.121.3
	jfTy8Hld20.exe	Get hash	malicious	Browse	• 140.82.121.3
	yxHYlyS6ec.exe	Get hash	malicious	Browse	• 140.82.121.3
	CxarNMwOrM.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
sonatype.map.fastly.net	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
	USpstracKER.jar	Get hash	malicious	Browse	• 199.232.19 2.209

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FASTLYUS	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quotation.jar	Get hash	malicious	Browse	• 199.232.192.209
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.192.209
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.192.209
	cs.exe	Get hash	malicious	Browse	• 151.101.1.194
	Exodus.exe	Get hash	malicious	Browse	• 185.199.108.133
	dhl paket.jar	Get hash	malicious	Browse	• 199.232.192.209
	dhl paket.jar	Get hash	malicious	Browse	• 199.232.192.209
	cs.exe	Get hash	malicious	Browse	• 151.101.1.194
	U6lZQUtrU5	Get hash	malicious	Browse	• 151.101.128.95
	tms.dll	Get hash	malicious	Browse	• 151.101.1.44
	qGGMaafxQt.dll	Get hash	malicious	Browse	• 151.101.1.44
	svQOxJeiVE.dll	Get hash	malicious	Browse	• 151.101.1.44
	u8KMSM5Yd4.dll	Get hash	malicious	Browse	• 151.101.1.44
	e2ngtxnWAP.dll	Get hash	malicious	Browse	• 151.101.1.44
GITHUBUS	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
	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 • 140.82.121.4
	Quotation sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	INQUIRY_____535262623.jpg.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	Quotation sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	RFQ_40ft Container.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	02_extracted.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	dhl paket.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	dhl paket.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	Quotation Sheet.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	USpstracKER.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	USpstracKER.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	Invoice.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	payment slip.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	Invoice.jar	Get hash	malicious	Browse	• 199.232.192.209 • 140.82.121.4
	payment slip.jar	Get hash	malicious	Browse	• 199.232.192.209 • 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):	4.896327242493616
Encrypted:	false
SSDEEP:	3:oFj4I5vpN6yUavp:oJ5X6yD
MD5:	A8A8C94C8D63B16960938AC6C0072DB5
SHA1:	EB93EB3812E0054D767D78B4818BF1035065AE07
SHA-256:	2506CFA73F44D2AEB618C5A2FBF8D81734D9B59BC1F26C2E469DF0FBE9E00124
SHA-512:	07E9C7D8A1E0A76EF7A5FBD486896BADD0DD875E6001136678C5E509ACDF00B23DB14D88CD5CC5404BE5EBD62A6E8DB4CCD8295BA8724A31CA031DCE9FAFBEC7
Malicious:	false
Reputation:	low
Preview:	C:\Program Files (x86)\Java\jre1.8.0_211..1632845399591..

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

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\83aa4cc77f591dfc2374580bbd95f6ba_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
SHA-256:	11E6ACA8E682C046C83B721EEB5C72C5EF03CB5936C60DF6F4993511DDC61238
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):	441941
Entropy (8bit):	5.040398967499683
Encrypted:	false
SSDEEP:	192:uMn3OOOOeeBeeR7mm0eeeee7mmvGGGrRBReeeOOOOO3OGGGGOOemOv3OOzeeeQeY:5G
MD5:	831332E72E8498EB18A6BD8338D3A99B
SHA1:	AF0ABAC4F8487276A286A78FA386DC8DBB153356
SHA-256:	58892D06E4C149B894736C14BDE3FD5F5CC1B8B5A9177611FE7E265064C57B24
SHA-512:	7C380E3183C04172DB5380C55A1DEC6920949CA791517967235AACA7A82DDBA3CE2A1AE1441612189713950A25C8F4B29D23B84A8B704E608F96F6320715FC01
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 #.# #.################################## ###################...returned false..C:\Users\user\lib\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/net/java/dev/jna/jna/5.5.0/jna-5.5.0.jar..EXCEPTION: https://github.com/kristian/system-hook/releases/download/3.5/system-hook-3.5.jar..EXCEPTION: https://repo1.maven.org/maven2/org/xerial/sqlite-jdbc/3.14.2.1/sqlit

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..-l.r....\...O..4...._r......s....N:.{.ry^B.:...eh.;}..\h.C...Z............2{,..&...............Hu.......w./-.....{..h-Y..

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 09:10:03.930704117 CEST	192.168.2.3	8.8.8.8	0x2c9c	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 09:10:03.931329012 CEST	192.168.2.3	8.8.8.8	0x3013	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:10:34.116592884 CEST	192.168.2.3	8.8.8.8	0x46	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 09:10:34.117388964 CEST	192.168.2.3	8.8.8.8	0xfacf	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:11:04.432183027 CEST	192.168.2.3	8.8.8.8	0xe712	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:11:04.432224989 CEST	192.168.2.3	8.8.8.8	0xf904	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 09:11:34.707647085 CEST	192.168.2.3	8.8.8.8	0x84c5	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 09:11:34.992959976 CEST	192.168.2.3	8.8.8.8	0x6e0d	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:04.783384085 CEST	192.168.2.3	8.8.8.8	0x783e	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:05.089884043 CEST	192.168.2.3	8.8.8.8	0x3893	Standard query (0)	github.com	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:34.830089092 CEST	192.168.2.3	8.8.8.8	0x3d24	Standard query (0)	repo1.maven.org	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:35.189574957 CEST	192.168.2.3	8.8.8.8	0xedee	Standard query (0)	github.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 28, 2021 09:10:03.950185061 CEST	8.8.8.8	192.168.2.3	0x2c9c	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:10:03.950185061 CEST	8.8.8.8	192.168.2.3	0x2c9c	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:10:03.950185061 CEST	8.8.8.8	192.168.2.3	0x2c9c	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:10:03.953293085 CEST	8.8.8.8	192.168.2.3	0x3013	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Sep 28, 2021 09:10:34.137681007 CEST	8.8.8.8	192.168.2.3	0x46	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:10:34.137681007 CEST	8.8.8.8	192.168.2.3	0x46	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:10:34.137681007 CEST	8.8.8.8	192.168.2.3	0x46	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:10:34.139309883 CEST	8.8.8.8	192.168.2.3	0xfacf	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Sep 28, 2021 09:11:04.471071005 CEST	8.8.8.8	192.168.2.3	0xe712	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Sep 28, 2021 09:11:04.471095085 CEST	8.8.8.8	192.168.2.3	0xf904	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:11:04.471095085 CEST	8.8.8.8	192.168.2.3	0xf904	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:11:04.471095085 CEST	8.8.8.8	192.168.2.3	0xf904	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 09:11:34.735385895 CEST	8.8.8.8	192.168.2.3	0x84c5	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:11:34.735385895 CEST	8.8.8.8	192.168.2.3	0x84c5	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:11:34.735385895 CEST	8.8.8.8	192.168.2.3	0x84c5	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:11:35.017296076 CEST	8.8.8.8	192.168.2.3	0x6e0d	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:04.802145958 CEST	8.8.8.8	192.168.2.3	0x783e	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:12:04.802145958 CEST	8.8.8.8	192.168.2.3	0x783e	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:04.802145958 CEST	8.8.8.8	192.168.2.3	0x783e	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:05.111862898 CEST	8.8.8.8	192.168.2.3	0x3893	No error (0)	github.com		140.82.121.3	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:34.849394083 CEST	8.8.8.8	192.168.2.3	0x3d24	No error (0)	repo1.maven.org	sonatype.map.fastly.net		CNAME (Canonical name)	IN (0x0001)
Sep 28, 2021 09:12:34.849394083 CEST	8.8.8.8	192.168.2.3	0x3d24	No error (0)	sonatype.map.fastly.net		199.232.192.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:34.849394083 CEST	8.8.8.8	192.168.2.3	0x3d24	No error (0)	sonatype.map.fastly.net		199.232.196.209	A (IP address)	IN (0x0001)
Sep 28, 2021 09:12:35.215615034 CEST	8.8.8.8	192.168.2.3	0xedee	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: 4536 Parent PID: 1360

General

Start time:	09:09:56
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\NRB-RTGS 28-Sept 2021.jar" >> C:\cmdlinestart.log 2>&1
Imagebase:	0xd80000
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: 4660 Parent PID: 4536

General

Start time:	09:09:57
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: 4348 Parent PID: 4536

General

Start time:	09:09:57
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\NRB-RTGS 28-Sept 2021.jar'
Imagebase:	0xd80000
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: 6780 Parent PID: 4348

General

Start time:	09:09:59
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:	0xed0000
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: 6780

General

Start time:	09:10:00
Start date:	28/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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