ID: 358324
Sample Name: UAE Contract Supply.jar
Cookbook: defaultwindowsfilecookbook.jbs
Time: 12:13:35
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report UAE Contract Supply.jar 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Compliance: 5
Software Vulnerabilities: 5
System Summary: 5
Data Obfuscation: 5
Persistence and Installation Behavior: 5
Boot Survival: 5
Malware Analysis System Evasion: 5
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 12
General Information 12
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 13
ASN 13
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 14
General 14
File Icon 14
Network Behavior 15
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: cmd.exe PID: 4864 Parent PID: 3880 15
General 15

File Activities 15
File Created 15
Analysis Process: conhost.exe PID: 4012 Parent PID: 4864 16
General 16
Analysis Process: java.exe PID: 6084 Parent PID: 4864 16
General 16
File Activities 16
File Created 16
File Written 17
File Read 18
Registry Activities 22
Analysis Process: icacls.exe PID: 6196 Parent PID: 6084 22
General 22
File Activities 22
Analysis Process: conhost.exe PID: 6208 Parent PID: 6196 23
General 23
Analysis Process: mx8043.exe PID: 6240 Parent PID: 6084 23
General 23
File Activities 23
Disassembly 23
Code Analysis 23

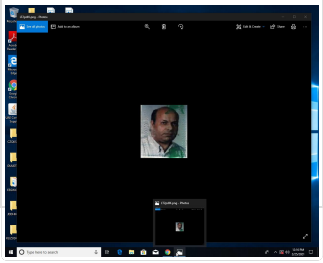
Analysis Report UAE Contract Supply.jar

Overview

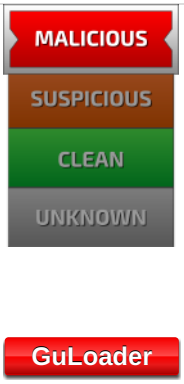
General Information

Sample Name:	UAE Contract Supply.jar
Analysis ID:	358324
MD5:	d23d186daf02db3.
SHA1:	1b2054ff2c9a3ff1..
SHA256:	459787308dd55a..
Tags:	jar
Infos:	

Most interesting Screenshot:



Detection



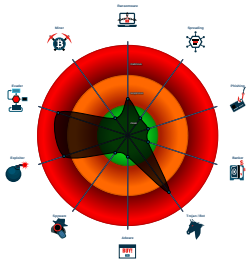
GuLoader

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

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Drops PE files to the user root direc…
- Exploit detected, runtime environme…
- Exploit detected, runtime environme…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…

Classification



Startup

- **System is w10x64**
- cmd.exe (PID: 4864 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\UAE Contract Supply.jar'' >> C:\cmdlinestart.log 2>&1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
  - conhost.exe (PID: 4012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - java.exe (PID: 6084 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\UAE Contract Supply.jar' MD5: 28733BA8C383E865338638DF5196E6FE)
    - icacls.exe (PID: 6196 cmdline: C:\Windows\system32\icacls.exe C:\ProgramData\Oracle\Java\.oracle_jre_usage /grant 'everyone':(OI)(CI)M MD5: FF0D1D4317A44C951240FAE75075D501)
      - conhost.exe (PID: 6208 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - mx8043.exe (PID: 6240 cmdline: C:\Users\user\mx8043.exe MD5: 335AA2DB46F51A80F6BE08948B564026)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

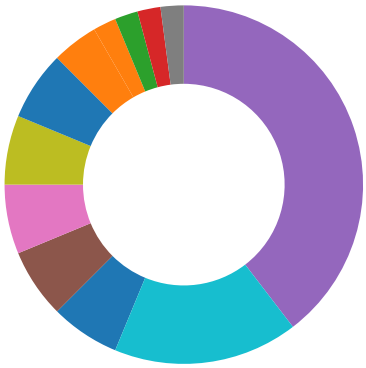
Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.247780398.0000000004D60000.00000004.00000001.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x4fd8:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
Process Memory Space: mx8043.exe PID: 6240	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: mx8043.exe PID: 6240	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Compliance:

Uses new MSVCR Dlls

Software Vulnerabilities:

Exploit detected, runtime environment starts unknown processes

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Persistence and Installation Behavior:

Exploit detected, runtime environment dropped PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

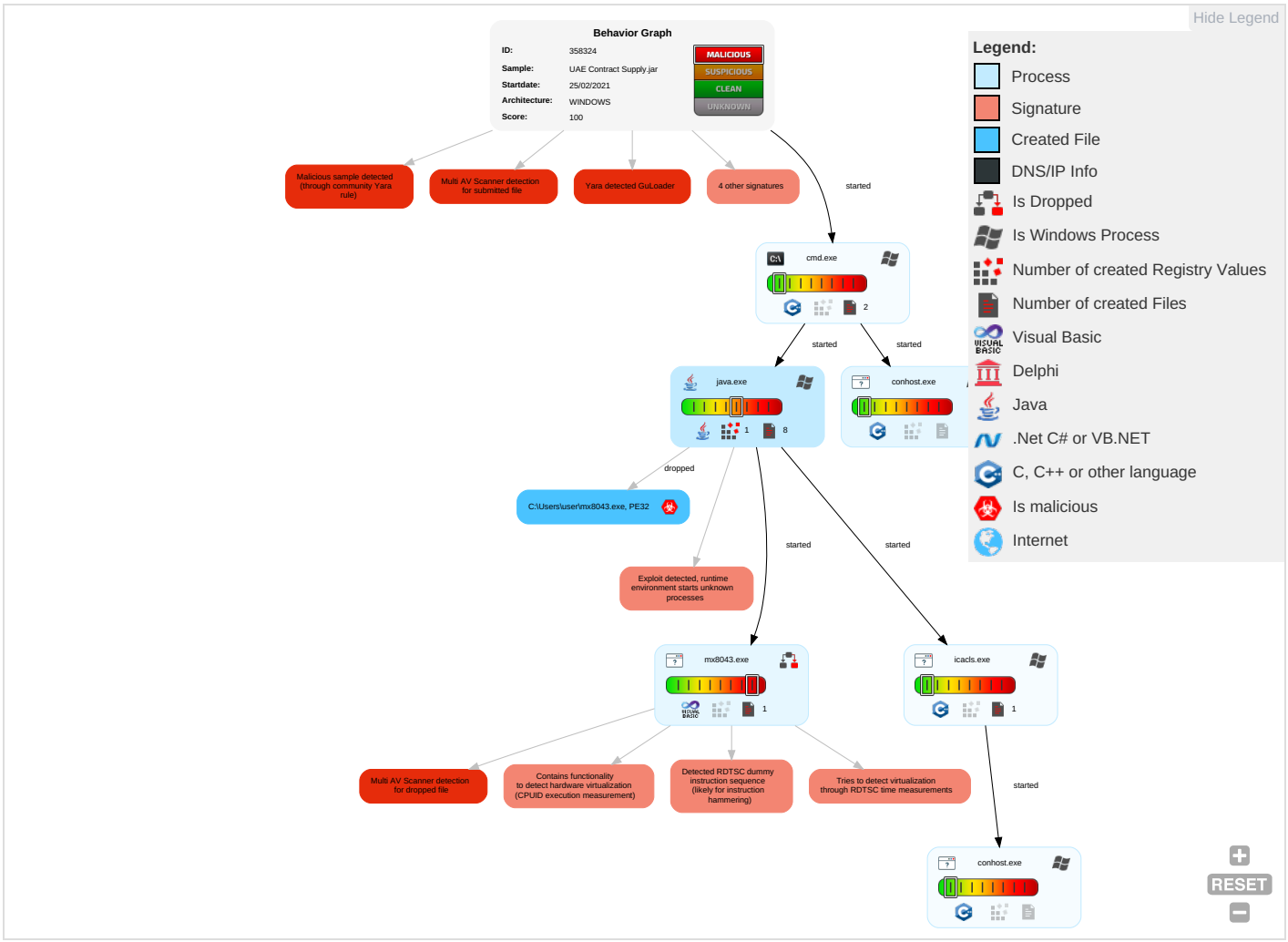
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

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	Command and Scripting Interpreter 2	Services File Permissions Weakness 1	Process Injection 1 2	Masquerading 1 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Exploitation for Client Execution 2	Boot or Logon Initialization Scripts	Services File Permissions Weakness 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 5 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 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	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Services File Permissions Weakness 1	Cached Domain Credentials	System Information Discovery 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

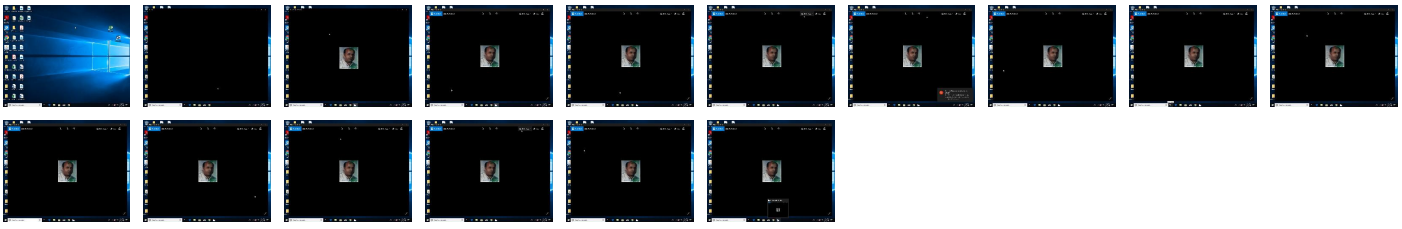
Behavior Graph

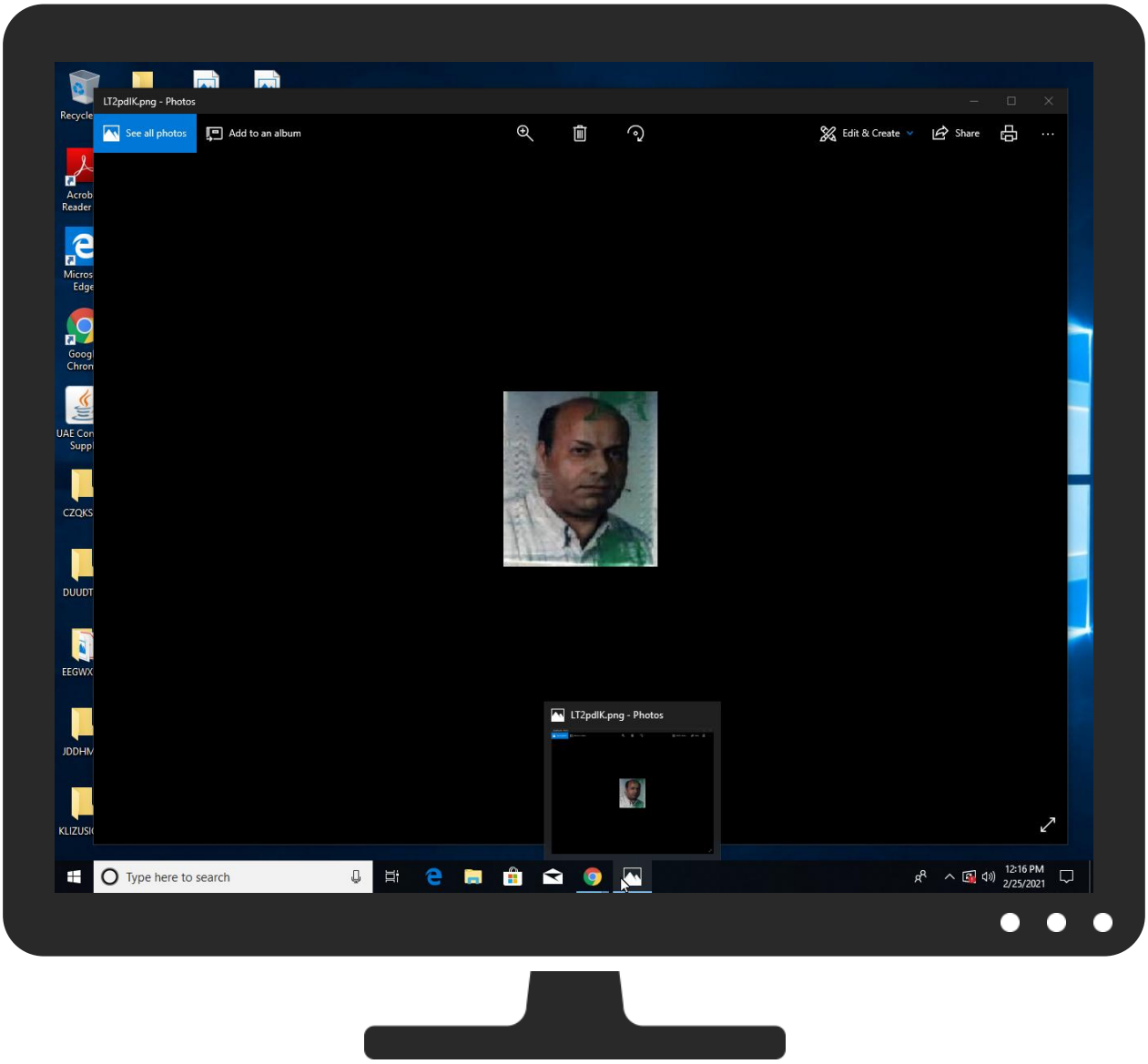


Screenshots

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
UAE Contract Supply.jar	20%	Virustotal		Browse
UAE Contract Supply.jar	33%	ReversingLabs	ByteCode-JAVA.Trojan.AdWind	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\mx8043.exe	17%	ReversingLabs	Win32.Trojan.Vebzenpak	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.java.exe.4d604e4.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.xrampsecurity.com/XGCA.crl	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
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://www.certplus.com/CRL/class2.crl	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl	0%	URL Reputation	safe	
http://policy.camerfirma.com3LT	0%	Avira URL Cloud	safe	
http://bugreport.sun.com/bugreport/	0%	Avira URL Cloud	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl0	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://cps.chambersign.org/cps/chambersroot.html	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.crl	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crl3	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	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://crl.securetrust.com/STCA.crl	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://www.certplus.com/CRL/class2.crl0	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://crl.xrampsecurity.com/XGCA.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://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersroot.htmlK#O	0%	Avira URL Cloud	safe	
http://www.quovadis.bm	0%	URL Reputation	safe	
http://www.quovadis.bm	0%	URL Reputation	safe	
http://www.quovadis.bm	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://policy.camerfirma.comk	0%	Avira URL Cloud	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://crl.securetrust.com/STCA.crlC/O	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://crl.chambersign.org/chambersroot.crl	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl	0%	URL Reputation	safe	
http://policy.camerfirma.com3	0%	Avira URL Cloud	safe	
http://www.chambersign.org	0%	URL Reputation	safe	
http://www.chambersign.org	0%	URL Reputation	safe	
http://www.chambersign.org	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	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

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.xrampsecurity.com/XGCA.crl	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class2.crl	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://policy.camerfirma.com3LT	java.exe, 00000002.00000002.248736888.000000000504D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://bugreport.sun.com/bugreport/	java.exe, 00000002.00000002.249049473.000000000A1C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/CJT	java.exe, 00000002.00000002.248736888.000000000504D000.00000004.00000001.sdmp	false		high
http://java.oracle.com/	java.exe, 00000002.00000002.249073461.000000000A1D6000.00000004.00000001.sdmp	false		high
http://null.oracle.com/	java.exe, 00000002.00000003.239994256.0000000015109000.00000004.00000001.sdmp, java.exe, 00000002.00000002.252839548.0000015712000.00000004.00000001.sdmp, java.exe, 00000002.00002.249357252.000000000A3B4000.00000004.00000001.sdmp	false		high
http://www.chambersign.org1	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	java.exe, 00000002.00000002.252951545.0000000015810000.00000004.00000001.sdmp	false		high
http://policy.camerfirma.com	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false		high
http://repository.swisssign.com/s	java.exe, 00000002.00000002.248954130.0000000005113000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://repository.swisssign.com/kKT	java.exe, 00000002.00000002.248736888.000000000504D000.00000004.00000001.sdmp	false		high
http://https://ocsp.quovadisoffshore.com	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl0	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadisglobal.com/cps	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/chambersroot.html	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp, java.exe, 00000002.00000002.248736888.000000000504D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl3	java.exe, 00000002.00000002.248954130.0000000005113000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	java.exe, 00000002.00000002.252951545.0000000015810000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crl	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/#	java.exe, 00000002.00000002.248736888.000000000504D000.00000004.00000001.sdmp	false		high
http://www.certplus.com/CRL/class2.crl0	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadisglobal.com/cps0	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false		high
http://crl.xrampsecurity.com/XGCA.crl0	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadisglobal.com/cps3	java.exe, 00000002.00000002.248736888.000000000504D000.00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/chambersroot.htmlK#O	java.exe, 00000002.00000002.248954130.0000000005113000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quovadis.bm	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp, java.exe, 00000002.00000002.248736888.000000000504D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://policy.camerfirma.comk	java.exe, 00000002.00000002.248736888.000000000504D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ocsp.quovadisoffshore.com0	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.securetrust.com/STCA.crlC/O	java.exe, 00000002.00000002.248954130.0000000005113000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.swisssign.com/S$Q	java.exe, 00000002.00000002.248736888.000000000504D000.00000004.00000001.sdmp	false		high
http://crl.chambersign.org/chambersroot.crl	java.exe, 00000002.00000002.249513940.000000000A46E000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://policy.camerfirma.com3	java.exe, 00000002.00000002.248954130.0000000005113000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://repository.swisssign.com/	java.exe, 00000002.00000002.24 9513940.000000000A46E000.00000 004.00000001.sdmp	false		high
http://www.chambersign.org	java.exe, 00000002.00000002.24 9513940.000000000A46E000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://policy.camerfirma.com0	java.exe, 00000002.00000002.24 9513940.000000000A46E000.00000 004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358324
Start date:	25.02.2021
Start time:	12:13:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UAE Contract Supply.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:	26
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:	mal100.troj.expl.evad.winJAR@9/3@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 32.2% (good quality ratio 24.4%) • Quality average: 47.6% • Quality standard deviation: 31.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .jar
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, Microsoft.Photos.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, ApplicationFrameHost.exe, svchost.exe • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

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)\Java\jre1.8.0_211\bin\java.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.847995882806536
Encrypted:	false
SSDEEP:	3:oFj4I5vpN6yUYUXOvn:oJ5X6y8XAn
MD5:	9B416AAFCA54628313A96E06881D3711
SHA1:	238B699D6C8B2FBB15B558A28EBAE1B83B192A0C
SHA-256:	ACE4B289380CAB58D2A29A98EE8032AD628F1004C493E269FCDA38AF115CC62C
SHA-512:	711FA7481C975EA0A7049AE1C4E45D9B052F09447878580B0DFC6AF638494B41B5FE7B2576B6EBA2F32782F59A50866E0885040498586D7D9B15ABD4152E4FF2
Malicious:	false
Reputation:	low
Preview:	C:\Program Files (x86)\Java\jre1.8.0_211..1614284065233..

C:\Users\user\LT2pdIK.png	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	PNG image data, 190 x 216, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68600
Entropy (8bit):	7.9810935688737725
Encrypted:	false
SSDEEP:	1536:VxaDM0hvN4cro9ToaHymKnenubWp71Az/AJ0:CD914cr+o9qBjAz/AC
MD5:	79E0DAD14E7C20A777E72FC023B59252

C:\Users\user\LT2pdIK.png	
SHA1:	50F959BAB2FF58E44DBA17EF85375EC7EBD66924
SHA-256:	A089D9AD3875FFA321D2DFD38661992721EFF5E0ACF36D76A7A5C8FE054B7992
SHA-512:	39F4EF3E670C40314F0364CEC370EAF9B19BC44A693BB47C669517059D220A2D41F8622850D7F969CE4FAB1CF6A7D39ADCF9F41637AF1335702A14750D7EBC2
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....U.Y.....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^|.i.&K...=.Y.Y.v....=.....A..I..)...@.....C.f'@.?C}.....@.$..d F.H.ER.+Rf ...1.}..oY.U.....{{F.g Dx..?.....=y.{..dwrz...'_.|.l.....G.7..w.....RNw.v.r.....9;{.{.....a.....}...\:h.@.e...%.Ey.r.....i..Kk.6.T.R..{..r5..s\|)....b..\k.....i.Hd.t)..x.Sn.U.uK..M.)Wxi.m9P..<x..i;\|QFqE../ ..l..`....{..r\|.{..ux../_=..}.{.....Y./.....;.\|P..ys..r.(...^.\|.....{}z...gl.....R....Rn...ge...<.&.`w..C9P.g.y.f.../_.....li..NOOJ...~.v..i..+W.....a.....k.C.....`s.....x.....rxew\|t.;.....a....K)$. .8...X..A.R...l...4u.d..)d..D./..qA4e.....A ....BQb.....L..e.f.....F..~...W..C...(.R..-?{t...H.0.y...ul..0$...>ma.(>*...s.(.[.F.ay....a..+G...8...I....B..H[.i.P.....S..u.'0..).r.....A...y...F .i.....RD.)....K:|....=..... .....d.....<I.>.y.fw..4J}Vc}.'y..wQ.wo.4O.Oj;..0.\.s=..^..E.....C.u.....".....4<...W.w.GWw.W.

C:\Users\user\mx8043.exe	
Process:	C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	299008
Entropy (8bit):	5.515398750036674
Encrypted:	false
SSDEEP:	6144:PPfEI/UKHsSDjuHl9IfNpmhb5mFCQcGN:Xf5sSuMfNQJ5mFvcy
MD5:	335AA2DB46F51A80F6BE08948B564026
SHA1:	848D5909A84BACA2255C932C61EF58A34072AFDA
SHA-256:	92B87477B4589030A4D6E94B07CDEFA4712426FCCEC7FDFEEBE0EC4BDC358048
SHA-512:	C7F7168B7F4DAA87B874E2EC6B45C7196BF24710C961FF5B33C37205DC074D6F5653A455D437C9B1A16CDD7ED83D0A16D8684E080591DF8F7F778EF969961CD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L...[. S.....0...`.....H.....@....@.....T9..<....`...7.....8...0.....text...d-... ....0..... ..`.data.....@.....@.....@....rsrc....7...`...@...P.....@..@8|.\.....I#.....USER32.DLL.MSVBVM60.DLL..... ....

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract
Entropy (8bit):	7.998905736237949
TrID:	• Java Archive (13504/1) 62.80% • ZIP compressed archive (8000/1) 37.20%
File name:	UAE Contract Supply.jar
File size:	312777
MD5:	d23d186daf02db3cecee462c5b1fe15c
SHA1:	1b2054ff2c9a3ff13920f07905b7e313a75b77dc
SHA256:	459787308dd55a6822b80ee2fd9d4add4e44602f783e8c9 84697a8918839ff22
SHA512:	ad01ec9e3a41b5258d80fe8cd5b513cf379ac4dce5f5727 4379dc1ef893379c83062da7f24780b1844dd2d8c07f370 025eaed47eec20264ce4ded822aca089e2
SSDEEP:	6144:qZifZoLlSASY5iE0XtGlX47i+Co7TmbB6PP+alppn e5VTzSo:akZoxSI0E0wCe63+alppneT2o
File Content Preview:	PK.....D0XR.....META-INF/..PK.....PK..... .D0XR.....META-INF/MANIFEST.MFM.1..0...@.... !..R...Rj.PJ..4..H.....7vi.....^.....(.,7.I>`...,.ct..t...(...F.s. OD...i.v...n..}8....q.W.}..=D..uu.eP.2.KaVZCK.R....}.y.Z/.. MJ

File Icon

Icon Hash:	d28c8e8ea2868ad6

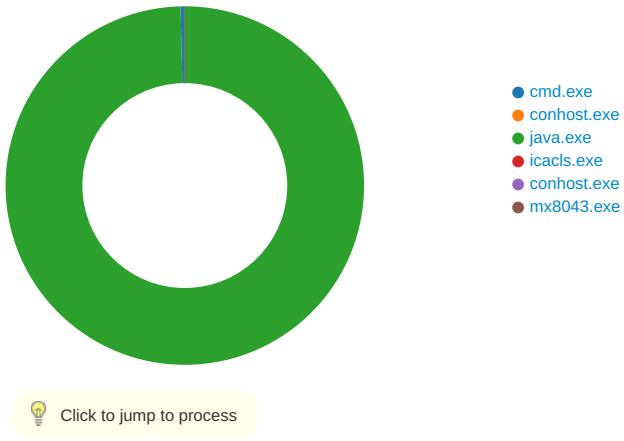
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: 4864 Parent PID: 3880

General

Start time:	12:14:22
Start date:	25/02/2021
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\UAE Contract Supply.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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\cmdlinestart.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	15D194	CreateFileW

Analysis Process: conhost.exe PID: 4012 Parent PID: 4864

General

Start time:	12:14:22
Start date:	25/02/2021
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: 6084 Parent PID: 4864

General

Start time:	12:14:23
Start date:	25/02/2021
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\UAE Contract Supply.jar'
Imagebase:	0x9c0000
File size:	192376 bytes
MD5 hash:	28733BA8C383E865338638DF5196E6FE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Java
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000002.00000002.247780398.0000000004D60000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\hsperfdata_user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6DA58C5B	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\hsperfdata_user\6084	read attributes | delete | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | delete on close	success or wait	1	6DA58D58	CreateFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Oracle\Java\.oracle_jre_usage	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	732C845C	CreateDirectoryW
C:\ProgramData\Oracle\Java\.oracle_jre_usage\cce3fe3b0d8d83e2.timestamp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open reparse point	success or wait	1	732C80CF	CreateFileW
C:\Users\user\mx8043.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	732C9D3D	CreateFileW
C:\Users\user\LT2pdIK.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	732C9D3D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Oracle\Java\.oracle_jre_usage\cce3fe3b0d8d83e2.timestamp	unknown	57	43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 4a 61 76 61 5c 6a 72 65 31 2e 38 2e 30 5f 32 31 31 0d 0a 31 36 31 34 32 38 34 30 36 35 32 33 33 0d 0a	C:\Program Files (x86)\Java\jre1.8.0_211..1614284065233..	success or wait	1	732C9FBC	WriteFile
C:\Users\user\mx8043.exe	unknown	299008	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 37 62 c4 da 73 03 aa 89 73 03 aa 89 73 03 aa 89 f0 1f a4 89 72 03 aa 89 3c 21 a3 89 76 03 aa 89 45 25 a7 89 72 03 aa 89 52 69 63 68 73 03 aa 89 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 5b ec aa 53 00 00 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 30 01 00 00 60 03 00 00 00 00 00 48 13 00 00 00 10 00 00 00 40 01 00 00 00 40	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......7b..s...s...s.......r... <!..v...E%..r...Richs....... ....................PE..L...[. .S.................0...`...... H........@....@	success or wait	1	732C9FBC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\LT2pdIK.png	unknown	68600	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 be 00 00 00 d8 08 06 00 00 00 55 d9 59 da 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 ff a5 49 44 41 54 78 5e 7c fd 69 93 26 4b 96 1f f6 3d 95 59 95 59 fb 76 b7 be dd d3 3d d3 03 80 a4 19 41 83 00 49 90 19 29 ca f0 01 40 02 1a 01 98 05 43 0c 66 27 40 19 3f 43 7d 0a bd 90 de 8b 12 40 83 24 a3 99 64 20 46 00 48 18 45 52 d2 2b 52 66 20 84 ad a7 31 dd 7d bb ef bd b5 6f 59 99 55 a5 ff ef 7f c2 9f cc 7b 7b 46 f1 a4 67 44 78 b8 1f 3f bb 1f f7 f0 88 b8 f4 ff fc 7f ff d7 ef 1f 3d 79 bc 7b f5 e6 64 77 72 7a b6 fb ec 27 5f ec be 7c f4 6c f7 c5 c3 87 bb d3 b3 b7 bb cb 47 c7 bb 37 a7 ef 77 bb f7 87 bb	.PNG.....IHDR.....U .Y.....sRGB.....gAMA..... a.....pHYs.....+.....IDA Tx^|.i.&K...=.Y.Y.v....=.....A ..I..)...@.....C.f'@.?C}..... @.$..d F.H.ER.+Rf ...1.}....oY.U..... {{F..gDx..?.....=y. {..dwrz...'_..|.l..... ....G..7..w....	success or wait	1	732C9FBC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	22	success or wait	1	9D70AE	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	1024	success or wait	1	9D70AE	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\i386\jvm.cfg	unknown	4096	success or wait	1	9D70AE	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\i386\jvm.cfg	unknown	4096	end of file	1	9D70AE	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	1024	success or wait	1	6DA0ADA8	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	4096	success or wait	1	6D8CC013	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	4096	end of file	1	6D8CC2CA	unknown
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	128	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	97	success or wait	3	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	749	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\meta-index	unknown	8192	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\meta-index	unknown	8192	end of file	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	6760	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	8192	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\meta-index	unknown	8192	end of file	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	154	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\resources.jar	unknown	128	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	3	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	3954	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	7	732C9F67	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	4	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	30	success or wait	103	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\AppData\Local\Temp\jartracer.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	466	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	164	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\java.security	unknown	8192	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\java.security	unknown	8192	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\java.security	unknown	8192	end of file	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	147	success or wait	2	732C9F67	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	30	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	128	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Users\user\Desktop\UAE Contract Supply.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	128	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	128	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jsse.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	128	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\US_export_policy.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\US_export_policy.jar	unknown	128	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\US_export_policy.jar	unknown	407	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\US_export_policy.jar	unknown	149	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\US_export_policy.jar	unknown	30	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\local_policy.jar	unknown	4	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\policy\unlimited\local_policy.jar	unknown	128	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	8192	success or wait	6	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	3	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\blacklisted.certs	unknown	8192	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\blacklisted.certs	unknown	8192	end of file	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\cacerts	unknown	8192	success or wait	4	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunec.jar	unknown	160	success or wait	1	732C9F67	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\security\cacerts	unknown	32768	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\ext\sunjce_provider.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\jce.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\accessibility.properties	unknown	8192	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\accessibility.properties	unknown	8192	end of file	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	5	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	16	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	2	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	2562	success or wait	748	732C9F67	ReadFile
C:\Program Files (x86)\Java\jre1.8.0_211\lib\rt.jar	unknown	160	success or wait	1	732C9F67	ReadFile

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: icacls.exe PID: 6196 Parent PID: 6084

General

Start time:	12:14:25
Start date:	25/02/2021
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:	0xb70000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6208 Parent PID: 6196

General

Start time:	12:14:25
Start date:	25/02/2021
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: mx8043.exe PID: 6240 Parent PID: 6084

General

Start time:	12:14:27
Start date:	25/02/2021
Path:	C:\Users\user\mx8043.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\mx8043.exe
Imagebase:	0x400000
File size:	299008 bytes
MD5 hash:	335AA2DB46F51A80F6BE08948B564026
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Antivirus matches:	• Detection: 17%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis